UNIVERSITÀ DEGLI STUDI DI ROMA

LA SAPIENZA

FACOLTÀ DI INGEGNERIA

Dottorato in Ingegneria Industriale e Gestionale

Implementazione di un modello di Fraud Detection basato su logiche di Machine Learning

Dottorando

Riccardo Maestri

Docente Guida:

Prof. Giulio Di Gravio

I shall be telling this with a sigh
Somewhere ages and ages hence:
Two roads diverged in a wood, and I—
I took the one less traveled by,
And that has made all the difference.

Robert Frost

INDICE

Sommario

INTRODUZIONE 1

1. FRAUD MANAGEMENT 7

1.1 Il concetto di frode 8

1.2 Aspetti Normativi 9

1.3 La Convenzione Di Budapest 12

1.4 Il Fraud Act 12

1.5 Le Esperienze Oltre Oceano 13

1.6 Natura Ed Elementi Della Frode 14

1.7 Classificazione Delle Frodi 17

1.8 Aspetti Psicologici Della Frode 20

1.9 Il Triangolo Della Frode 23

1.10 Lo Sviluppo Di Un Sistema Antifrode 25

1.11 La Realizzazione Di Un Programma Antifrode 28

1.12 La Governance Del Rischio Di Frode 30

1.13 La Valutazione Del Rischio Di Frode 33

1.14 Fraud Prevention E Fraud Detection 36

1.15 Fraud Prevention: Analisi Per Fattori di Rischio 38

1.16 Fraud Detection: Analisi Per Fattori Di Rischio 61

1.17 Controllo E Monitoraggio 67

1.18 Focus: whistleblowing 71

1.19 Fraud Investigation And Audit 95

1.20 Focus: computer forensic 103

2. FRAUD MANAGEMENT NELL'INFORMATION AND COMMUNICATION TECHNOLOGY 134

2.1 Frodi e banche 135

2.2 Il rischio operativo e frode in banca – il caso Intesa San Paolo Personal Finance 144
2.3 Frodi e telecomunicazioni 174
2.4 La gestione delle frodi nelle comunicazioni – Il caso Wind 184
2.5 Frodi e assicurazioni 197
2.6 Frodi e gaming 201
2.7 Le frodi ict tipiche di alcuni canali 208
2.8 Pagamenti on-line 208
2.9 Mobile 214
2.10 Carte di Credito 220
3. PROGETTAZIONE DEL MODELLO DI FRAUD DETECTION 227
3.1 Il Machine Learning 228
3.2 Il Processo di Machine Learning 231
3.3 Azure machine learning 233
3.4 Fasi progettuali del machine learning 235
3.5 Implementazione del modello 242
3.6 Aggregazione dei dati 244
3.7 Strutturazione dei dati 250
3.8 Implementazione logiche di arricchimento 255
3.9 Addestramento del modello 261
3.10 Definizione metriche di valutazione 264
3.11 Valutazione delle capacità predittive del modello 270
3.12 Publish web service 277
4. CONCLUSIONI 278
5. BIBLIOGRAFIA 281

INTRODUZIONE

La descrizione delle fenomenologie fraudolente, nonché delle modalità e dei contesti in cui le stesse si manifestano, richiede un approccio multidisciplinare come in pochi altri campi di osservazione [3]. Nel fraud management non esiste un unico body of knowledge, ma un approccio organico che comprende aspetti umani, organizzativi, normativi, nonché una conoscenza delle tecnologie e delle fenomenologie sociali e culturali [9].

La frode, nelle sue diverse forme, si manifesta in ogni contesto e situazione ove c'è qualcuno che possiede un valore e qualcun altro che ne vuole ottenere il possesso senza pagare però alcun "prezzo", utilizzando tecniche volte a eludere ostacoli che si frappongono tra lui e il bene senza l'impiego di mezzi violenti, facendo ricadere su altri (inclusa la vittima) la responsabilità delle proprie azioni [15]. La frode è un reato di opportunità, nel senso che si manifesta laddove le "barriere" non esistono o non sono sufficientemente efficaci [10]. È caratterizzata da una forte componente umana e colpisce indifferentemente persone giuridiche e fisiche a prescindere dalla loro localizzazione, natura e status economico e sociale [27].

Nelle realtà aziendali la frode è finalizzata alla sottrazione di tutto ciò che possa avere un valore commerciale ed economico e può essere perpetrata da soggetti interni ed esterni all'azienda attraverso differenti tecniche [32]. Diversi indicatori registrano come i danni economici, ma anche reputazionali e gestionali, provenienti da questo rischio possano compromettere l'efficenza e l'efficacia di un'organizzazione nel perseguimento dei propri obiettivi di business [6]. La frode è un rischio, ed in quanto tale, necessita di un dedicato sistema capace di identificare, analizzare, valutare, prevenire e in ultima istanza gestire tale fattualità [62]. Il sistema antifrode implementato in un'azienda deve necessariamente includere nel proprio perimetro di azione tutte le funzioni aziendali che, in

relazione alle proprie attività, hanno necessità di rafforzare i sistemi di controllo e di monitoraggio dei rischi di business per contenere le minacce in una visione olistica [86]. La funzione aziendale deputata al Security Risk Management può, in questo campo, essere un elemento strategico che, grazie alle sue expertise e capabilities nel campo delle indagini e delle investigazioni, è in grado di implementare corretti sistemi di fraud prevention e fraud detection. La fraud prevention riguarda le procedure, le policies, la formazione e la comunicazione, mentre la fraud detection invece riguarda sistemi e metodologie di rilevamento di comportamenti sospetti o atti fraudolenti una volta che sono stati compiuti [103]. Naturalmente, l'implementazione di un sistema efficiente di fraud detection agisce anche come deterrente, operando quindi da fattore di prevenzione [107].

La frode è antica quanto l'umanità stessa e può assumere una varietà illimitata di forme diverse. Inoltre, lo sviluppo di nuove tecnologie fornisce ulteriori modi con cui si può commettere una frode [45], ad esempio nel commercio elettronico le informazioni sulla carta sono sufficienti per perpetrare una frode [40]. L'uso delle carte di credito è prevalente ai nostri giorni, e le frodi in questo ambito sono cresciute negli ultimi anni. Perdite finanziarie dovute alle frodi riguardano non solo i commercianti e le banche, ma anche i singoli clienti. Se la banca perde denaro, i clienti alla fine pagano anche attraverso interessi più elevati, tariffe, quote associative più alte, etc.. La frode può anche influenzare la reputazione e l'immagine di un commerciante causando perdite non finanziarie che, sebbene difficili da quantificare a breve termine, possono diventare visibili nel lungo periodo [83]. Ad esempio, se un titolare della carta è vittima di una frode con una certa azienda, potrebbe non fidarsi più e scegliere un concorrente. Le azioni intraprese contro le frodi derivanti dalle transazioni con carte di credito possono essere suddivise in preventive, che tentano di bloccare le transazioni fraudolente

alla fonte, e di rilevamento delle frodi, laddove le frodi abbiano avuto successo e le transazioni sono identificate a posteriori [58].

Alcune Tecnologie che sono state utilizzate per prevenire le frodi sono Address Verification Systems (AVS), Card Verification Method (CVM) e numero di identificazione personale (PIN). AVS prevede la verifica dell'indirizzo con codice postale del cliente mentre CVM e PIN comportano il controllo del codice numerico che viene digitato dal cliente.

Il rilevamento delle frodi derivanti da carte di credito è, dato un insieme di transazioni, il processo di identificazione che porta a comprendere se una transazione autorizzata appartiene alla classe delle transazioni fraudolente o meno [33]. Un sistema di rilevamento delle frodi non dovrebbe solo rilevare i casi di frode in modo efficiente, ma essere anche conveniente dal punto di vista dei costi, in quanto il valore investito nello screening delle transazioni non deve essere superiore alla perdita dovuta a frodi [110]. Al fine di minimizzare costi di rilevazione è possibile utilizzare modelli statistici per fare un controllo tra frode reale e potenziale, permettendo così di esaminare solo i casi ad alto rischio [36]. Attraverso l'uso delle tecniche di Machine Learning possiamo efficacemente scoprire modelli fraudolenti e prevedere le transazioni che hanno maggiori probabilità di essere fraudolente [67]. Queste consistono nel dedurre un modello di previsione sulla base di un insieme di esempi. Nella maggior parte dei casi il modello è una funzione parametrica, che consente di prevedere la probabilità che una transazione sia considerata una frode, data una serie di funzioni che descrivono la transazione [84]. Nel campo del rilevamento delle frodi, l'uso di tecniche di apprendimento è interessante per diverse ragioni. Innanzitutto, consentono di rilevare schemi di comportamento in flussi di dati ad alta numerosità, come le transazioni che generano un flusso continuo di dati ed

ognuna è definita da variabili [20]. In secondo luogo, le transazioni fraudolente sono spesso correlate sia nel tempo che nello spazio. Ad esempio, i truffatori in genere cercano di commettere frodi nello stesso negozio con diverse carte in un breve periodo di tempo. In terzo luogo, le tecniche di apprendimento possono essere utilizzate per rilevare e modellare strategie fraudolente esistenti ed identificarne nuove, associate ai comportamenti abituali dei titolari di carta. Quando una frode non può essere prevenuta, è auspicabile rilevarla il più rapidamente possibile. In entrambi i casi di prevenzione e rilevazione, il problema è amplificato da un certo numero di vincoli e caratteristiche [17]. Innanzitutto, bisogna fare attenzione a non prevenire troppe transazioni legittime o bloccare erroneamente carte valide, evitando così l'irritazione del cliente. In secondo luogo, la maggior parte delle banche elabora un gran numero di transazioni, di cui solo una piccola parte è fraudolenta. In terzo luogo, solo un numero limitato di transazioni possono essere verificate dagli investigatori, ovvero si può chiedere ad una persona umana di controllare tutte le transazioni una per una e decidere se queste siano fraudolente o no. In altre parole, aziende e istituzioni pubbliche, hanno bisogno di sistemi automatici in grado di supportare il rilevamento di frodi [34].

Un modo di automatizzare il rilevamento è mediante i metodi data driven, come ad esempio impostare un sistema di rilevamento basato su logiche di machine learning, in grado quindi di apprendere dai dati in modo supervisionato quali schemi sono probabilmente legati a un comportamento fraudolento [53]. Gli approcci basati sui dati presentano vantaggi e svantaggi. Con gli algoritmi di Machine Learning, ad esempio, possiamo apprendere complesse configurazioni fraudolente, gestire grandi volumi di dati e prevedere nuovi tipi di frode. Tuttavia presentano alcuni svantaggi, come la necessità di volumi di dati sufficienti.

Quindi, le soluzioni data driven devono esser viste come uno strumento di supporto agli esperti per ottenere un rilevamento più accurato [48].

L'obiettivo di questa tesi riguarda l'applicazione di metodi data driven basati sul machine learning. La progettazione di un sistema di rilevazione delle frodi basato su metodi data driven non è un processo semplice [137], richiede decisioni in merito a quale features usare, quale strategia (apprendimento supervisionato o non supervisionato), algoritmo (ad es. alberi decisionali, rete neurale) e con quale frequenza deve essere aggiornato il modello (una volta all'anno, mensilmente o ogni volta nuovi dati disponibili).

La progettazione di un fraud detection system che impiega metodi data driven basati su algoritmi di Machine Learning è particolarmente impegnativo per i seguenti motivi:

- Le frodi rappresentano una piccola parte di tutte le transazioni giornaliere;
- La distribuzione delle frodi si evolvono nel tempo a causa della stagionalità e della nuova strategia di attacco;
- La vera natura della maggior parte delle transazioni è generalmente nota solo alcuni giorni dopo la transazione, poiché solo poche di esse sono tempestivamente controllate dagli investigatori.

Il primo punto è noto anche come problema sbilanciato, dal momento che la distribuzione delle transazioni tende verso quelle non fraudolente [79]. La maggior parte degli algoritmi di machine learning non sono progettati per far fronte a distribuzioni di classi di questo tipo. Il cambiamento nelle attività fraudolente e nel comportamento del cliente è il principale responsabile della non stazionarietà nel flusso delle transazioni. Questa situazione è di estrema rilevanza per i sistemi di rilevazione, che devono essere costantemente aggiornati

sfruttando gli elementi supervisionati più recenti e dimenticando quindi informazioni obsolete che potrebbero risultare fuorvianti, facendo perdere loro le capacità predittive a lungo termine. La terza sfida è legata al fatto che, in un contesto reale, non risulta possibile controllare tutte le transazioni [54]. Il costo del lavoro umano limita seriamente il numero di alert restituiti dal sistema di rilevazione che possono essere convalidati dagli investigatori. La verifica degli investigatori può essere fatta chiamando il titolare della carta, fornendo al sistema di rilevazione feedback che indicano se le segnalazioni fossero correlate a transazioni fraudolente o autentiche [56]. Questi feedback, che si riferiscono a una minima parte dell'importo delle transazioni giornaliere, sono le uniche informazioni che possono essere fornite per addestrare o aggiornare i modelli.

Nel capitolo terzo viene presentato quindi un modello di fraud detection basato su logiche di machine learning, implementato in Azure Machine Learning [151], un tool fornito da Microsoft che può essere acceduto via browser, in quanto servizio in cloud. Azure Machine Learning fornisce un ambiente di progettazione integrato e completo, che rende disponibili moduli precompilati che vengono utilizzati per le varie fasi del processo di implementazione del modello. La scelta, oltre che di natura tecnica, è stata anche di natura commerciale, in quanto la società per cui lavoro è Gold Partner Microsoft®.

1. FRAUD MANAGEMENT

La frode rappresenta una grave minaccia per le aziende. Diversi indicatori registrano come i danni economici, ma anche reputazionali e gestionali, provenienti da questo rischio possano compromettere l'efficienza e l'efficacia di un'organizzazione nel perseguimento dei propri obiettivi di business [15].

La frode è un rischio, ed in quanto tale necessita di un dedicato sistema capace di identificare, analizzare, valutare, prevenire ed in ultima istanza gestire tale fattualità. Un'azienda che decida di implementare un modello di fraud management deve necessariamente includere nel proprio perimetro di azione tutte le funzioni aziendali che, in relazione alle proprie attività, abbiano necessità di rafforzare i sistemi di controllo e di monitoraggio dei rischi di business per contenere le minacce in un'ottica olistica. La funzione aziendale deputata al Security Risk Management può, in questo campo, essere un elemento strategico, grazie alle sue expertise e capabilities nel campo delle indagini e delle investigazioni, risultando essere quindi in grado di progettare corretti sistemi di fraud detection e fraud prevention [73].

Lo sviluppo di un sistema antifrode capace di inglobare sinergicamente tutte le rilevanti funzioni aziendali, è conseguenzialmente la chiave per contrastare fenomeni fraudolenti che possono arrecare ingenti danni all'azienda se non considerati in un contesto di Enterpise Risk Management.

1.1 Il concetto di frode

A tutt'oggi non esiste ancora a livello internazionale una definizione di "frode" univoca e condivisa, ne esistono molteplici varianti, ciascuna legata al punto di vista dell'area di provenienza, talvolta anche a prescindere dal quadro normativo vigente. Tendenzialmente, la frode è un comportamento illecito con il quale si mira ad eludere precise disposizioni di legge oppure un inganno inteso a danneggiare gli altri a proprio vantaggio. L'Association of Certified Fraud Examiners intende per frode "qualsiasi reato che comporti guadagno e che usi l'inganno come suo principale modus operandi" [112]. Si potrebbe ampliare la definizione indicando come frode "qualsiasi azione scorretta che venga commessa intenzionalmente, attraverso, a volte, l'utilizzo di mezzi iniqui, al fine di ottenere per sè o per terze parti, direttamente o indirettamente, un tangibile o intangibile vantaggio non dovuto, ovvero di evadere un'obbligazione di qualsiasi natura" [107]. Spesso i termini frode e truffa vengono confusi, scambiati o usati l'uno come sinonimo dell'altro. La truffa infatti, come definita dal nostro diritto, è "l'ottenimento di un vantaggio a scapito di un altro soggetto indotto in errore attraverso artifici e raggiri". Potremmo affermare quindi che "si froda truffando" o che "si truffa per mezzo della frode".

1.2 Aspetti Normativi

Nella lingua italiana, il dizionario fornisce la seguente definizione di frode: "Atto o comportamento diretto a ledere con l'inganno un diritto altrui. In diritto penale, il termine *frode* indica una serie di condotte caratterizzate da modalità elusive previste come reato dal codice o dalle leggi speciali (frode in commercio, frode fiscale, frode alla legge, frode pia, frode processuale). Più in generale, si può definire frode qualsiasi inganno, artificio o astuzia malvagia con cui si sorprende l'altrui buona fede.

La frode consta di due elementi distintivi: l'intento di conseguire un risultato che altrimenti non si sarebbe realizzato e la concretizzazione dell'intento attraverso inganni, astuzie o raggiri. Gli articoli rilevanti del codice penale da prendere in considerazione sono sostanzialmente inerenti al reato di truffa e ad alcune fattispecie specifiche come la frode informatica, la frode assicurativa, l'insolvenza fraudolenta.

La truffa è un reato previsto dall'art. 640 del codice penale, ai sensi del quale chiunque, con artifizi o raggiri, inducendo taluno in errore, procuri a sé o ad altri un ingiusto profitto con altrui danno, viene punito secondo quanto previsto dall'articolo. È un reato a dolo generico e di evento, cioè si consuma nel momento della verifica dell'evento dannoso per la vittima e proficuo per il reo. È perseguibile a querela di parte a meno che non si verifichi una delle circostanze aggravanti previste dall'art. 61 codice penale, nel qual caso è perseguibile d'ufficio.

Vi sono due particolari circostanze aggravanti del reato di truffa, al verificarsi delle quali il reato è parimenti perseguibile d'ufficio:

- se la truffa è a danno dello Stato o di altro ente pubblico;

- se è commessa facendo nascere nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dover eseguire un ordine dell'autorità.

Inoltre, sono presenti alcune fattispecie particolari, alcune delle quali denominate frode. In particolare:

- Art. 640-bis: truffa aggravata per il conseguimento di erogazioni pubbliche. La pena è la reclusione da uno a sei anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o della Comunità Europea;
- Art. 640-ter: frode informatica. Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito ai sensi dell'articolo;
- Art. 641: insolvenza fraudolenta. Chiunque, dissimulando il proprio stato d'insolvenza, contrae un'obbligazione col proposito di non adempierla è punito, a querela della persona offesa, qualora l'obbligazione non sia adempiuta, ai sensi dell'articolo;
- Art. 642: frode assicurativa. Fraudolenta distruzione della cosa propria e mutilazione fraudolenta della propria persona. Chiunque, al fine di conseguire per sé o per altri il prezzo di un'assicurazione contro infortuni, distrugge, disperde, deteriora od occulta cose di sua proprietà è punito. Alla stessa pena soggiace chi, al fine predetto, cagiona a sé stesso una

lesione personale, o aggrava le conseguenze della lesione personale prodotta dall'infortunio.

Appaiono rilevanti anche alcuni articoli del codice civile che disciplinano la materia. Di seguito si espongono gli articoli di particolare interesse per declinare il concetto di frode e comprenderne pienamente le caratteristiche:

- Art. 2041. Azione generale di arricchimento. Chi, senza giusta causa, si è arricchito ai danni di un'altra persona è tenuto, nei limiti dell'arricchimento, a indennizzare quest'ultima della corrispettiva diminuzione patrimoniale. Qualora l'arricchimento abbia per oggetto una cosa determinata, colui che l'ha ricevuta è tenuto a restituirla in natura, se sussiste ancora al tempo della domanda.
- Art. 2043. Risarcimento per fatto illecito. Qualunque fatto doloso o colposo, che cagiona un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno.

Si vede quindi come il legislatore abbia inquadrato la frode in fattispecie di reato specifiche, attribuendo, tuttavia, a queste norme un'efficacia ridotta laddove la vittima, che non sia ente pubblico o non ricada nei casi denunciati d'ufficio, non proceda con regolare querela verso il frodatore.

Al di fuori degli enunciati articoli, in Italia, come del resto in Europa, non è ad oggi attivo uno specifico impianto normativo a eccezione della fattispecie dei reati informatici (Convenzione di Budapest) e nelle esperienze anglosassoni con riferimento al *Fraud Act* emanato nel Regno Unito nel 2006 [110].

1.3 La Convenzione Di Budapest

La Convenzione di Budapest è il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche, e tratta in particolare le violazioni dei diritti d'autore, la frode informatica, la pornografia infantile e le violazioni della sicurezza della rete. Contiene inoltre una serie di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati. [62]

Il suo obiettivo principale, enunciato nel preambolo, è perseguire una politica penale comune per la protezione della società contro la cybercriminalità, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale.

1.4 Il Fraud Act

Nel 2006 la Gran Bretagna ha varato una speciale normativa, il *Fraud Act*, volto alla definizione e punizione di questa tipologia di attività nelle sue varie forme e applicazioni [87]. Tra le previsioni della norma, è interessante notare come siano state individuate principalmente tre tipologie di frode:

- Frode per falsa rappresentazione: nei casi in cui una persona effettua una rappresentazione di un fatto o una legge, in maniera implicita o esplicita, che sa essere falsa o fuorviante;
- Frode per non rivelazione di informazioni: nel caso in cui una persona non riveli delle informazioni in violazione di un obbligo di legge;

- Frode per abuso di posizione: nei casi in cui un soggetto che riveste un ruolo professionale che comporti un dovere di tutela degli interessi finanziari di un altro soggetto abusi della propria posizione, inclusi i casi di omissione.

In tutti e tre i casi vi deve essere una condotta disonesta posta in essere da un soggetto nei confronti di una parte offesa, perpetrata con l'intento di trarre per sé o altri un ingiusto guadagno, così facendo cagionando una perdita alla parte offesa.

1.5 Le Esperienze Oltre Oceano

Altri ordinamenti, a esempio quello statunitense, prevedono una definizione della frode maggiormente flessibile e omnicomprensiva. Nel predetto ordinamento, infatti, il crimine di frode è costituito, così come stabilito dalla Corte Suprema della Carolina del Sud nel 2009 [61], da nove elementi:

- la rappresentazione di un fatto esistente;
- la sua falsità;
- la sua materialità;
- la conoscenza, da parte dell'attore, della falsità del fatto;
- l'intento dell'attore di incidere sulla vittima;
- l'ignoranza da parte della vittima della falsità del fatto;
- la convinzione della vittima della buona fede e della veridicità del fatto portato dall'attore;
- il diritto della vittima di basarsi sul fatto riportato dal soggetto;
- il danno che la vittima ha in conseguenza della frode.

1.6 Natura Ed Elementi Della Frode

Una frode tipica presenta una serie di elementi e caratteristiche distinte. In primis, l'autore della frode deve aver acquisito la fiducia della persona o della società vittima, che rende possibile commettere e nascondere la frode [38]. Infatti, quando sussiste una compromissione del rapporto di fiducia, si parla del c.d. "furto di fiducia". Questo, in fondo, è ciò che caratterizza la frode rispetto ad altri reati, al di là delle definizioni che i diversi ordinamenti ne danno. Non è sempre facile individuare questo aspetto proprio perché individuare il momento esatto in cui la fiducia viene richiesta e concessa risulta complicato. Il momento in cui il rapporto di fiducia viene compromesso viene individuato non tanto quando i soldi vengono sottratti dai conti, bensì allorquando il correntista, fino a quel momento confidente nella correttezza della propria banca e nella sua capacità di svolgere il proprio lavoro secondo le aspettative e le promesse, scopre che la propria fiducia è stata mal riposta. Furto, violenza, corruzione e altri comportamenti illeciti possono essere di volta in volta presupposto o conseguenza del "furto di fiducia", ma non sono l'essenza caratteristica della frode che rimane incentrata sulla fiducia. Contrariamente alla maggior parte degli altri crimini, colui che commette la frode usa l'inganno o l'astuzia piuttosto che la forza. Invece di usare una pistola, un coltello o una forza fisica per commettere un crimine, i responsabili usano solitamente informazioni false o fuorvianti, convincendo qualcuno a dare loro denaro o beni per poi nascondere le loro tracce. La maggior parte delle frodi, una volta iniziate, vengono raramente risolte volontariamente dagli autori, in quanto la loro avidità è tale che continuano a sfruttare l'opportunità di ottenere quanto maturato, cercando in alcune occasioni di aumentarlo ed estenderlo [52]. Infatti, una volta iniziato a commettere una

frode, è molto difficile per loro fermarsi. I seguenti fattori sono i motivi per cui gli autori continuano a perpetrare l'atto:

- Solitamente iniziano a dipendere dal beneficio ottenuto illecitamente e non possono permettersi di smettere;
- Di fronte alla prospettiva di avere denaro aggiuntivo a disposizione, molti passano ad uno stile di vita più elevato che richiede quantità di denaro ancora maggiori;
- La maggior parte degli autori prende tutti i soldi che lo schema o metodo messo in atto permette loro;
- Alcune frodi si autoalimentano. Se gli autori si fermassero, la loro azione sarebbe scoperta, e verrebbero quindi catturati.
- Gli autori di frodi raramente salvano o investono ciò che sottraggono ma, al contrario, lo spendono.
- Se gli autori non vengono catturati poco dopo l'inizio, in genere diventano più fiduciosi rispetto allo schema da loro attuato. Molti diventano avidi ed acquisiscono quantità sempre maggiori di denaro ad intervalli più frequenti. Ovviamente le quantità in questione sono più inclini ad essere esaminate, ed uno schema che potrebbe non essere stato rilevato per un certo tempo viene scoperto perché gli importi acquisiti aumentano a livelli inaccettabili.
- Col passare del tempo, molti autori diventano negligenti o troppo sicuri di sé e non prendono cautele sufficienti per nascondere efficacemente la loro frode. Tali autori di solito commettono nel tempo un errore che porta alla luce il metodo usato per perpetrare la frode.

Gli elementi costitutivi della frode sono quindi:

- l'attore: il soggetto attivo che compie l'atto fraudolento;

- la vittima: il soggetto passivo che subisce la frode;
- l'inganno: il comportamento, azione o atto teso a raggirare la vittima della frode;
- l'ingiusto guadagno per l'attore e il danno per colui che subisce l'atto.

La frode si sviluppa quindi sulla base dell'interazione tra attore e vittima, caratterizzata dall'inganno da parte dell'attore nei confronti della vittima. Lo schema dell'attività fraudolenta può essere efficacemente ripreso dalla figura seguente:

Figura 1: schema basico di un'attività fraudolenta

1.7 Classificazione Delle Frodi

Le frodi a danno delle aziende

La frode risulta particolarmente pericolosa per le realtà aziendali, principalmente per le conseguenze economiche che ne derivano ed in seconda istanza per i danni reputazionali e di immagine. Per frode aziendale s'intende "qualsiasi atto illegale, commesso da persone interne o esterne all'azienda, caratterizzato da condotte quali il raggiro, l'artificio, l'occultamento, l'abuso di fiducia" [118]. Le finalità sono di ottenere illecitamente denaro, beni o servizi, di evitare un pagamento o la perdita di servizi, oppure procurarsi ingiusti vantaggi personali o aziendali". All'interno del grande insieme delle frodi societarie perciò è possibile comprendere una serie molto variegata di reati, diversi per natura e complessità, tra cui si possono citare la corruzione, la cattiva gestione caratterizzata da espedienti premeditati, l'assunzione non autorizzata di rischi, le manipolazioni, i furti ecc. È possibile però classificare le frodi societarie in due macro categorie: le frodi commesse contro la società e quelle commesse a vantaggio della società. Nella prima ipotesi la società ricopre il ruolo di vittima mentre nella seconda essa stessa è la beneficiaria dell'atto fraudolento. Mentre non risulta troppo difficile immaginare casi relativi alla prima tipologia, potrebbe essere più difficile immaginare situazioni in cui la frode venga perpetrata a solo vantaggio della società. A titolo esemplificativo si possono menzionare alcuni esempi, quali: l'evasione fiscale, la violazione di norme ambientali, la falsa pubblicità e propaganda del prodotto o del servizio offerto e la determinazione di prezzi fittizi). Le frodi a vantaggio della società sono solitamente commesse da membri del management che il più delle volte mirano ad ottenere anche un vantaggio personale dalla situazione in atto, tentando ad esempio di incrementare il loro

profitto manipolando il livello di fatturato, piuttosto che cercando di ridurre il valore dei costi. Tra le due categorie, quella delle frodi attuate a svantaggio della società è però la più ampia e variegata, in quanto esse possono includere diversi soggetti (membri del top management, impiegati, fornitori, clienti, terzi esterni alla società), e possono avere differenti obiettivi e molteplici modalità di attuazione. Un'altra importante distinzione all'interno delle frodi societarie riguarda le frodi interne, commesse direttamente o indirettamente da soggetti che già operano all'interno dello staff aziendale, e le frodi esterne, messe in atto da individui non operanti all'interno della società ma che comunque hanno con essa un certo tipo di rapporto, che può essere di fornitura, di clientela, di consulenza, di agenzia ecc. Nell'ambito delle frodi societarie di tipo interno si è soliti poi distinguere il *white collar crime* in senso stretto dal *corporate fraud* [124]. Con il primo si indicano le frodi compiute dai vertici aziendali, nella maggior parte dei casi proprio dal Consiglio di Amministrazione. Nel corporate fraud, invece, il comportamento fraudolento si muove internamente all'impresa nel suo sistema di controllo, sfruttandone le imperfezioni. Tale tipologia di frode risulta particolarmente pericolosa proprio perché insita nei meccanismi e nelle procedure aziendali e perché, se scoperta, difficilmente procederà in processi pubblici nel tentativo di tutelare l'immagine esterna della società. La frode, di qualunque tipo essa sia, può lasciare tracce nel sistema delle rilevazioni d'azienda oppure può svilupparsi in modo da non interessare assolutamente il sistema contabile. L'atto fraudolento si può così ulteriormente qualificare come contabile (altrimenti detto anche *on the book*) o extracontabile (noto anche come *off the book*). Le frodi che rientrano in quest'ultima categoria sono indubbiamente più complesse da individuare, tenendo conto del fatto che né le procedure di auditing né il controllo strettamente contabile sono in grado di identificarle, essendo

necessaria a tal fine un'analisi dei fatti sottostanti e non riportati in contabilità [31].

La seguente tabella riporta schematicamente le classificazioni delle frodi:

	CATEGORIE	
Tipologie di **FRODI**	a favore della società	contro la società
	interne *corporate fraud* / *white collar crime*	esterne
	contabili	extracontabili

Figura 2: classificazione delle frodi aziendali

1.8 Aspetti Psicologici Della Frode

Non è semplice tracciare un profilo del frodatore, perché così facendo si rischia di generalizzare un fenomeno che, correttamente, va sempre visto ed analizzato nel suo ambito particolare. È in primis l'ambiente circostante a colui che commette l'atto che permette, ad una persona fino a quel momento "normale", di far emergere in presenza dell'occasione giusta, le sue potenzialità e motivazioni di autore, fornendo indirettamente gli strumenti adatti a perpetrare la frode. Esistono una serie di tendenze o condizioni nelle società che contribuiscono direttamente o indirettamente alla frode. Queste leve sociali sono influenzate dalle condizioni politiche ed economiche e dalle aspettative sociali [41]. Di seguito le più rilevanti:

- Ostracismo nei confronti del *whistleblower*;
- Mancata segnalazione di frode;
- Volontà delle imprese di perseguire gli autori di frodi;
- Incapacità delle forze dell'ordine di perseguire penalmente gli autori di frodi;

Ostracismo nei confronti del *Whistleblower*

L'ostracismo nei confronti dei cosiddetti *whistleblower*, ovvero degli informatori, è un fattore sociale che contribuisce indirettamente alla commissione di atti fraudolenti. Molto numerosi sono i casi in cui la persona che ha "fischiato" una frode ha sofferto le conseguenze dell'azione messa in atto. Quando le altre persone notano le conseguenze che possono subire coloro che denunciano un atto fraudolento, sono riluttanti nel farsi avanti, pensando che non vogliono che accada loro quello che è successo a colui che ha denunciato l'accaduto.

Mancata segnalazione di frode

Molte aziende sono riluttanti a denunciare frodi rilevate, perché questa azione può causare un danno reputazionale e di immagine. In alcuni casi, la società perde più dal cattivo ritorno di immagine che dalla frode stessa. Inoltre denunciando il danno subito, può rivelare anche la vulnerabilità di una parte dei sistemi aziendali impattati, che potrebbe conseguenzialmente attirare l'attenzione di potenziali criminali, rendendo l'azienda ancora più esposta ad atti fraudolenti.

Volontà delle imprese di perseguire gli autori di frodi

Molte aziende non perseguono i dipendenti che commettono una frode. Alcune delle motivazioni sono le seguenti:

- Le azioni legali sono costose da perseguire;
- La società non vuole impelagarsi in una causa, ad esempio per diffamazione, attuata da parte degli attori in gioco.

Incapacità dei funzionari delle forze dell'ordine di perseguire penalmente gli autori di frodi

Ci sono una serie di ragioni per cui le forze dell'ordine e i tribunali non perseguono gli autori di atti fraudolenti:

- Molti funzionari delle forze dell'ordine, avvocati e giudici, non dispongono delle competenze necessarie per indagare, perseguire e valutare alcuni tipi di frode, come ad esempio la frode informatica;
- Quando vengono perseguiti casi di frode e si ottiene una condanna, le sentenze ricevute sono spesso molto leggere rispetto ai danni perpetrati;

- Le forze dell'ordine e i tribunali tendenzialmente sono più impegnati con crimini di natura violenta che in casi di reati di natura fraudolenta in cui non vi sono danni fisici;
- I reati fraudolenti richiedono tempistiche lunghe per effettuare le dovute indagini;
- Gli atti fraudolenti sono difficili da dimostrare e non è semplice ottenere prove ammissibili;

Di conseguenza è più difficile perseguire con successo casi di atti fraudolenti per ottenere condanne di quanto non lo sia per molti altri tipi di crimini.

Scientificamente esistono strumenti in grado di supportare l'analisi del profilo dei criminali [70], chiamata appunto dagli addetti ai lavori "*Criminal Profiling*", riferendosi all'identificazione degli autori di reati, reali o potenziali, sulla base del comportamento o di altri attributi che essi hanno, quali:

- età;
- grado d'istruzione;
- reddito;
- sesso;
- eventuali precedenti condanne ed altre caratteristiche comuni.

Inoltre, provando poi a mettere a fattor comune quanto elaborato in letteratura dagli studiosi di criminologia, quali Donald Cressey ed Edwin Sutherland [6], ci si accorge di alcune ricorrenze:

- Non vi è alcun crimine ideale o prevalente;
- I reati fraudolenti sono spesso più facili da individuare a posteriori, mentre sono assai più difficili da prevedere;
- I reati fraudolenti implicano un'interazione tra opportunità, razionalizzazione ed incentivazione.

1.9 Il Triangolo Della Frode

Le frodi vengono attuate a livelli diversi in un'ampia gamma di situazioni. Ciascuno di coloro che commettono illeciti ha motivazioni proprie e opportunità specifiche. Tuttavia è possibile individuare alcuni elementi tipici che caratterizzano tutti i comportamenti fraudolenti. Queste variabili sono state evidenziate dal ricercatore americano Donald R. Cressey che, a seguito di un'indagine empirica sulle frodi svolta negli anni Cinquanta, ha elaborato una teoria che, ad oggi, è la più adatta a rispondere alla domanda: "perché si commettono delle frodi?".

Tale teoria, meglio nota come "*The fraud triangle*" [52], spiega i presupposti per il verificarsi di una frode considerando tre elementi caratterizzanti:

- la *pressione* a compiere reati fraudolenti, generata dalla percezione di una molteplicità di bisogni;
- l'*opportunità* di compiere la frode e di celare il crimine evitando la sanzione (mancanza o fallacità dei sistemi di controllo, meccanismi aziendali che permettono la commissione della frode);
- La *razionalizzazione* della frode, in altri termini la giustificazione che l'attore si dà per la commissione dell'evento fraudolento ("in fondo non danneggio nessuno", "l'azienda se lo merita", ecc.);

La teoria è stata sviluppata con un ardito ma efficace riferimento al triangolo del fuoco, che rappresenta, invece, i presupposti allo scoppio di un incendio e l'utilizzo di questo schema per identificare la tecnica più efficace per il suo spegnimento. Nella teoria del triangolo del fuoco si fa riferimento ai tre elementi principali, ossia l'ossigeno, l'elemento combustibile e la fonte di calore: per spegnere un incendio è sufficiente agire su uno solo di questi tre elementi [112].

Analogamente, per agire efficacemente in chiave di prevenzione delle frodi, sarebbe sufficiente intervenire su almeno uno dei tre elementi tra motivazione, opportunità e incentivo.

La decisione di commettere una frode è determinata dall'interazione di tutte e tre le leve. Si verificano frodi quando le persone subiscono pressioni elevate, sussiste un'opportunità per commettere la frode e convertire l'azione in guadagno personale, ed è presente nell'autore la capacità di razionalizzare l'atto, non intaccando la sua integrità personale. Di conseguenza, è meno probabile che un evento fraudolento si verifichi quando si è in presenza di un ambiente con pressione non alta, dove ci sono poche opportunità e delle caratteristiche personali che indicano onestà ed integrità.

Se gli individui hanno una forte caratteristica di onestà, possono teoricamente resistere al peso cumulativo delle altre due variabili. Si narra che Abraham Lincoln una volta cacciò un uomo dal suo ufficio. Quando chiesero spiegazione in merito alla motivazione, Lincoln dichiarò di aver rifiutato una tangente sostanziosa ed aggiunse: "Ogni uomo ha il suo prezzo e quella persona si stava avvicinando al mio." [100].

Quindi le condizioni per una possibile frode diventano più allettanti in presenza di individui con minore integrità personale, posti in situazioni dove esistono pressioni crescenti e con maggiori opportunità di commettere l'atto. Gli individui che si trovano in circostanze difficili possono pensare che l'unica via d'uscita sia scegliere tra la loro integrità ed uno o più dei seguenti fattori:

- i loro affari;
- le loro posizioni nella comunità;
- la loro reputazione o prestigio.

Quando scelgono di sacrificare la loro integrità, la frode è spesso il risultato. Nella vita di un possibile autore, le tre variabili che contribuiscono alla creazione di

frodi crescono fino a quando non sono sufficientemente consistenti da sfociare quindi in un atto fraudolento.

1.10 Lo Sviluppo Di Un Sistema Antifrode

A livello internazionale ci sono diversi studi da cui trarre interessanti informazioni sulle diverse tipologie di frode e sulle dimensioni del fenomeno su scala globale. Particolarmente interessante è il rapporto *Global Fraud Report*, elaborato da Kroll Advisory Solutions , con il supporto dell'Economist Intelligence Unit, inerente all'impatto delle frodi sulle aziende [69]. Lo stesso, condotto su 839 imprese di diverse regioni mondiali, ha rilevato come il 61% di queste abbia registrato eventi di frode, di cui i due terzi (67%) consistenti in frodi interne. Inoltre, il rapporto ha evidenziato come, in media, il costo degli eventi di frode sia pari a 0,9% dei ricavi delle imprese. I principali eventi fraudolenti registrati dalle imprese intervistate sono il furto di asset fisici e di informazioni, il conflitto di interessi del management, le frodi provenienti da venditori, fornitori o dal procurement, le frodi finanziarie interne, la corruzione. Forte elemento di preoccupazione risultano le frodi informatiche, anche nella forma di cyber attacchi. Un'azienda, quindi, non può fare a meno di implementare un programma antifrode, nella forma di policy e procedure. Gli elementi fondamentali da implementare in azienda, sono:

- assessment dei fattori che determinano la frode (analisi e valutazione dei rischi di frode per l'azienda);
- definizione di un sistema di controllo interno (audit, organismo di vigilanza, ecc.);

- creazione di un ambiente di controllo e commitment da parte del top management;
- adozione di un codice etico per favorire l'instaurarsi di una cultura aziendale contro i comportamenti fraudolenti;
- adozione di hotline e sistemi di whistleblowing che permettono di denunciare in modo anonimo i fenomeni di frode;
- gestione delle assunzioni e incentivazione del personale. Tale processo deve prevedere la verifica del background di un candidato in fase di assunzione e l'adozione di una politica di premi e promozioni per il personale più fedele;
- promozione di processi per l'investigazione delle frodi;
- proceduralizzazione delle attività investigative;
- certezza della sanzione;
- miglioramento continuo;
- monitoraggio continuo dei rischi di frode.

Nel prosieguo si andrà ad analizzare l'articolazione di un sistema di gestione del rischio di frode, sulla base delle best practices a livello internazionale. Si vedrà come tutti questi elementi indicati vengono inclusi nelle varie parti fondanti un programma di fraud governance a livello aziendale. In conclusione, quindi, la frode rappresenta una fonte di rischio molto rilevante per le aziende. Si tratta, infatti, di un rischio operativo che investe molteplici aspetti della realtà aziendale. È stato ampiamente dimostrato che le aziende che intraprendono percorsi proattivi nell'implementazione di meccanismi volti a prevenire il verificarsi di comportamenti fraudolenti, ne registrano un minor numero di casi e, ricevendo minori danni, conseguentemente risultano maggiormente tutelate. In questo senso, bisogna sempre ricordare che la frode rappresenta un rischio: in quanto

tale, deve essere gestito attraverso opportuni modelli di risk management. La sola adozione di un modello di gestione, però, non è sufficiente. La definizione e introduzione di un programma di fraud governance permette di mitigare il livello di rischio, grazie all'effetto di deterrenza, ma non assicura di per sé una soluzione del problema [103]. Un serio e organico programma di contrasto ai fenomeni illeciti, per essere davvero efficace, deve essere adottato in modo esteso dalla struttura organizzativa e deve essere costantemente aggiornato per riflettere le continue evoluzioni degli scenari esterni e interni all'impresa. In questo senso, si può affermare che il sistema deve essere adottato ed efficacemente implementato.

Come visto precedentemente inoltre, la frode rappresenta oltre che un rischio per l'azienda, anche un reato ai sensi della legislazione italiana. In questo senso, un programma di fraud governance aziendale, non solo rappresenterebbe uno strumento per la protezione dei beni, materiali e immateriali, dell'impresa, ma altresì un meccanismo esimente della responsabilità dell'azienda nel caso in cui risorse interne (in posizione apicale o subordinata) effettuino un reato di frode a vantaggio della stessa (art. 640 c.p. truffa, art. 640-bis truffa aggravata per erogazioni pubbliche, art. 640-ter frode informatica, art. 642 frode assicurativa). Di seguito saranno sviluppate quindi le considerazioni fondamentali per l'implementazione e la realizzazione di un programma di fraud governance efficace all'interno dell'azienda.

1.11 La Realizzazione Di Un Programma Antifrode

A seguito degli enormi scandali accaduti a grandi aziende americane (si pensi ai casi Worldcom e Enron) negli USA è stata pubblicata la *Sarbanes-Oxley Act* del 2002, che, oltre a rappresentare il punto di riferimento per l'introduzione, a livello internazionale, di regolamentazioni sulla governance aziendale, (il SOX delinea alcuni fondamentali principi di gestione, di accounting e di corporate governance), è il punto di partenza su cui sviluppare programmi di fraud governance aziendale. Lo standard di riferimento a livello internazionale per l'implementazione di un sistema di gestione del rischio di frode aziendale è la guida *Managing the Business Risk of Fraud: A Practical Guide*, sviluppata da un gruppo di lavoro internazionale e sponsorizzata dall'*Institute of Internal Auditors*, dal *The American Institute of Certified Public Accountants* (AICPA) e dall'*Association of Certified Fraud Examiners* (ACFE) [82] [112].

Questa Guida inoltre è sostenuta da diverse organizzazioni, tra le quali:

- l'Institute of Management Accountant;
- l'Association of Chartered Certified Accountants;
- la Society of Corporate Compliance and Ethics;
- la Chartered Accountants of Canada.

Il documento, quindi, risulta particolarmente utile per accompagnare le aziende nel delineare gli elementi principali costitutivi di un efficace sistema di gestione del rischio di frode, in quanto sviluppata sulle best practices organizzative e gestionali, sul framework CoSO, e su varie normative (per lo più statunitensi). La Guida descrive un modello di gestione basato sui seguenti cinque principi [27]:

1. Un programma di *fraud risk governance* deve essere parte attiva della struttura di governance di una organizzazione. Il programma deve prevedere più policy per garantire il coinvolgimento del top e del senior management;

2. L'esposizione dell'organizzazione al rischio di frode dovrebbe essere periodicamente valutata al fine di identificare gli schemi e gli eventi che necessitano di essere mitigati;

3. Dovrebbero essere sviluppate e implementate tecniche di prevenzione di potenziali eventi di frode, per mitigare i possibili impatti sull'organizzazione (*fraud prevention*);

4. Dovrebbero essere sviluppate e implementate tecniche di rilevazione al fine di scoprire gli eventi di frode (*fraud detection*), quando le misure di prevenzione o di mitigazione del rischio falliscono;

5. Ogni organizzazione deve implementare un sistema di reporting e di flussi comunicativi che fungano da input alle attività di investigazione e che aiutino ad attivare azioni correttive.

1.12 La Governance Del Rischio Di Frode

Il primo aspetto fondamentale è lo sviluppo di un impianto organizzativo atto a gestire, in maniera diretta, il rischio di frode. Il sistema di gestione può essere sviluppato su una serie di componenti alquanto articolati, comuni ai sistemi di gestione improntati alla qualità. Le componenti fondamentali del sistema, sono [18]:

- Impegno del CdA e del top management: all'interno del CdA andrebbe definito un sistema di attribuzioni di responsabilità sulle attività di fraud governance. Inoltre, il management, deve farsi parte attiva nel comunicare e rendere noto il suo impegno nella gestione efficace del rischio di frode. Uno dei metodi più utilizzati è lo sviluppo di policy antifrode e codici etici o di condotta, rivolti al personale interno, ai clienti, ai fornitori e a tutte le terze parti che a diverso titolo si relazionano con l'azienda. Il CdA deve assumersi la responsabilità del monitoraggio dell'efficacia dei processi antifrode e garantire adeguate risorse a quest'area;
- Concretezza: il programma di fraud governance deve prevedere un insieme di documenti scritti, dove obiettivi, attribuzioni di responsabilità, piano di comunicazione, incentivazione, azioni disciplinari e legali, sono definiti in modo chiaro e portati a conoscenza del personale a tutti livelli attraverso specifiche e periodiche attività di formazione e assessment;
- Consapevolezza: coerentemente con la definizione degli obiettivi aziendali in termini di politica di gestione dei rischi, il programma deve prevedere un'attività costante di monitoraggio delle tipologie di rischio, probabilità e rilevanza, efficacia delle misure adottate per la loro prevenzione e mitigazione dei livelli di rischio;

- Informazione/accettazione comportamento antifrode: va definito un piano di formazione e informazione attraverso il quale il management, i dipendenti, e in genere tutte le risorse coinvolte nell'organizzazione aziendale prendono ufficialmente visione del documento che delinea il codice di comportamento accettandone i contenuti;
- Conflitto d'interessi: dovrebbe essere sviluppato un processo che faccia emergere e consenta di prevenire e gestire possibili conflitti di interesse di dipendenti, dirigenti e agenti dell'organizzazione;
- Valutazione del rischio di frode: dovrebbe essere sviluppato un processo continuo di analisi e valutazione del rischio di frode che identifichi i possibili eventi e schemi fraudolenti di interesse per l'organizzazione, con la relativa misura sulle probabilità di accadimento e di impatto (economico e reputazionale in primis) sull'azienda;
- Procedure di reporting e whistleblowing: si dovrebbero definire piani di comunicazione e procedure che permettano di riportare alle funzioni competenti eventi fraudolenti e comportamenti sospetti;
- Processo di investigazione: le organizzazioni dovrebbero sviluppare processi investigativi opportunamente proceduralizzati, che riescano a intervenire a seguito del sospetto e della segnalazione di un fatto considerato fraudolento;
- Azioni correttive: dovrebbero essere sviluppate, anche in funzione di deterrenza, delle procedure di azione correttiva che sanzionino e prevedano conseguenze per l'attore che effettua una frode (sanzioni amministrative, risoluzione di contratto, denuncia,ecc.);
- Monitoraggio continuo: Il processo nel suo complesso e nei singoli sotto-processi dovrebbe essere documentato e continuamente monitorato, al fine di poter effettuare la valutazione e il miglioramento del sistema;

- Valutazione e miglioramenti del processo antifrode: ispirandosi agli standard di qualità, il processo complessivo di fraud management dovrebbe essere valutato in termini di efficienza ed eventualmente migliorato nel suo complesso;
- Analisi del contesto normativo: tutte le attività ricomprese in un programma di fraud governance devono essere sviluppate in coerenza e nel rispetto delle vigenti normative, nazionali e internazionali, con particolare riferimento a normative giuslavoristiche, Privacy, norme internazionali sull'Anti Corruption e Anti Bribery, norme sul rispetto dei diritti umani, etc.

1.13 La Valutazione Del Rischio Di Frode

Un processo chiave di un efficace programma di fraud governance aziendale è il processo di valutazione del rischio di frode, che può essere assimilato ai principi generali del risk management (fraud risk assessment) per la valutazione di altre tipologie rischi. Lo svolgimento di questa attività può essere condotta da diverse funzioni aziendali, o essere parte di un più ampio processo di enterprise risk management, se presente nell'organizzazione [38].

Questo processo diventa più efficace quanto più ampio è il coinvolgimento delle diverse funzioni aziendali, in un fraud risk assessment team che sviluppa il processo di valutazione del rischio di frode. In relazione alla natura della frode, il team sarà quindi composto da diverse funzioni aziendali, coinvolte nel processo di risk management, al fine di disporre di risorse con le necessarie abilità, competenze e conoscenze.

Si potrà quindi avere un gruppo di lavoro con figure professionali di [32]:

- contabilità e finanza;
- unità di business;
- risk management;
- security;
- legale;
- internal audit;
- it;
- hr;
- sales;
- consulenti e fraud specialist interni e esterni.

Il processo si articola nelle fasi di identificazione dei rischi, valutazione e predisposizione delle azioni correttive [47].

- Identificazione dei rischi di frode: si identificano le fattispecie di frode rilevanti che possono interessare l'organizzazione, identificando, al contempo, gli schemi fraudolenti e i possibili scenari, gli incentivi, le motivazioni e le opportunità di commettere una frode nell'organizzazione;
- Valutazione del rischio di frode: si valutano i rischi di frode identificati, in particolare con riguardo alla probabilità di accadimento e ai possibili impatti, valutandone, quindi, la rilevanza per l'organizzazione;
- Predisposizione delle azioni di risposta ai rischi di frode considerati rilevanti e probabili: si identificano e pianificano le possibili azioni di risposta, in chiave costi-benefici, da intraprendere per mitigare il rischio di frode.

Un modo per sviluppare un programma di prevenzione delle frodi è seguire la strategia di valutazione del rischio mostrata di seguito [12]:

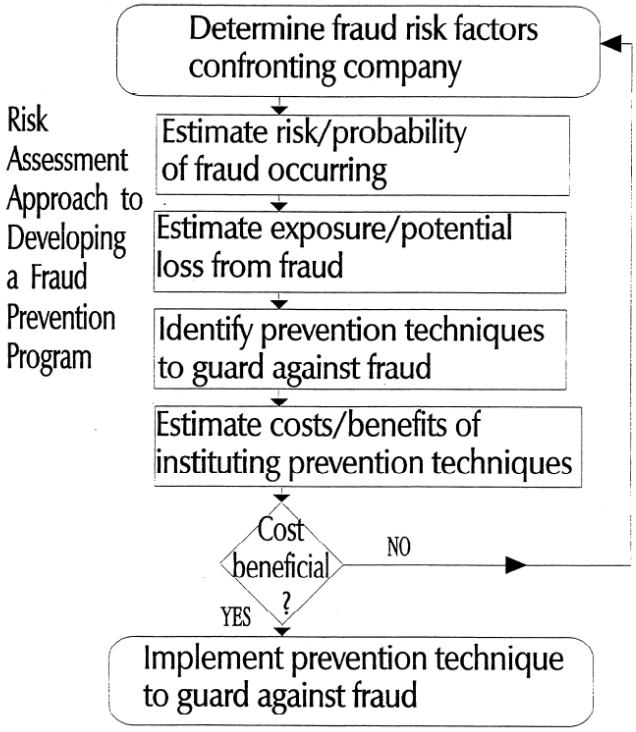


Figura 3: schema basico di un'attività fraudolenta

Una società deve identificare i potenziali fattori di rischio frode, come un sistema di controlli interni poco efficace ed efficiente, pressioni sul posto di lavoro causate da ridimensionamenti o, ad esempio, un processo di assunzione che non vaglia adeguatamente i potenziali dipendenti. La probabilità che si verifichi effettivamente una frode viene definita rischio di frode [9]. Alcuni fattori comportano un rischio maggiore perché è più alta la probabilità che si verifichino. L'importo monetario che potrebbe essere perso se un particolare fattore di rischio ha portato a una frode è indicato come esposizione alla frode, che può variare da molto piccola a molto grande, a seconda della natura della frode ed al tempo che persiste.

Il rischio di frode e l'esposizione devono essere considerati congiuntamente. Il rischio di frode presente nel top management di una azienda potrebbe ad esempio essere basso, ma l'esposizione può essere enorme, costringendo un'azienda in situazioni critiche o addirittura di fallimento. D'altra parte, il rischio di una frode ai livelli operativi potrebbe essere molto maggiore, ma con una esposizione minore [3].

1.14 Fraud Prevention E Fraud Detection

Al fine di minimizzare la possibilità di accadimento di eventi fraudolenti si devono sviluppare ed implementare dei processi e delle procedure di prevenzione delle frodi (fraud prevention) e di rilevazione degli eventi sospetti o accaduti (fraud detection). La fraud prevention riguarda le procedure, le policies, la formazione e la comunicazione, mentre la fraud detection invece riguarda sistemi e metodologie di rilevamento di comportamenti sospetti o atti fraudolenti una volta che sono stati compiuti [102]. Naturalmente, l'implementazione di un sistema efficiente di fraud detection agirà anche come deterrente, operando quindi da fattore di prevenzione.

Tecniche di prevenzione delle frodi

È necessario identificare una o più tecniche per proteggere l'azienda da ciascun fattore di rischio. Nel valutare i benefici di tecniche specifiche, la direzione dovrebbe considerare la loro efficacia ed il loro tempismo.

A parità di fattori, le tecniche di prevenzione sono superiori alle tecniche di rilevazione. Una tecnica di rilevazione identifica un problema che potrebbe aver generato già una certa perdita monetaria, rispetto alla quale potrebbero essere necessari costi aggiuntivi per correggere il problema. Se le tecniche di prevenzione falliscono, tuttavia, e si verifica una frode, le tecniche di rilevamento sono essenziali per scoprire una frode. Le tecniche di prevenzione e rilevazione si completano quindi a vicenda, ed un buon sistema antifrode deve impiegarle entrambi. Tutto ciò deve avere come premessa che nessun programma di prevenzione delle frodi potrà fornire ad un'organizzazione una protezione infallibile contro tutte le possibili frodi, perché il suo costo, ammesso che sia

possibile implementarlo, sarebbe proibitivo. Le tecniche di prevenzione delle frodi possono influire negativamente sull'efficienza operativa, rendendola minore, limitando la capacità di un'azienda di soddisfare le sue esigenze. Pertanto, l'obiettivo nella progettazione di un programma di prevenzione delle frodi è fornire una "ragionevole garanzia" che non si verifichi una frode. Ciò significa che il vantaggio di una tecnica di prevenzione delle frodi non deve superare il suo costo [114].

I costi delle tecniche di prevenzione sono più facili da misurare rispetto ai loro benefici. L'elemento di costo principale include il tempo per eseguire le procedure di prevenzione, i costi di assunzioni aggiuntive di dipendenti per raggiungere un'efficace segregation of duties ed i costi di implementazione di un sistema informatico, qualora sia necessario.

I benefici delle tecniche di prevenzione derivano dalla riduzione delle perdite per frode. Un modo per calcolare i benefici delle tecniche di prevenzione delle frodi è la perdita prevista di frode, il prodotto matematico tra il rischio della frode e l'esposizione alla frode [29]:

Perdita di frode prevista (€) = Rischio di frode% x Esposizione di frode (€)

Il vantaggio di una tecnica di prevenzione è la differenza tra la perdita attesa con una tecnica di prevenzione e la perdita attesa senza di essa. Una volta che i benefici ed i costi di un particolare controllo sono stati stimati, deve essere determinato se il controllo è conveniente. Per fare ciò, il costo della tecnica di prevenzione viene sottratta dal beneficio. Nel valutare i costi e i benefici delle tecniche di prevenzione, bisogna considerare fattori ulteriori oltre quelli che si riflettono nel semplice calcolo del beneficio atteso [16]. Ad esempio, un'esposizione fraudolenta può essere così grande da minacciare l'esistenza

stessa dell'organizzazione. In tali casi, la direzione dovrebbe essere disposta ad attuare le tecniche di prevenzione anche ad un costo superiore alla semplice riduzione della perdita attesa, che può essere considerato un premio assicurativo per proteggere l'organizzazione da perdite catastrofiche.

1.15 Fraud Prevention: Analisi Per Fattori di Rischio

Considerando il modello del fraud triangle, precedentemente esposto, che circostanzia gli atti fraudolenti secondo le interazioni dei seguenti fattori [14]:

- pressione/incentivo;
- opportunità;
- atteggiamento/razionalizzazione,

verrà condotta in questo paragrafo un'analisi degli elementi dei possibili fattori di rischio.

Pressione e razionalizzazione

La lista delle pressioni che i dipendenti di un'azienda possono subire, sia per questioni legate direttamente all'ambiente aziendale che a quello della vita quotidiana, è molto ampia [23] [39]. Di seguito saranno illustrate e discusse alcune delle pressioni più comuni.

Pressioni Finanziarie relative ai dipendenti

Retribuzione inadeguata

Una pressione finanziaria è la retribuzione inadeguata. Alcuni datori di lavoro si aspettano che un dipendente mantenga un determinato stile di vita per mostrare una certa immagine di sé, o impegnarsi in determinate attività per attrarre nuovi affari, nonostante non vengano forniti compensi adeguati per consentire al dipendente di farlo.

Stile di vita

Molti autori di frodi sembrano essere attratti da quella che può essere definita una vita basata sul consumo. Sono individui sociali estroversi, amanti del divertimento che amano le emozioni che derivano dall'essere influenti, dallo status sociale e dalla spesa di ingenti somme di denaro. Sono spesso fantasiosi e più che pronti e disposti a correre grandi rischi per ottenere ciò che vogliono.

Debiti personali

Un'altra pressione finanziaria è la presenza di un debito personale che ammonta ad una quantità cospicua. Ciò può derivare da:

- La perdita di un'azienda o casa;
- Divorzio;
- Periodi prolungati di disoccupazione;
- Decisioni che non si rilevano essere corrette.

In sostanza, gli autori arrivano a compromettere la propria integrità personale per risolvere le pressioni di cui sopra.

Orgoglio e ambizione

L'orgoglio e l'ambizione possono portare alcune persone a commettere atti fraudolenti. Queste persone si sentono al di sopra delle regole in quanto migliori di altre persone e più meritevoli. Sono spesso insoddisfatti del lavoro e delle

entrate ordinarie. Il successo e l'ambizione possono diventare un'ossessione che può manifestarsi nello stile di vita condotto. Questo atteggiamento provoca nei trasgressori la volontà di ottenere ciò che vogliono con qualsiasi mezzo, rendendoli ciechi rispetto alle possibili conseguenze.

Necessità di Potere e Controllo

Per alcuni, la necessità di potere o controllo può superare la considerazione di ciò che è giusto o sbagliato. Ad esempio, qualora risulti essere bloccata la strada per raggiungere il potere o il prestigio, il denaro può rappresentare la via più semplice per affermarsi socialmente.

Frustrazione

Alcuni autori di atti fraudolenti non sono in grado di tollerare fallimenti, generando così in loro frustrazione. In tali personalità, il fallimento negli sforzi stimola una ricerca di una scorciatoia per il successo, compromettendo così la loro integrità e cercando di risolvere i loro problemi al più presto possibile con il minimo sforzo e costo, indipendentemente dall'impatto che questi possono avere sul business aziendale o altre persone.

Sfida intellettuale

Una scoperta comune, riguardante specialmente i criminali informatici, è che spesso coloro che commettono atti fraudolenti sono motivati da sfide intellettuali. Molti tecnici informatici sono insaziabilmente curiosi e ritengono sfidante capire come funzionano le cose. Un tecnico potrebbe facilmente ritrovarsi a pensare: "Io capirò come hanno reso sicuro questo sistema, infrangendo i criteri di sicurezza e dimostrando le mie superiori capacità

tecniche. Una volta tentato da questo tipo di gioco, possono risultare così coinvolti da perdere di vista le implicazioni morali delle loro azioni.

Risentimento

Il sentimento di risentimento può far sì che venga compromessa l'integrità personale. Questo può derivare da varie percezioni che i dipendenti hanno nei confronti del posto di lavoro, quali ad esempio:

- Sono trattati ingiustamente;
- Sono sottopagati e meritevoli di più denaro;
- I loro contributi alla società non sono né sufficientemente apprezzati né riconosciuti;
- Il loro lavoro non porta loro alcuna soddisfazione personale;
- Non possono mai raggiungere obiettivi non realistici che sono stati fissati per loro.

Pressioni finanziarie relative al Management

Le pressioni possono anche motivare un individuo a commettere frodi per conto di un'organizzazione anziché contro di esso. Di seguito vengono esposti alcuni dei principali fattori [74] [86].

Cicli economici, inflazione e recessione

Il ciclo economico e i conseguenti effetti dell'inflazione e della recessione sono elementi di rilievo. In tempi di recessione, i dirigenti che temono licenziamenti o ridimensionamenti possono ricorrere a espedienti finanziari per aumentare i profitti e proteggere il proprio posto di lavoro e quello dei lavoratori.

Fallimenti aziendali

Un'altra pressione aziendale è il fallimento. Sebbene questi aumentino in modo significativo nei tempi di recessione, esiste una relazione significativa tra fallimenti aziendali e frodi anche nei periodi migliori per le aziende.

Obiettivi non realistici

Per le aziende crescere e progredire è importante. Tuttavia, quando il management fissa obiettivi o aspettative per i propri dipendenti o unità operative non realistici, potrebbero far scattare motivazioni e comportamenti che portano maggiormente verso la commissione di atti fraudolenti piuttosto che verso il miglioramento delle prestazioni.

Esistono diverse altre importanti pressioni dell'azienda, alcune delle quali vengono di seguito elencate:

- Nuovi requisiti contabili o regolamentari, che potrebbero compromettere la situazione di stabilità finanziaria o la redditività dell'azienda;
- Un elevato grado di concorrenza o saturazione del mercato, accompagnato da margini in calo;
- Rapidi cambiamenti in un settore. Alcuni esempi sono:
    - Calo della domanda;
    - Elevata vulnerabilità alla tecnologia in rapida evoluzione;
    - Necessità di importanti spese di sviluppo per rimanere competitivi sul mercato, rendendo necessario un aumento di capitale significativo.

Pressioni derivanti dallo stile di vita

Un altro tipo di pressione è quello derivante dallo stile di vita, di cui di seguito vengono riportati a titolo esemplificativo alcuni fattori [104] [97].

Gioco d'azzardo

Chi è dipendente dal gioco d'azzardo farà di tutto per ottenere i soldi necessari a sostenere la propria dipendenza.

Dipendenza da droghe o alcol

La dipendenza da droghe o alcol è un motivatore molto potente, che porta a commettere atti che normalmente non sarebbero compiuti, tra cui commettere una frode.

Relazioni sessuali

Diverse persone sono state motivate a commettere una frode perché avevano bisogno di fondi extra per supportare una o più relazioni intime.

Minimizzare le pressioni

Se si desidera scoraggiare gli atti fraudolenti e massimizzare le possibilità di rilevazione quando questi si verificano, è necessario adottare misure per monitorare e controllare le pressioni. Tuttavia, questo è molto difficile all'atto pratico. Per mettere in atto questo è necessario essere consapevoli delle pressioni esistenti sia all'interno dell'azienda che nell'ambito personale dei dipendenti.

Risulta quindi necessario:

- Prestare più attenzione agli stili di vita ed alle abitudini dei dipendenti rispetto a quanto si è fatto in precedenza;
- Selezionare individui con alti livelli di integrità morale per occupare posizioni importanti e di fiducia;

- Sforzarsi di creare un ambiente che contribuisca a mantenere alto il livello di integrità personale.

Tecniche di prevenzione

Il seguente paragrafo elenca alcune delle azioni che è possibile attuare per minimizzare e monitorare le pressioni al fine di scoraggiare atti fraudolenti [113] [109].

Creare un clima aziendale adeguato

Frodi, furti e appropriazione indebita da parte dei dipendenti sono più frequenti in alcune organizzazioni che in altre. Se l'azienda crea un clima di onestà, il rischio di frode può essere notevolmente ridotto.

Ci sono diversi modi per farlo, tra cui:

- Mantenere condizioni di lavoro positive in cui i dipendenti sono ben ricompensati e in cui si soddisfano le esigenze personali;
- Creare un clima di apertura e fiducia in cui dipendenti e dirigenti si sentano liberi di comunicare. Se i dipendenti sentono di poter parlare liberamente, i manager capiranno l'aumentare o il diminuire delle pressioni prima che diventino acute;
- Implementare politiche relative a condizioni di lavoro, indennità, incentivi al lavoro e carriera.

Stabilire programmi di assistenza ai dipendenti

Sviluppare programmi di assistenza che forniscano ai dipendenti l'aiuto di cui hanno bisogno per superare i loro i problemi. In alcuni casi possono essere gestiti dall'azienda stessa, mentre in altri possono risultare così sensibili da essere gestiti al meglio da un'organizzazione esterna, assunta per fornire assistenza con la

riservatezza di cui i dipendenti sentono di aver bisogno. Sono possibili diversi tipi di possibilità, tra cui i seguenti:

- Consulenza finanziaria a coloro che lo desiderano. Ciò dovrebbe includere informazioni su questioni come acquisizione di prestiti, budget, investimenti, usi propri del debito, etc;
- Consulenza personale per problemi come il gioco d'azzardo e problemi familiari;
- Anticipi in denaro ai dipendenti con emergenze a breve termine e assistenza nell'assunzione di prestiti per quei dipendenti con esigenze a lungo termine.

Valutare regolarmente le prestazioni dei dipendenti

Il management dovrebbe valutare regolarmente le prestazioni dei dipendenti e, a valle di questa attività, rivedere regolarmente stipendi e benefici. Andrebbero anche stabilite procedure per gestire le rimostranze, fornendo così ai dipendenti uno sbocco per manifestare il disaccordo ed essere ricettivi rispetto ai reclami presentati [121].

Monitorare le pressioni dei dipendenti

Esistono diversi modi per rilevare le pressioni che devono affrontare i dipendenti, tra cui:

- Aumentare il volume del monitoraggio per osservare le abitudini di lavoro, gli atteggiamenti, lo stile di vita e i sentimenti dei dipendenti;
- Valutare l'efficacia e l'efficienza delle operazioni;
- Osservare modelli o stili di vita insoliti dei dipendenti e dare seguito ad azioni correttive.

Riduzione al minimo delle pressioni aziendali

Molte pressioni viste precedentemente possono essere minimizzate facendo leva su uno o più dei seguenti punti:

- Stabilire politiche del personale eque ed uniformi in modo che i dipendenti siano remunerati in modo adeguato alle loro responsabilità e siano trattati in modo equo e senza pregiudizi o favoritismi;
- Fornire consulenza sulla carriera, valutando le aspirazioni dei dipendenti ed aiutandoli a comprendere come possono migliorare per raggiungere tali aspettative;
- Sviluppare sistemi di comunicazione formali, come procedure di reclamo, che consentano ai dipendenti di esprimersi;
- Valutare regolarmente le prestazioni dei dipendenti;
- Rivedere regolarmente stipendi, salari, e benefici;
- Evitare aspettative elevate ed irrealistiche, facendo partecipare i dipendenti attivamente alla definizione dei propri obiettivi di performance;
- Evitare ricompense e punizioni eccessive per il successo o il fallimento di un dipendente in una attività;
- Fare tutto il possibile per eliminare o minimizzare specifiche pressioni aziendali.

Massimizzazione dell'integrità dei dipendenti e minimizzazione delle razionalizzazioni

L'integrità personale si riferisce al codice etico personale di comportamento adottato da ciascuna persona. Le persone che mancano di questo possono comportarsi o meno correttamente, a seconda delle pressioni e delle opportunità

loro offerte, direttamente o indirettamente. La loro integrità non è quindi interiorizzata personalmente e non ha risvolti applicabili in tutte le situazioni [123].

Tecniche di prevenzione

I seguenti fattori di prevenzione contribuiscono a minimizzare le razionalizzazioni e massimizzare l'onestà dei dipendenti [43].

Recruiting

Una buona quantità di atti fraudolenti può essere eliminata selezionando attentamente i dipendenti. La selezione di dipendenti onesti può essere facilitata in diversi modi:

- Chiedere ai potenziali dipendenti nel colloquio di lavoro se sono onesti e affidabili. Mentre i dipendenti possono facilmente mentire, la domanda segnala al candidato l'importanza del valore onestà all'azienda;
- Usare deterrenti psicologici, come informare i richiedenti che vengono eseguiti controlli di sicurezza per verificare il loro background in conformità con le normative vigenti;
- Utilizzare uno dei numerosi strumenti progettati per misurare l'integrità personale dei candidati. Le prove dimostrano che questi strumenti possono prevedere in modo affidabile l'integrità personale.

Creare una cultura dell'onestà

Un modo in cui le aziende possono prevenire le frodi è creare una cultura organizzativa che insegni e sottolinei l'onestà. I dipendenti aziendali tendono naturalmente verso gli standard culturali di gestione, facendo sì che sia più difficile commettere atti fraudolenti quando:

- Un comportamento accettabile è chiaramente definito per i dipendenti;
- La direzione segue i principi e le procedure di controllo messi in atto;
- I dirigenti ed i collaboratori sono onesti;
- I dipendenti ritengono che la disonestà sia normalmente punita o perseguita.

Definire chiaramente le azioni corrette

È necessario definire quali siano i comportamenti accettabili e quali quelli inaccettabili in modo che i dipendenti siano a conoscenza della posizione dell'azienda in caso di problemi [72].

Nel definire queste azioni, le aziende dovrebbero:

- Stabilire standard di condotta espliciti e principi generali di comportamento;
- Preparare politiche chiaramente definite che descrivano esplicitamente comportamenti onesti e disonesti;
- Assicurarsi che tutti i dipendenti conoscano e comprendano le regole e gli standard aziendali.

Sviluppare adeguate pratiche di licenziamento

Le aziende devono prestare molta attenzione quando un dipendente viene licenziato. I dipendenti licenziati dovrebbero essere rimossi immediatamente dalle attività sensibili e negare loro l'accesso a dati importanti, per prevenire il sabotaggio o la copia di dati riservati.

Formare correttamente i dipendenti

È molto meno probabile che si verifichino frodi in un ambiente in cui i dipendenti ritengono che la sicurezza sia affari di tutti. Una cultura aziendale ideale per la deterrenza alle frodi esiste quando i dipendenti sono orgogliosi della loro compagnia e protettivi nei confronti dei suoi asset. Sentono di avere una responsabilità nel denunciare frodi perché ciò che danneggia l'azienda danneggia anche loro. Questa cultura deve essere creata, insegnata e praticata. Per sviluppare questo tipo di cultura, un'azienda dovrebbe educare e formare i dipendenti nelle seguenti aree [108]:

- Misure di sicurezza: i dipendenti devono essere istruiti sul perché le misure sono importanti ed essere motivati a prenderle seriamente. La sicurezza dovrebbe essere monitorata per rafforzare questa formazione;
- Considerazioni etiche: l'azienda dovrebbe promuovere i propri standard etici nelle proprie pratiche aziendali, erogando corsi di formazione e mettendo a disposizione la documentazione in un ambiente condiviso;
- Sanzioni per comportamenti non conformi: i dipendenti devono essere informati delle conseguenze di comportamenti non conformi agli standard definiti.

Questo processo di formazione può essere realizzato attraverso:

- La conduzione di discussioni informali e incontri formali;
- L'emissione periodica di promemoria dipartimentali;
- La distribuzione di linee guida e codici scritti di etica professionale;
- La distribuzione di rapporti di violazioni e delle loro conseguenze;
- La promozione di programmi di formazione in materia di sicurezza e frodi.

OPPORTUNITÀ

L'opportunità è la condizione o situazione che consente ad una persona di commettere un atto fraudolento. Come le pressioni, le opportunità non causano di per sé frodi, tuttavia le probabilità di frode aumentano man mano che le opportunità diventano maggiori e più allettanti. Questo paragrafo tratta alcuni dei più importanti fattori di rischio che rendono maggiormente probabile il verificarsi di frodi, proponendo tecniche per la mitigazione e la riduzione di questi [111].

Controllo interno - Fattori di rischio e tecniche di prevenzione

Fattori di rischio

Questi fattori sono tra i più importanti:

- Controllo interno inadeguato;
- Mancata applicazione del controllo interno;
- Monitoraggio inadeguato dei controlli significativi.

Il fattore di rischio più significativo legato al concetto di opportunità nella maggior parte delle frodi è la non esistenza di controlli interni o la non adeguatezza di questi.

Tecniche di prevenzione

- Sviluppare un forte controllo interno: il modo migliore per scoraggiare le frodi è progettare, attuare e applicare controlli sufficienti a rendere difficile la commissione di atti fraudolenti. Il controllo interno deve includere controlli per le autorizzazioni, definire l'autorità dei ruoli, garantire controlli indipendenti sulle performance, essere redatto con adeguate procedure e documenti. Contestualmente deve essere garantita la

separazione delle funzioni addette a tutto ciò. Il controllo interno dovrebbe contenere:

  - Controlli preventivi per scoraggiare le frodi;
  - Controlli investigativi per scoprire frodi subito dopo che si verificano;
  - Controlli correttivi per porre rimedio ai problemi causati dalla frode.

- La responsabilità generale, per un controllo interno sicuro ed adeguato, spetta al top management. Questo deve inoltre stabilire procedure per garantire che i controlli siano rispettati ed applicati.

Inoltre valgono le seguenti considerazioni:

- I controlli sono molto più efficaci se inseriti in un sistema mentre viene costruito, piuttosto che successivamente. Devono essere presenti controlli per garantire l'applicazione del controllo interno e controlli per garantire che il controllo interno non venga ignorato;
- Il top management deve essere coinvolto nella progettazione e nel monitoraggio dei controlli.

Fattore di rischio: separazione dei compiti insufficiente

Un buon controllo interno richiede un'adeguata separazione dei compiti. Nessun singolo dipendente deve essere sovraccaricato di troppe responsabilità. Per ottenere un'efficace separazione dei compiti, devono essere separate le seguenti attività:

- Autorizzazione: il top management delega alcuni dipendenti ad autorizzare transazioni ed a prendere decisioni. I dipendenti che successivamente elaborano le transazioni devono verificare la presenza delle appropriate autorizzazioni;

- Registrazione: implica la preparazione di documenti, il mantenimento di libri contabili e di file connessi, nonché la preparazione dei report sulle prestazioni;
- Custodia: può essere diretta, come nel caso della gestione di contanti o della gestione di un inventario, o indiretta, come nel caso in cui si ricevono assegni dai clienti.

Se due di queste tre attività sono di responsabilità di una sola persona, possono sorgere problemi.

Tecniche di prevenzione

- Progettare ed applicare il controllo interno calcolando un'adeguata separazione dei compiti;
- Implementare procedure di autorizzazione chiare e adeguate.

Salvaguardia degli Assets: fattori di rischio e tecniche di prevenzione

Fattore di rischio: inadeguata salvaguardia degli Assets

Quando le persone pensano alla salvaguardia degli assets, molto spesso si pensa a contanti, assegni e beni fisici, come inventario e attrezzature. Tuttavia, oggi uno dei beni più importanti di un'azienda sono le sue informazioni. Di conseguenza degli steps devono essere declinati per salvaguardare sia le informazioni che i beni fisici.

Tecniche di prevenzione

Progettare e attuare adeguate garanzie sulle risorse fisiche. Le seguenti azioni sono utilizzate per salvaguardare i beni da minacce quali furto, uso non autorizzato e atti vandalici:

- Limitare l'accesso a posizioni fisiche, come sale computer e inventario;

- Limitare l'accesso fisico alle risorse, limitando così le possibilità di perdita. Ad esempio, contanti, registri e cassette di sicurezza;
- Limitare l'accesso ai file e alle informazioni del computer utilizzando password e codici di sicurezza;
- I documenti cartacei eliminati devono essere distrutti;
- I dipendenti devono essere informati delle conseguenze dell'uso di copie illegali di software, e la società dovrebbe istituire controlli per verificare che non vengano utilizzate copie illegali.

Fattore di rischio: conservazione inadeguata della documentazione

Anche il mantenimento di documenti e registrazioni inadeguati comporta rischi significativi [125].

Tecniche di prevenzione

- Richiedere che vengano conservati e controllati accuratamente i registri per rilevare eventuali irregolarità;
- Realizzare documenti progettati ed utilizzati in modo appropriato. I documenti dovrebbero:
    - Essere il più semplice possibile per ridurre al minimo gli errori di registrazione e facilitarne la corretta manutenzione, revisione e verifica;
    - Contenere uno spazio per le autorizzazioni o la firma della persona ricevente, se sono utilizzati ad esempio per trasferire beni a qualcun altro;
    - Essere numerati in sequenza in modo che ciascuno possa essere contabilizzato.

Supervisione - Fattori di rischio e tecniche di prevenzione

Fattore di rischio: supervisione inadeguata

È più probabile che si verifichino frodi quando la direzione non riesce a istituire una gestione appropriata della funzione di supervisione [7].

Tecnica di prevenzione

Sviluppare e attuare controlli per garantire un'efficace supervisione dei dipendenti, che preveda la formazione e l'assistenza dei dipendenti, il monitoraggio delle prestazioni dei dipendenti, la correzione delle criticità che vengono riscontrate.

Struttura organizzativa - Fattori di rischio e tecniche di prevenzione

Fattore di rischio: struttura aziendale complessa

Una struttura organizzativa inutilmente complessa è un altro fattore che rende la commissione di un atto fraudolento più facile. Gli esempi includono avere una numerosità alta di filiali e divisioni. La complessità non necessaria rende più facile la perdita di controllo ed il manifestarsi di inefficienze.

Tecnica di prevenzione

Le aziende dovrebbero adottare una struttura organizzativa adeguata, evitando complessità inutil. Per far ciò, devono:

- Avere chiare le linee di autorità e responsabilità;
- Assegnare la responsabilità di compiti specifici a dipartimenti e individui;
- Avere un framework che faciliti la pianificazione, la direzione e il controllo delle operazioni.

Fattore di rischio: figure di autorità che non possono essere messe in discussione

La gestione dominante ed incontrastata rappresenta un rischio di frode significativo.

Tecniche di prevenzione

- Accertarsi che nessuna persona o gruppo abbia un potere incontrastato. Nessuno deve avere così tanto potere che le decisioni ed azioni intraprese non possano essere messe in discussione ed esaminate. Riguardo al top management, deve avere l'autorità di agire con decisione e deviare dalle normali procedure quando le circostanze lo necessitano, ma deve comunque essere interrogato e tenuto a spiegare le azioni dei singoli componenti;
- Impostare dei controlli di compensazione. Un esempio potrebbe essere l'effettiva supervisione da parte del consiglio di amministrazione o di un comitato di revisione.

Fattore di rischio: disprezzo da parte della direzione per linee guida, controlli o autorità regolatorie

Quando la direzione non segue i controlli e le linee guida dell'azienda, costituisce un cattivo esempio per dipendenti. I dipendenti tendono a vedere l'azienda come se avesse due livelli di regole, una per loro ed un altro per la gestione. Quando il management vive secondo un diverso insieme di regole, i dipendenti si concentrano più su ciò che il management fa rispetto a quello che viene detto [5].

Tecniche di prevenzione

Un aspetto critico dell'ambiente di controllo di un'organizzazione è la filosofia di gestione e lo stile operativo che enfatizza l'onestà e l'adesione ai controlli. Più responsabile è la filosofia di gestione e lo stile operativo, più è probabile che i dipendenti si comporteranno responsabilmente nel lavoro per raggiungere gli obiettivi dell'organizzazione. La filosofia del management può essere valutata rispondendo alle seguenti domande:

- La direzione si assume rischi aziendali indebiti per raggiungere i propri obiettivi o valuta potenziali rischi e benefici prima di agire?
- Il management tenta di manipolare le misure di performance come il reddito netto in modo tale che le prestazioni sono viste in una luce più favorevole?
- Il management fa pressione sui dipendenti affinché raggiungano risultati indipendentemente dai metodi o richiedono un comportamento corretto nello svolgere le attività?

Fattore di rischio: dipendenti con precedenti penali o discutibili

Una caratteristica di controllo che spesso manca è un chek sul background di tutti i potenziali dipendenti.

Tecnica di prevenzione

Effettuare controlli in background, controllare i potenziali dipendenti, clienti ed i principali fornitori. I parametri da verificare sono:

- La storia finanziaria per determinare la posizione creditizia, l'indebitamento eventuale, possibili fallimenti;
- La storia occupazionale, incluso il numero di anni trascorsi in precedenti aziende;

- Condotte indesiderate, come gioco d'azzardo, abuso di droghe, etc;
- I precedenti penali.

Fattore di rischio: relazioni personali reciprocamente vantaggiose con clienti o fornitori

Agenti e venditori che sviluppano strette associazioni con venditori e clienti sono spesso in grado di commettere una frode. Ciò è particolarmente vero laddove si trovano ingenti somme di denaro. Ad esempio le frodi negli appalti sono particolarmente difficili da individuare poiché l'autore non deve modificare i libri contabili dell'azienda per coprire la frode.

Tecniche di prevenzione

- Richiedere dichiarazioni esplicite sul conflitto di interessi. Le aziende devono sviluppare un manuale che delinea le politiche e le procedure aziendali relative alle associazioni di imprese di acquirenti, rappresentanti di vendita e altri;
- Comunicare periodicamente a venditori e clienti le politiche dell'azienda in merito. Quando queste sono chiaramente comunicate ai clienti ed ai fornitori, si è in grado di determinare se gli agenti ed i venditori agiscono in conformità con le regole aziendali.

Fattore di rischio: andamento in periodi di crisi

Durante i periodi di crisi o di pressioni maggiori, ci sono ulteriori opportunità per commettere una frode [26]. Ad esempio, quando viene affrettato il completamento di un progetto, i controlli normali sono spesso messi da parte, il che si traduce in quanto segue:

- Si ottengono firme autorizzando acquisti incerti;
- I rimborsi vengono effettuati rapidamente e con poca documentazione;

- La gestione dei registri è in ritardo e non può essere ricostruita;
- I materiali vanno e vengono rapidamente e possono essere facilmente collocati male;
- In definitiva, nessuno è del tutto sicuro di chi sta facendo cosa.

Tecnica di prevenzione

Continuare a rafforzare il controllo interno in ogni momento.

Gestione strutturale ed amministrativa

Fattore di rischio: mancanza di un efficace Internal Audit

La presenza di una funzione aziendale che controlli e monitori il lavoro è una forte motivazione a non commettere atti fraudolenti. Quando questa è assente, sale la probabilità di poter commettere e nascondere una frode [28].

Tecnica di prevenzione

Mantenere un dipartimento di audit interno competente ed efficace, che effettui audit di verifica in maniera autonoma e indaghi sulle possibili irregolarità, è un deterrente significativo.

Fattore di rischio: assenza di un sistema di sicurezza interno

Sapere che non esiste un sistema di sicurezza interno può indurre un aspirante autore a perpetrare attività fraudolente.

Tecnica di prevenzione

Progettare e implementare un sistema di sicurezza interno. Un buon sistema di sicurezza interno si concentra su:

- Traffico di beni ed informazioni in entrata e in uscita dall'azienda;
- Procedure che regolano lo stoccaggio e il flusso dei materiali;
- Procedure di blocco interne ed esterne;
- Protezione delle informazioni sensibili all'interno dell'azienda.

Fattore di rischio: politiche e procedure poco chiare

Quando le politiche e le procedure non sono chiaramente definite, non funzionano più da deterrente [30].

Tecnica di prevenzione

Pubblicare un manuale di politiche e procedure contenente specifiche dichiarazioni sul conflitto di interessi, che sono uno strumento importante per assegnare autorità e responsabilità nelle organizzazioni.

Fattore di rischio: riporre troppa fiducia nei dipendenti

Le opportunità sorgono quando viene posta troppa fiducia nei dipendenti chiave che non sono soggetti a controlli. Una frase che frequentemente viene detta una volta scoperta una frode è: "Non posso credere che quella persona abbia commesso un atto fraudolento, era una dei miei impiegati più fidati."

Tecniche di prevenzione

Le persone in posizioni di fiducia dovrebbero essere soggette a controlli più rigorosi ed approfonditi rispetto alle responsabilità.

Fattore di rischio: lungo mandato in un lavoro chiave

I dipendenti che ricoprono posizioni chiave per periodi temporali molto lunghi possono iniziare a pensare di essere al di sopra delle regole.

Tecnica di prevenzione

Attuare la job rotation periodicamente per i dipendenti, in modo da portare alla luce possibili cattive condotte.

Fattore di rischio: nessuna supervisione efficace da parte del Consiglio di amministrazione

Se non vi è alcuna supervisione di una parte indipendente, come un consiglio di amministrazione, aumenta la confidenza dei potenziali autori di poter eseguire i loro schemi senza mai essere scoperti.

Tecnica di prevenzione

Organizzare un comitato di revisione composto da membri indipendenti del consiglio di amministrazione.

Fattore di rischio: formazione inadeguata

Una formazione inadeguata del personale comporta un rischio di frode significativo.

Tecnica di prevenzione

Sviluppare e attuare un programma di formazione che fornisca ai dipendenti le competenze necessarie.

1.16 Fraud Detection: Analisi Per Fattori Di Rischio

La fraud detection può essere definita come tutte le procedure ed azioni intraprese per accertare che una frode è stata commessa. La maggior parte degli autori di atti fraudolenti lasciano prove inconfondibili [8]. Ad esempio, quando una banca è vittima di una rapina, ci sono spesso testimoni e persino materiale video del furto. Al contrario, la frode è un crimine che è difficile da rilevare perché non viene quasi mai osservata direttamente. Quando si ricercano le frodi, è necessario imparare ad identificare gli indicatori (red flag), chiamati sintomi di frode, che possono indicarne l'esistenza, anche se questo non significa che sia realmente accaduto un atto fraudolento [13].
I sintomi devono essere attentamente studiati, per determinare se sono presenti a causa di una frode o di altre condizioni.

Sintomi di frode

La frode non è facile da rilevare, Il colpevole di solito si impegna molto per coprire la frode e per far sembrare tutto normale [55]. Tuttavia, l'autore è esposto a tre punti chiave:

- Furto: l'elemento di valore, come denaro contante, è materialmente travisato.
- Occultamento: l'autore nasconde le proprie azioni in modo tale da non far rilevare lo schema messo in atto. L'occultamento richiede spesso la creazione o la modifica di documenti o record, o altre azioni messo in atto per non farsi scoprire;

- Conversione: l'autore converte gli asset materiali in un modo che può essere utilizzato o speso.

Questi segni o manifestazioni sono indicati come sintomi di frode. Essere consapevoli di questi sintomi e cercarli attivamente è uno dei modi migliori per rilevare possibili frodi. Spesso però, coloro che hanno familiarità con i sintomi di frode sono talmente abituati alle azioni quotidiane da non notarli, mentre quelli che vengono notati non vengono investigati correttamente. Di conseguenza, molte frodi non sono rilevate in tempi corretti. Un approccio proattivo alla ricerca dei sintomi di frode funziona anche da deterrente. Di seguito saranno discussi alcuni sintomi di frode.

Sintomi contabili

Tutte le organizzazioni hanno un sistema di contabilità che raccoglie dati sulle transazioni aziendali. In un'azienda tipica:

- I dati vengono acquisiti su documenti cartacei o moduli elettronici;
- I dati vengono riepilogati e inseriti in file per la contabilità;
- I dati in questi file vengono aggiornati periodicamente ed organizzati per fornire una reportistica da mostrare al top management.

Quando viene commessa una frode, spesso è presente qualche elemento nei documenti o nei registri alterato, manipolato o distrutto per nasconderla. Questa azione di solito produce ciò che è indicato come un sintomo contabile. Questa sezione del paragrafo tratta alcuni dei più rilevanti.

Documenti alterati, falsi o insoliti

Di seguito sono riportati diversi tipi di sintomi relativi alla documentazione.

- Documenti modificati: la documentazione può contenere cancellature o modifiche. Un trucco utilizzato dagli autori è creare nuovi documenti con

parti di documenti originali. Quindi il nuovo documento viene fotocopiato in modo che non si possa dire che è stato creato da altri;

- Documenti distrutti o mancanti;
- Documenti duplicati: un esempio è un secondo pagamento per una singola fattura;
- Documenti annullati;
- Documenti che contengono elementi insoliti o anomali: possono includere elementi come ad esempio una calligrafia discutibile;

Transazioni grandi, insolite o complesse a fine anno

Particolare interesse devono destare le transazioni uniche eseguite verso la fine dell'anno o del semestre.

Voci di bilancio insolite

Ogni volta che una voce non rispetta il normale gli standard, è passibile di sospetto. Le voci in questione hanno i seguenti aspetti:

- Voci che sono inaccurate, come quelle che non sono in equilibrio.
- Voci inserite una persona non autorizzata.
- Voci che non dispongono della solita documentazione di supporto.

Sintomi comportamentali

Comportamento alterato

Psicologi comportamentali ed esperti investigatori di frodi affermano che la maggior parte degli autori di frodi, soprattutto se sono autori di reati per la prima volta, alterano il loro comportamento in modi riconoscibili [63]. Alcune delle modifiche più riconoscibili sono:

- Nervosismo e irrequietezza;

- Incapacità di guardare gli altri negli occhi;
- Stress, tensione ed incapacità di rilassarsi;
- Irritabilità insolita, costantemente sulla difensiva;
- Essere molto sospettosi degli altri;
- Non essere in grado di ammettere errori o giustificare sempre il comportamento.

Hotlines

Se i dipendenti sono in grado di segnalare atti commessi da altri in modo anonimo, sono spesso in grado di superare le riluttanze che comporta questa azione. Pertanto, un modo importante per scoprire le frodi è creare un hotline anonima per frode, che risulta essere uno strumento molto efficace [1]. Il rovescio della medaglia è che molte delle segnalazioni non sono meritevoli di indagine. Le motivazioni possono essere personali, come rabbia, gelosia o desiderio di vendetta. Pertanto è essenziale che nessun segnalato attraverso un canale di una hotline sia ritenuto colpevole fino a quando non sarà dimostrato il fatto. Un potenziale problema con una hotline è che le persone che gestiscono la hotline possono riferire a persone del top management o ad altri dipendenti. Questa criticitò può essere superata gestendo in outsourcing l'hotline istituita.

Sintomi derivanti dalla struttura organizzativa

Le aziende dovrebbero essere organizzate in modo ordinato ed efficiente. Quando una parte dell'organizzazione non ha uno scopo ben definito o logico, deve essere condotta un'analisi per determinare se la società sta cercando di nascondere qualcosa.

Struttura organizzativa eccessivamente complessa

I seguenti sono sintomi di una struttura organizzativa troppo complessa:

- Determinare quale organizzazione o persona controlla l'entità;
- Mancanza di un comitato di revisione composto da membri esterni al consiglio di amministrazione.

Sintomi derivanti dal controllo interno

Nel capitolo precedente sono state discusse in dettaglio le carenze del controllo interno che consentono la frode. L'assenza di uno di questi controlli è un sintomo di frode [11].

Quando viene rilevata una debolezza del controllo interno, la reazione tipica è

- Preoccupazione (deve essere risolverlo immediatamente?);
- Mancanza di preoccupazione.

Valutare periodicamente il controllo interno e indagare su tutti i punti deboli è uno dei metodi di rilevazione delle frodi più efficaci disponibili. Durante questa valutazione, è importante non guardare solo ai controlli interni che sono in atto, ma valutare se sono applicati. Avere un controllo interno in atto non efficiente è come non averlo.

Sintomi dettati dallo stile di vita

Quasi tutti i perpetratori spendono i loro guadagni illeciti con la stessa rapidità con cui il loro stile di vita migliora. Gli autori sembrano aver bisogno di una gratificazione immediata, portandoli ad una forma di consumo evidente, ad esempio:

- Auto;
- Case di lusso;
- Vacanze costose;

- Vestiti costosi, gioielli e pasti al ristorante;
- Regali per famiglia e amici;
- Gioco d'azzardo, droghe, alcol e relazioni sessuali.

Qualsiasi prova dei dipendenti dell'azienda che vivono al di là dei loro mezzi dovrebbe essere approfondita ed indagata.

Sintomi ambientali

I seguenti sono sintomi ambientali che possono indicare la presenza di frodi:

- Confusione sui corretti comportamenti;
- La società non effettua controlli in background su tutti i potenziali dipendenti ;
- La società opera spesso in modalità crisi;
- Il top management ignora regolarmente le linee guida e i controlli dell'azienda;
- Sussistono piani di performance che dipendono dal raggiungimento di obiettivi eccessivamente aggressivi;
- Standard di prestazione non realistici, che possono portare a disperazione e rabbia, con conseguente morale o lealtà di basso livello dei dipendenti.

1.17 Controllo E Monitoraggio

Nell'istituzione di un programma di fraud governance aziendale, fondamentali risultano le attività volte al controllo e al monitoraggio costante nonché alla definizione di un piano di comunicazione e reporting aziendale. Accanto alle metodologie classiche di fraud auditing, consistenti principalmente in verifiche su base campionaria o su rilevazione di alert da sistemi di hot-line e processi di whistleblowing, oggi si possono utilizzare nuove tecniche e strumenti basati su modelli logico/matematici in grado di elaborare e analizzare enormi quantità di dati [24]: attraverso specifici algoritmi, questi sistemi sono in grado di elaborare schemi di segnalazione e prevenzione di possibili attività fraudolente. Questi strumenti sono indispensabili in aziende moderne, grazie alla possibilità che offrono di integrare e analizzare i dati dei differenti sistemi informativi e gestionali aziendali [51]. In sintesi, quindi, tecnologie avanzate permettono di sviluppare sistemi antifrode di fraud prevention e fraud detection. Per essere efficaci, queste indagini devono essere supportate da modelli di data mining, ovvero da "modelli di estrazione dati idonei ad aggregare, collegare o associare informazioni provenienti da sistemi informativi diversi ed eterogenei" [83]. Il data mining viene definito come "il processo che utilizza intelligenze statistiche, matematiche, artificiali e tecniche di machine learning al fine di estrarre e identificare informazioni utili e conseguentemente ottenere conoscenza da un grande database". Un'altra definizione afferma che "il data mining utilizza diverse tecniche al fine di ricercare fra grandi quantità di dati e identificare relazioni e connessioni passate, estrarre regole di decisione o costruire modelli predittivi".

Al fine di sviluppare un sistema di data mining [71], è necessario sviluppare specifiche capacità, e, in particolare, implementare delle metodologie che garantiscono di:

- assicurare la qualità del dato in origine;
- assicurare la normalizzazione delle informazioni;
- definire le correlazioni e il modello logico/matematico più efficiente per estrarre informazioni in grado di individuare, con il minor numero di errori (falsi positivi e negativi) il fenomeno fraudolento da prevenire e/o rilevare;
- definire i criteri di controllo sull'efficacia del modello applicato;
- assicurare la qualità del dato intesa come unificazione della semantica delle varie tipologie di dati da sottoporre al processo di data mining. Il dato deve rispecchiare la qualità sintattica e deve essere affidabile.

Il secondo aspetto necessario alla definizione del modello di data mining è la normalizzazione del dato. Questa operazione è volta a uniformare la semantica e la sintassi delle diverse informazioni al fine di poterle fare elaborare e riconoscere dall'applicativo di data mining [91].

Le metodologie per le attività di fraud prevention e di fraud detection sono:

- i *link* o *pattern analysis*: si tratta di ricerca di associazioni e interconnessioni tra gruppi di eventi e/o di persone;
- i *geometric clustering*: sotto-insieme del precedente modello, in cui i raggruppamenti sono funzioni di distanze geometriche; sia le *link pattern analysis* che i *geometric clustering* sono spesso denominati social network *analysis*, in quanto permettono di identificare le interconnessioni tra diversi avvenimenti-fattori e ricostruirne il nesso causa-effetto;
- *machine learning*: modelli auto-apprendenti che modificano i propri parametri in funzione delle variazioni nel tempo dei dati esaminati,

vengono generalmente utilizzati per analizzare database con grandi quantità di dati e rinvenire le reciproche relazioni fra essi. Gli strumenti di *machine learning* sono estremamente utili per la predisposizione di modelli di prevenzione essendo in grado di correlare centinaia di migliaia di eventi, definendone le dinamiche e potendone quindi prevedere gli accadimenti;

- *neural networks:* sistemi particolari di auto-apprendimento derivati dalla teoria delle reti neurali. Sono gli strumenti più avanzati, che simulano il processo neuronale di apprendimento e memorizzazione dell'essere umano. Anche gli strumenti sviluppati sulle reti neurali sono estremamente efficaci per lo sviluppo di sistemi che riescano a "prevedere" la commissione di attività fraudolente.

Tendenzialmente sono previste sei tipologie di classi di applicazione di data mining [76]:

- *classification:* prevede la costruzione e l'utilizzo di un modello al fine di poter categorizzare i dati e, attraverso ciò, prevedere la categoria di appartenenza di dati sconosciuti. Per fare ciò si identificano e stabiliscono delle relazioni e schemi comuni ai dati classificando in relazione a essi le informazioni e i dati a disposizione in classi o concetti;
- *clustering:* utilizzato per effettuare una partizione di oggetti in gruppi concettuali inediti (i cluster), che per caratteristiche degli oggetti all'interno dei cluster sono molto simili, ma con differenze fra un cluster e un altro sostanziali. L'analisi cluster scompone quindi i dati in gruppi dissimilari al fine di far sì che i dati in un gruppo siano il più simili possibile e che i dati contenuti fra i gruppi siano il più differenti possibile.

- *prediction:* stima valori futuri su base numerica e ordina sulla base dello schema di un set di dati;
- *outlier detection*: misura la "distanza" tra i dati al fine di individuare quelli che sono molto differenti dai set predeterminati. Quelli che hanno caratteristiche diverse dai set predeterminati vengono denominati outlier;
- *regression:* è un metodo statistico che rivela le relazioni tra una o più variabili indipendenti e una variabile dipendente. Spesso questa tecnica viene utilizzata nelle ricerche di evidenza empirica come benchmark;
- *visualization:* metodologia che converte le complicate caratteristiche e schemi di dati in presentazioni grafiche facilmente comprensibili.

Sulla base di queste sei tipologie ci sono otto tecniche di data mining specificamente destinabili all'applicazione in funzione antifrode [59]:

- Regression model;
- Neural networks;
- Bayesian Belief Network;
- Decision Trees;
- Naive Bayes;
- Nearest Neighbour Method;
- Fuzzy logic and Genetic Algorithm;
- Expert Systems.

Nel terzo capitolo verrà descritta la progettazione di un sistema antifrode basato sull'apprendimento automatico attraverso l'uso di alberi decisionali.

1.18 Focus: whistleblowing

Il Whistleblowing è uno strumento di derivazione anglosassone attraverso il quale i dipendenti di una organizzazione, pubblica o privata, segnalano a specifici individui o organismi, (compresi organi di polizia e autorità pubbliche) una possibile frode, un reato, un illecito o qualunque condotta irregolare, commessa da altri soggetti appartenenti all'organizzazione. I dipendenti normalmente sono le prime persone che vengono a conoscenza di eventuali situazioni di rischio e, pertanto, sono anche le prime persone in grado di segnalarle tempestivamente all'organizzazione. Lo scopo del WB è quello di permettere alle organizzazioni di affrontare il problema segnalato il prima possibile, rendendo note situazioni di rischio o di danno e contribuendo alla prevenzione e al contrasto di eventuali illeciti. La gestione virtuosa del WB contribuisce non solo ad individuare e contrastare possibili illeciti e a diffondere la cultura dell'etica e della legalità all'interno delle organizzazioni, ma anche a creare un clima di trasparenza ed un senso di partecipazione e appartenenza, generato dal superamento del timore dei dipendenti di subire ritorsioni da parte degli organi sociali o dei colleghi, o dal rischio di vedere inascoltata la propria segnalazione.

NORMATIVA VIGENTE

Panorama Internazionale

In ambito internazionale diversi sono stati gli interventi volti a sollecitare gli Stati ad introdurre specifiche disposizioni normative in materia di WB, tra cui hanno assunto un ruolo di rilievo [139]:

- La Convenzione civile sulla corruzione emanata dal Consiglio d'Europa il 4 novembre 1999, ratificata in Italia con la legge n. 112/2012, che richiede

agli Stati membri l'introduzione di meccanismi di protezione adeguata per i dipendenti che in buona fede denunciano di fatti di corruzione;

- La Convenzione delle Nazioni Unite contro la corruzione del 31 ottobre 2003, ratificata in Italia con la legge n. 116/2009, che richiede agli Stati aderenti di prevedere meccanismi di tutela per le persone che segnalano fatti di corruzione;
- La "Recommendation of the Council on Guidelines for managing conflict of interest in the public service" dell'OCSE del 28 maggio 2003, che include principi generali per favorire l'adozione da parte degli Stati di procedure di WB che prevedano, da un lato, la protezione dei segnalanti da eventuali ritorsioni e, dall'altro, regole per impedire eventuali abusi dei meccanismi di denuncia.

A differenza dell'Italia, dove il percorso di assimilazione di questi principi internazionali è stato piuttosto lento e frammentario, in altri Paesi la disciplina del WB è stata puntualmente oggetto di interventi normativi.

Panorama Italiano

Le Linee Guida si inseriscono nel quadro normativo italiano piuttosto limitato in materia di WB. È noto, infatti, che solo alcune normative di settore trattano espressamente e forniscono una regolamentazione del fenomeno del WB, in particolare [139]:

- Il D.Lgs. 165/2001 o Testo Unico sul pubblico impiego e, segnatamente, l'art. 54 bis del D.Lgs. 165/2001 che prevede la tutela del pubblico dipendente che denuncia o riferisce condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro;
- Il D.Lgs. 385/1993 o Testo Unico Bancario ("TUB"), così come modificato dal D.Lgs. 72/2015, che richiede che le banche adottino procedure

specifiche per la segnalazione da parte del personale, sia all'interno che verso l'esterno, di atti o fatti the possano costituire una violazione delle norme disciplinanti l'attività svolta; procedure che devono essere disegnate prevedendo canali specifici, autonomi e indipendenti per la segnalazione, nonché meccanismi idonei a garantire la riservatezza dei dati personali del segnalante e del segnalato e a tutelare adeguatamente il segnalante da ritorsioni (art. 52 bis);

- Il D.Lgs. 58/1998 o Testo Unico sugli intermediari finanziari ("TUF"), così come modificato dal D.Lgs. 72/2015, che prevede che gli intermediari e le relative capogruppo adottino procedure di segnalazione aventi le stesse caratteristiche di quelle disciplinate dal TUB (art. 8 bis).

Altre fonti normative prevedono, invece, obblighi di informazione che possono, in qualche modo, essere paragonate alle segnalazioni tipiche del WB, tra queste:

- Il D.Lgs. 231/2001, sulla responsabilità amministrativa da reato degli enti, il quale prevede comunque degli «obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e sull'osservanza dei modelli»;
- Il D.Lgs. 81/2008, Testo Unico in materia di sicurezza, che prevede, tra gli obblighi dei lavoratori, quello di segnalare tempestivamente al datore di lavoro le anomalie presenti in attrezzature, sostanze, materiali e dispositivi.

LINEE GUIDA PER LA PREDISPOSIZIONE DI PROCEDURE DI WHISTLEBLOWING

Ambito di applicazione

Le procedure per la gestione del WB possono essere adottate sia da enti pubblici che da organizzazioni private, ove per:

- Enti pubblici: si intendono tutte le amministrazioni pubbliche così qualificate dalla normativa vigente e, quindi, gli enti di diritto pubblico nazionali, regionali o locali, comunque denominati, istituiti, vigilati o finanziati da Pubbliche Amministrazioni. Le presenti Linee Guida possono essere di supporto, a titolo esemplificativo, a Regioni, Province, Comuni, Comunità Montane e loro consorzi e associazioni; istituti e scuole di ogni ordine e grado comprese le università; aziende ed amministrazioni dello Stato ad ordinamento autonomo; camere di commercio, industria, artigianato e agricoltura e loro associazioni; tutti gli enti pubblici non economici nazionali, regionali e locali comunque denominati, istituiti, vigilati o finanziati da Pubbliche Amministrazioni; le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale, nonché gli enti di diritto privato in controllo pubblico di livello nazionale e locale.
- Enti privati e imprese: si intendono tutti gli enti forniti di personalità giuridica e tutte le società ed associazioni anche prive di personalità giuridica. Le presenti Linee Guida, si prefiggono l'obiettivo di diffondere le buone prassi in materia di WB al maggior numero possibile di organizzazioni.

Principi chiave

È opportuno che le Procedure adottate all'interno di organizzazioni pubbliche e private siano improntante e contengano espresso richiamo ai seguenti principi fondamentali [139]:

1) Regole chiare: la procedura di WB per essere compresa e correttamente applicata dai destinatari deve esplicitare nel modo più semplice e chiaro possibile i diversi principi e passaggi rilevanti. In particolare nelle Procedure deve essere chiaro:

- Chi sono i destinatari;
- Quali sono gli standard di comportamento che l'organizzazione si aspetta dal dipendente;
- Quali tipologie di irregolarità possono essere oggetto di segnalazione;
- Quali caratteristiche deve avere la segnalazione;
- Quali sono i canali attraverso cui effettuare la segnalazione;
- Quali sono le azioni che l'organizzazione intraprende a seguito della segnalazione;
- Quali sono le tutele che vengono garantite al segnalante e al segnalato;
- Quali sono le conseguenze in caso di abuso o di uso strumentale dello strumento del WB.

2) Promozione della cultura della trasparenza: è fondamentale che le Procedure siano espressione di una precisa volontà e di un serio impegno del vertice dell'organizzazione ad essere promotore della cultura della trasparenza e ad ascoltare le segnalazioni dei dipendenti (cosiddetto Top Level Commitment). È importante che i vertici siano percepiti come i primi soggetti che promuovono attivamente il WB e che incoraggiano l'intera organizzazione a segnalare ogni possibile situazione di rischio. La promozione della cultura della trasparenza può

essere affidata alle iniziative più varie ma deve puntare a far sì che ogni dipendente:

- Non si senta obbligato ad effettuare una segnalazione, ma si senta invogliato a farlo dal proprio management;
- Sia consapevole del fatto che le sue segnalazioni verranno prese in considerazione seriamente dall'organizzazione.

A titolo di esempio, per sviluppare il Top Level Commitment, si può anche immaginare che l'organizzazione:

- Realizzi una specifica formazione per ogni livello aziendale.
- Organizzi incontri che coinvolgano tutto lo staff al fine di permettere una piena conoscenza a tutti i livelli dell'importanza del WB nell'impresa;
- Affigga messaggi positivi e incoraggianti nelle bacheche;
- Utilizzi l'intranet aziendale anche con la creazione di un'apposita newsletter e FAQ mirate a spiegare le procedure di segnalazione.

3) Riservatezza e protezione dei dati personali: tra gli aspetti centrali che dovrebbero essere rappresentati nelle procedure vi sono certamente la riservatezza e la protezione dei dati personali dei soggetti coinvolti. È essenziale che le procedure garantiscano che i destinatari della segnalazione trattino con confidenzialità l'identità del segnalante e del segnalato, nelle more dell'accertamento della sua eventuale responsabilità. I nomi di segnalante e segnalato, pertanto, non devono essere rivelati senza il loro consenso, a meno che non sia la legge a richiederlo espressamente, al fine di proteggere tali soggetti da possibili speculazioni e ritorsioni da parte dei colleghi o dei superiori. A tale riguardo, il disegno di legge n. 2208 recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato", trasmesso al Senato per

l'approvazione, rappresenta l'unico punto di riferimento "organico" sulla materia. Non è escluso, peraltro, che il Garante per la protezione dei dati personali sia interpellato nel corso dell'iter legislativo diretto all'approvazione del disegno di legge. Il Garante, peraltro, già nel 2009 aveva auspicato, per il settore privato, l'adozione di apposite disposizioni legislative, volte a regolamentare canali di comunicazione per la segnalazione di presunti illeciti, attraverso:

- L'individuazione dei presupposti di liceità del trattamento effettuato per il tramite dei canali di comunicazione, indicando tra l'altro l'ambito soggettivo di applicazione della disciplina;
- Individuazione puntuale delle finalità che si intendono perseguire e le fattispecie oggetto di possibile "denuncia" da parte dei segnalanti;
- La definizione dell'eventuale ammissibilità dei trattamenti derivanti da segnalazioni anonime.

4) Anonimato: al fine di poter diffondere la cultura del WB ed incoraggiare le segnalazioni appare opportuno che le procedure prevedano anche la possibilità di effettuare segnalazioni anonime. È importante ammettere l'anonimato per due motivi:

- Attualmente gli individui, dato il contesto culturale in cui vivono, sono ancora restii ad effettuare segnalazioni: l'anonimato, da questo punto di vista, aiuterebbe la diffusione del WB;
- La segnalazione ha precipuamente una funzionedi allerta, non di denuncia: è l'ente ad essere chiamato ad approfondire, accertare e verificare i fatti segnalati, a prescindere dalla conoscenza dell'identità del segnalante. È, in ogni modo, preferibile che le segnalazioni anonime siano

tenute distinte dalle segnalazioni confidenziali, prevedendo, ad esempio, apposite modalità operative per la segnalazione anonima.

I segnalanti anonimi, devono essere consci del fatto che:

- La loro segnalazione potrebbe comportare per le organizzazioni maggiori difficoltà di accertamento, potendo essere più complicato per l'ente mantenere i contatti con il segnalante anonimo e chiedere, ove necessario, la sua collaborazione nonché fornire un feedback sull'andamento della verifica della segnalazione;
- Non è possibile per le organizzazioni, in assenza di dati che possano aiutare a determinare l'identità del segnalante, porre in essere tutte le tutele previste per i casi di segnalazioni confidenziali.

5) Differenze tra whistleblowing e lamentela personale: è importante che le procedure chiariscano che la lamentela personale non può formare oggetto di segnalazione. Le segnalazioni, infatti, riguardano tutte quelle situazioni in cui il segnalante agisce a tutela di un interesse non personale, in quanto il fatto segnalato, solitamente, attiene a pericoli o rischi che minacciano l'organizzazione nel suo complesso, altri dipendenti, i terzi, i soci o anche, in via più generale, la collettività. Le procedure devono, quindi, chiarire quali sono le segnalazioni ritenute rilevanti al fine della successiva verifica, differenziandole dalle lamentele personali, che non formano oggetto del processo di segnalazione.

6) Feedback: le procedure devono prevedere che le organizzazioni forniscano sempre un feedback al segnalante in merito alla gestione della segnalazione, in quanto l'assenza di riscontro potrebbe scoraggiare le segnalazioni future dei lavoratori.

È opportuno che le procedure prevedano la possibilità per il segnalante di chiedere un aggiornamento o un riscontro in merito alla propria segnalazione, ma anche di fornire ulteriori informazioni nel caso in cui il fatto oggetto di segnalazione sia proseguito, interrotto, o addirittura aggravato. Le procedure dovrebbero prevedere, quanto meno, che il segnalante sia informato:

- Nel momento in cui la sua segnalazione è stata presa in carico oppure nel caso in cui la stessa necessiti di dettagli ulteriori per poter essere scrutinata;
- Quando la verifica si è conclusa.

7) Formazione: una adeguata formazione è fondamentale per garantire la migliore conoscenza delle procedure all'interno dell'organizzazione. Le procedure devono prevedere la strutturazione di apposite sessioni formative per ogni singola categoria di possibili destinatari. In particolare:

- Per i dipendenti devono essere sottolineate le modalità con cui effettuare una segnalazione efficace e rappresentate le tutele e garanzie esistenti in caso di segnalazione;
- Per i dirigenti e i soggetti individuati dall'organizzazione come destinatari delle segnalazioni deve essere prevista anche una formazione su come gestire le stesse.

8) Tutela del segnalante e del segnalato: le procedure devono prevedere meccanismi di tutela sia nei confronti del segnalante, sia nei confronti del segnalato, in modo che:

Venga garantita la riservatezza dei dati personali dei soggetti coinvolti, salve espresse previsioni di legge;

- Il segnalante venga protetto da qualsiasi azione discriminatoria e ritorsiva, quali ad esempio il demansionamento, il mobbing, il licenziamento;
- Il segnalato sia protetto dalle mere delazioni da parte dei colleghi, volte solo a danneggiare la sua reputazione;
- Siano evitate situazioni in cui il segnalante abusi della procedura per ottenere vantaggi personali;
- Nessun procedimento disciplinare si possa basare esclusivamente sulla segnalazione.

I SOGGETTI COINVOLTI

Le procedure di WB sono rivolte al maggior numero possibile di soggetti al fine di garantire la più ampia diffusione della cultura dell'etica e della trasparenza. È consigliabile, pertanto, che le procedure, sia per le organizzazioni pubbliche sia per quelle private, identifichino quali potenziali segnalanti [139]:

- Il personale dell'organizzazione, categoria in cui vanno ricompresi tutti i dipendenti, a tempo indeterminato e non, i dirigenti, gli stagisti;
- Gli amministratori e i membri degli organi sociali;
- Terze parti non dipendenti, categoria in cui vanno ricompresi collaboratori, consulenti, con qualsiasi tipologia di contratto o incarico, soggetti che agiscono per conto dell'organizzazione, quali intermediari ed agenti, terzi fornitori di prodotti o servizi.

L' OGGETTO DELLA SEGNALAZIONE

È importante che le Procedure chiariscano quali siano gli eventi meritevoli di segnalazione e quali, invece, siano da considerarsi estranei al perimetro del WB. Rilevanti, ai fini della segnalazione, in via esemplificativa sono:

- I fatti che possono integrare reati, illeciti, irregolarità;
- I comportamenti a danno dell'interesse pubblico e dell'azienda privata;
- Le azioni suscettibili di arrecare un pregiudizio patrimoniale o di immagine alla società, ente o amministrazione di riferimento;
- Le azioni suscettibili di arrecare un danno alla salute o sicurezza dei dipendenti, utenti e cittadini o di arrecare un danno all'ambiente;
- Le azioni poste in essere in violazione dei codici di comportamento o di altre disposizioni o procedure interne all'organizzazione sanzionabili in via disciplinare.

Con specifico riferimento al settore pubblico si raccomanda che le procedure chiariscano il concetto di corruzione, il quale deve essere inteso in senso lato, come comprensivo di tutte quelle situazioni in cui venga riscontrato l'abuso da parte di un soggetto del potere a lui affidato al fine di ottenere vantaggi privati e, quindi, tutte le situazioni in cui venga in evidenza un malfunzionamento dell'attività amministrativa a causa dell'uso a fini privati delle funzioni attribuite. Sia con riferimento al settore pubblico sia per il settore privato, è opportuno che le procedure chiariscano che non saranno meritevoli di segnalazione:

- Le mere voci o i "sentito dire";
- Le doglianze di carattere personale del segnalante o sue rivendicazioni/istanze.

IL CONTENUTO DELLA SEGNALAZIONE

Le procedure devono chiaramente indicare che il segnalante è chiamato a fornire elementi utili a consentire ai soggetti preposti di procedere alle dovute ed appropriate verifiche ed accertamenti a riscontro della fondatezza dei fatti oggetto di segnalazione, sebbene non sia indispensabile che il segnalante disponga di prove sufficienti a dimostrare il fatto riportato. A tal fine, le procedure possono prevedere che la segnalazione debba preferibilmente contenere i seguenti elementi:

- Le generalità del soggetto che effettua la segnalazione, con indicazione della posizione o funzione svolta nell'ambito dell'azienda;
- Una chiara e completa descrizione dei fatti oggetto di segnalazione;
- Se conosciute, le circostanze di tempo e di luogo in cui sono stati commessi i fatti segnalati;
- Se conosciute, le generalità o altri elementi che consentano di identificare il soggetto che ha posto in essere i fatti segnalati (ad esempio la qualifica o il settore in cui svolge l'attività);
- L'indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;
- Eventuali documenti che possano confermare la fondatezza dei fatti riportati;
- Ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

Al fine di poter al meglio gestire i contenuti della segnalazione, in modo che la stessa possa contenere tutte informazioni utili per la successiva verifica da parte dei soggetti preposti, è buona pratica che le procedure prevedano, tra le possibili modalità di segnalazione, la compilazione da parte del segnalante di un apposito

modulo predisposto dall'organizzazione. In questo modo sarà più agevole per il segnalante individuare le informazioni che l'organizzazione ritiene importanti per accertare i fatti oggetto di segnalazione. Per poter assicurare che il processo di segnalazione sia utilizzato evitando il più possibile strumentalizzazioni, si suggerisce che il modulo preimpostato riporti anche:

- Un campo in cui il segnalante è chiamato a dichiarare o meno l'esistenza di eventuali conflitti di interesse (dichiarazione obbligatoria per il settore bancario);
- La specificazione dell'impegno del segnalante a riferire quanto di sua conoscenza secondo verità.

LE SEGNALAZIONI ANONIME

Al fine di favorire l'emersione di segnalazioni è opportuno che le Procedure, sia nelle organizzazioni pubbliche sia in quelle private, annoverino la possibilità di verificare anche le segnalazioni anonime, ovvero quelle segnalazioni prive di elementi che consentano di identificare il loro autore [139].

È, quindi, opportuno che le Procedure:

- Prevedano appositi canali di comunicazione nel caso in cui il segnalante non volesse rivelare la propria identità;
- Evidenzino come la segnalazione anonima possa comunque determinare in capo al segnalante il rischio di eventuali ritorsioni da parte del segnalato, senza, d'altra parte, permettere all'organizzazione di apprestare gli appositi strumenti di tutela previsti in caso di segnalazione confidenziale.

Per poter assicurare che il processo di segnalazione sia utilizzato evitando il più possibile strumentalizzazioni, le procedure devono prevedere la presa in carico e successiva valutazione solamente delle segnalazioni:

- Recapitate tramite le modalità previste dalla procedura interna di WB;
- Adeguatamente circostanziate in modo tale da far emergere fatti e situazioni relazionati a contesti determinati (indicazione di nomi o qualifiche, di uffici specifici, di eventi particolari, ecc.).

I DESTINATARI DELLE SEGNALAZIONI

Le procedure devono specificare a quale soggetto/organo vanno indirizzate le segnalazioni. In particolare, a seconda delle dimensioni dell'organizzazione possono essere individuati:

- Il responsabile della funzione compliance;
- Il responsabile della funzione di internal audit;
- Un comitato rappresentato da soggetti appartenenti a varie funzioni (ad esempio legale, internal audit o compliance, finanziaria);
- Un soggetto specifico dedicato;
- Il datore di lavoro nelle PMI;
- Enti o soggetti esterni dotati di comprovata professionalità che si occupino di gestire la prima fase di ricezione delle segnalazioni in condivisione con l'organizzazione.

Oltre ad indicare chiaramente un soggetto/organo deputato a ricevere le segnalazioni è bene che le procedure prevedano anche la possibilità di invio della segnalazione a soggetti alternativi (detti anche "destinatari di garanzia"), quali possono essere, ad esempio, le altre funzioni sopra indicate quali destinatari

preferenziali della segnalazione. La creazione dei destinatari di garanzia, infatti, ha la funzione di assicurare il più possibile che la segnalazione non sia inoltrata ad un soggetto [114]:

- Gerarchicamente o funzionalmente subordinato all'eventuale segnalato;
- Che sia il presunto responsabile della violazione;
- Che abbia un potenziale interesse correlato alla segnalazione tale da comprometterne l'imparzialità e l'indipendenza di giudizio.

È consigliabile, inoltre, che le procedure individuino nel diretto superiore del segnalante un possibile elemento di raccordo tra lo stesso segnalante e l'organismo preposto a ricevere la segnalazione, ciò nel caso in cui il segnalante si sentisse più a suo agio a riferire al diretto superiore. In tal caso, si suggerisce che sia lo stesso diretto superiore ad informare della segnalazione il soggetto preposto alla ricezione. Da ultimo, è opportuno che le Procedure specifichino chiaramente come l'Organismo di Vigilanza ex D.lgs. 231/2001 rappresenti il destinatario dedicato delle segnalazioni che riguardano la violazione del Modello di Organizzazione, Gestione e Controllo. Con riferimento al settore pubblico, le Procedure devono prevedere, secondo quanto indicato dalla normativa, che la segnalazione sia rivolta a:

- Il Responsabile per la Prevenzione della Corruzione;
- L'ANAC stessa nel caso la segnalazione riguardi direttamente il Responsabile per la Prevenzione della Corruzione.

I CANALI PER LE SEGNALAZIONI

Al fine di facilitare le segnalazioni, le procedure devono definire canali alternativi e dedicati cui il segnalante può ricorrere. Potranno pertanto essere individuati e

indicati in procedura appositi canali, gestiti solamente dai soggetti individuati dall'organizzazione quali destinatari delle segnalazioni, quali:

- Indirizzi di posta elettronica dedicati alle segnalazioni;
- Un software interno dedicato;
- Numeri fax o indirizzi dedicati per comunicazioni scritte;

I canali qui elencati si possono ritenere alternativi tra loro e comunque validi e nel concreto vanno individuati sulla base della complessità delle organizzazioni. Ove possibile e nei casi richiesti dalla specifica regolamentazione di settore, come nel caso delle organizzazioni pubbliche è preferibile l'adozione di un sistema di WB informatizzato, che utilizzi un software per la gestione del processo di segnalazione. In tal modo, rispetto all'utilizzo di altri canali, risulta da un lato più agevole la completa proceduralizzazione degli adempimenti utili ad ottenere una segnalazione il più possibile efficace e dall'altro maggiormente garantita la riservatezza del segnalante. Attraverso un sistema informatizzato di gestione delle segnalazioni, infatti:

- I dati del segnalante e del segnalato possano essere tutelati attraverso la crittografia;
- L'accesso agli stessi e alla segnalazione può avvenire solamente attraverso l'inserimento di un codice specifico in possesso solamente dei soggetti individuati dall'organizzazione quali destinati delle segnalazioni e responsabili della successiva verifica.

È utile, infine, che le procedure prevedano l'utilizzo di apposite helpline per consentire ai dipendenti di chiedere chiarimenti in merito alle regole stabilite dall'organizzazione su come effettuare la segnalazione e su quali canali utilizzare.

I COMPITI E I POTERI DI CHI RICEVE LA SEGNALAZIONE

È essenziale che le procedure indichino chiaramente non solo quali attività devono essere poste in essere dall'organo/soggetto deputato a ricevere la segnalazione ma anche quali poteri sono a questo attribuiti per la verifica delle segnalazioni. Quanto alle attività, innanzitutto è necessario che l'organo/soggetto deputato effettui un primo screening di ammissibilità della segnalazione, poiché, come già evidenziato, è importante distinguere la segnalazione dalla mera lamentela personale.

Dovrà essere valutato:

- Se la segnalazione ha lo scopo di sottoporre all'attenzione dell'organizzazione un comportamento che pone a rischio la sua attività e/o i terzi, e non una mera lamentela;
- Quanto è grave e urgente il rischio per l'organizzazione e/o per i terzi;
- Se l'oggetto della segnalazione è già stato valutato in passato dall'organizzazione, o addirittura dall'Autorità competente;
- Se la segnalazione contiene sufficienti elementi per poter essere verificata o se, al contrario, risulta troppo generica e priva degli elementi necessari per una successiva indagine.

Il destinatario, valutata la segnalazione una semplice lamentela personale o verificato che il fatto riportato è già stato riscontrato dall'organizzazione o dall'Autorità competente, procederà all'archiviazione della segnalazione, informandone il segnalante. Allo stesso modo il destinatario contatterà il segnalante qualora ritenesse la segnalazione eccessivamente generica, al fine di chiedere di fornire elementi utili all'indagine. Il destinatario, poi, procederà all'archiviazione della segnalazione nel caso in cui non siano forniti elementi ulteriori o siano comunque forniti elementi ritenuti insufficienti. Nel caso, invece,

in cui il destinatario della segnalazione ritenga necessaria la verifica, si passerà ad un'indagine approfondita sui fatti oggetto della stessa, al fine di appurarne la fondatezza. Quanto ai poteri, è opportuno che le Procedure prevedano, in capo all'organismo destinatario delle segnalazioni, il potere di ricorrere alla collaborazione con altre funzioni aziendali, ad esempio attraverso la richiesta di condivisione di specifiche informazioni e/o documenti. È opportuno, altresì, che le Procedure prevedano:

- La compilazione da parte dei soggetti deputati di un report finale dell'indagine;
- L'archiviazione di tutta la documentazione pertinente l'indagine, incluso il report, in modo idoneo ad evitare l'accesso di terzi alle informazioni e documenti.

Le Procedure devono, infine, prevedere la necessità di fornire un feedback al segnalante in merito all'attività svolta, ciò al fine di rassicurarlo del fatto che la segnalazione è stata presa in considerazione e valutata.

LE TUTELE

Tutele per il segnalante

Le procedure devono prevedere apposite tutele per i diversi soggetti coinvolti nel processo di segnalazione, a partire dal segnalante. La prima forma di tutela deve consistere nell'adottare tutte le misure necessarie al fine di garantire la riservatezza del segnalante, ad eccezione dei casi in cui sia la normativa in vigore a richiedere che venga esclusa [139]. È necessario, pertanto, che le procedure assicurino che l'identità del segnalante rimanga segreta e, a tal proposito:

- Si deve prevedere una corretta informazione e formazione degli organi deputati a ricevere le segnalazioni affinché gestiscano in modo riservato le informazioni;
- Deve essere garantita l'impossibilità di accesso alla segnalazione e all'identità stessa del segnalante da parte del segnalato e di terzi che non siano stati indentificati dall'organizzazione quali destinatari delle segnalazioni o quali soggetti deputati alla successiva indagine in merito ai fatti segnalati.

In ambito bancario e finanziario, le procedure devono prevedere l'istituzione di appositi sistemi interni di segnalazione che garantiscono la riservatezza e la protezione dei dati personali del segnalante e del soggetto eventualmente segnalato, ferme restando sempre le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione. In particolare, per le banche deve essere nominato un responsabile dei sistemi interni di segnalazione, il quale assicura il corretto svolgimento del procedimento e riferisce direttamente e senza indugio agli organi aziendali le informazioni oggetto di segnalazione, ove rilevanti. Il suddetto responsabile, poi, unitamente a tutti i soggetti che ricevono, esaminano e valutano le segnalazioni, ha l'obbligo di garantire la confidenzialità delle informazioni ricevute, anche in merito all'identità del segnalante che, in ogni caso, deve essere opportunamente tutelato da condotte ritorsive, discriminatorie o comunque sleali conseguenti alla segnalazione. È fondamentale che le procedure definiscano una serie di rimedi contro le eventuali ritorsioni o comportamenti discriminatori in danno del segnalante, in ragione della segnalazione. Il pericolo di azioni ritorsive nei confronti dei segnalanti è ciò che solitamente induce questi ultimi ad astenersi

dal riportare possibili irregolarità o fatti illeciti. Le ritorsioni di cui può essere vittima il segnalante possono consistere, ad esempio, nel:

- Licenziamento;
- Demansionamento;
- Trasferimento ingiustificato;
- Mobbing;
- Molestie sul luogo di lavoro o qualsiasi altro tipo di comportamento che determini condizioni di lavoro intollerabili.

Si deve sottolineare, poi, così come affermato dall'ANAC per il settore pubblico, che la protezione accordata dalle organizzazioni può riguardare esclusivamente le ritorsioni che possono avere luogo nell'ambito del rapporto di lavoro, e non anche quelle di altro tipo. Pertanto, le procedure devono espressamente prevedere che non è consentita, né tollerata, alcuna forma di ritorsione o azione discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro del segnalante per motivi collegati direttamente o indirettamente alla segnalazione e che tali comportamenti sono passibili di sanzioni disciplinari. Devono, poi, chiaramente indicare che simili misure di tutela valgono esclusivamente per coloro che segnalino in buona fede, ossia per quei segnalanti che abbiano riportato la problematica ritenendo altamente probabile, sulla base alle proprie conoscenze, che si sia verificato un fatto illecito o un'irregolarità.

Eventuali meccanismi premiali

Sebbene non vi siano fonti normative nazionali che prevedano meccanismi premiali per il segnalante, esperienze internazionali, indicano la possibilità per le organizzazioni di prevedere forme di incentivazione delle segnalazioni. Si tratta

di individuare efficaci meccanismi premiali che non si risolvano nella semplice remunerazione diretta per la segnalazione ma che siano utili a favorire lo sviluppo di una cultura di apertura e trasparenza. Si possono indicare, ad esempio:

- Bonus aziendali per il segnalante, nel caso in cui la segnalazione abbia determinato la reale soluzione di una problematica per l'organizzazione;
- Benefit per tutti coloro che abbiano creato un clima aperto e trasparente;
- Valutazioni positive, per tutti quei lavoratori, dirigenti o dipendenti, che abbiano partecipato attivamente ai corsi di formazione.

Tutele per il segnalato

È essenziale che le procedure prevedano anche strumenti di tutela del soggetto segnalato nelle more dell'accertamento della sua eventuale responsabilità. Le organizzazioni, infatti, devono evitare che la propria politica di WB venga utilizzata abusivamente da segnalanti in malafede. Devono inoltre definire chiaramente le ipotesi in cui il segnalante potrebbe abusare dello strumento della segnalazione, come nel caso di:

- Segnalante che riporti falsamente un fatto solamente al fine di danneggiare il segnalato;
- Segnalante che abbia partecipato al comportamento irregolare unitamente ad altri soggetti e attraverso la segnalazione cerchi di assicurarsi una sorta di "immunità" dalle future azioni disciplinari che l'organizzazione vorrà intraprendere;
- Segnalante che voglia utilizzare la problematica riportata come possibile strumento di scambio per ottenere la riduzione, o l'esclusione, di una precedente sanzione disciplinare o per ottenere benefici all'interno dell'organizzazione, quali, ad esempio, bonus o promozioni.

Nelle Procedure deve, quindi, essere specificato che:

- Le segnalazioni non devono contenere accuse che il segnalante sa essere false e che, in generale, la segnalazione non deve essere utilizzata come strumento per risolvere mere questioni personali;
- La segnalazione non garantisce alcuna protezione al segnalante nel caso in cui abbia concorso alla realizzazione della condotta illecita;
- L'organizzazione si impegna a tutelare il segnalante solo rispetto a possibili condotte ritorsive o discriminatorie poste in essere in ragione della segnalazione, e che sono possibili eventuali sanzioni disciplinari a cui il segnalante potrebbe essere sottoposto per comportamenti passati;
- Impregiudicata la responsabilità penale e civile del segnalante, nell'ipotesi di segnalazione calunniosa o diffamatoria, le segnalazioni manifestamente false, opportunistiche e/o effettuate al solo scopo di danneggiare il segnalato nonché ogni altra ipotesi di abuso o strumentalizzazione intenzionale della procedura di WB sono passibili di sanzioni disciplinari.

Le procedure, inoltre, al fine di evitare eventuali abusi, devono chiaramente prevedere che non si possa sanzionare disciplinarmente il soggetto segnalato sulla base di quanto affermato dal segnalante, senza che vi siano riscontri oggettivi e senza che si sia proceduto ad indagare i fatti oggetto di segnalazione. Come già indicato nei paragrafi che precedono, devono prevedere meccanismi che garantiscono la riservatezza dell'identità del segalato, nelle more del processo interno di accertamento. In particolare è importante che evidenzino come il feedback al segnalante non comprenda l'eventuale specifico provvedimento disciplinare erogato nei confronti del segnalato.

Sanzioni per i dipendenti/dirigenti

Al fine di poter efficacemente attuare un sistema di WB è necessario che le procedure indichino chiaramente quelle che potrebbero essere le specifiche sanzioni disciplinari non solo per il segnalato in caso di conferma dei fatti segnalati, ma anche per tutti coloro agiscono in violazione delle procedure stesse. In particolare, le sanzioni potranno essere previste:

- Nel caso in cui il segnalato sia ritenuto responsabile a seguito dell'attività di indagine svolta dall'organo destinatario della segnalazione;
- In caso di comportamenti abusivi del segnalante;
- In caso di comportamenti ritorsivi o discriminatori da parte dei lavoratori ,dirigenti e subordinati, nei confronti del segnalante;
- Nel caso in cui l'organismo preposto a ricevere la segnalazione non verifichi quanto riportato dal segnalante;
- In caso di violazione degli obblighi di riservatezza associati alla gestione delle segnalazioni.

Le sanzioni verranno applicate sulla base dello Statuto dei Lavoratori (legge n. 300/1970) e dei singoli contratti collettivi nazionali, differenziando, quindi, tra soggetti dirigenti e dipendenti. Ogni organizzazione dovrà verificare concretamente, sulla base delle predette fonti, quale sanzione applicare. A titolo esemplificativo potrebbero essere previsti:

- Il richiamo verbale, l'ammonizione scritta, la sanzione pecuniaria, la sospensione dal servizio, la revoca dell'incarico per i dirigenti;
- Il richiamo verbale, il richiamo scritto, la multa, la sospensione dal servizio, il licenziamento con o senza preavviso per i dipendenti.

Resta fermo il diritto dell'organizzazione di adire le autorità competenti nel caso in cui rilevi che il fatto illecito sollevato dal segnalante presenti tutte le caratteristiche di un reato ovvero di un illecito civile.

Sanzioni per i terzi

Chiamati al rispetto delle procedure sono anche tutti quei soggetti che operano all'interno, o per conto dell'organizzazione, come ad esempio collaboratori, consulenti, lavoratori somministrati, procuratori e agenti ma anche tutti i partner e fornitori. Le procedure dovrebbero prevedere l'inserimento di specifiche clausole nei contratti o nelle lettere di incarico, con cui vengono regolati i rapporti con i terzi, che sanciscano il rispetto delle stesse e indichino le sanzioni applicabili in caso di violazione, quali, a titolo meramente esemplificativo:

- La diffida al puntuale rispetto delle Procedure;
- L'applicazione di una penale, anche in caso di mancato rispetto della diffida, prevista in misura percentuale rispetto al compenso pattuito;
- La risoluzione immediata del contratto.

1.19 Fraud Investigation And Audit

La frode è come un iceberg e quello che si nota in prima istanza è solo una piccola parte di ciò che è realmente accaduto. Per determinarne la dimensione effettiva, quindi, un investigatore di frodi deve andare a fondo per scoprire la sua vera portata. Lo scopo di un'indagine è determinare se si è verificata una frode e, in caso affermativo, scoprire quindi la sua entità [100]. Per fare questo, esistono diversi tipi di prove che possono essere raccolte ed analizzate, che sono state classificate in quattro principali categorie:

- documentali;
- derivate dall'interazione tra i dipendenti;
- derivate dall'osservazione personale;
- prove fisiche.

Ognuno di questi quattro tipi di prove saranno discussi in questo paragrafo, iniziando dalle fasi del processo di indagine.

Il processo di investigazione delle frodi

Le aziende che vogliono rilevare frodi devono essere alla ricerca dei sintomi analizzati nel capitolo precedente. Quando questi vengono notati, devono essere analizzati. Lo scopo di un'indagine è di raccogliere prove sufficienti per determinare se una frode si è verificata o meno. È necessario prestare molta attenzione nel determinare chi è sospettato e quindi potrebbe essere indagato, perché quando i dipendenti si rendono conto del target di un'indagine, possono presentarsi ripercussioni sull'ambiente che vanno tenute in conto [72].

Fase 1: riconoscimento e definizione dei problemi

L'obiettivo di questa fase è determinare se esiste una condizione sufficiente per indagare su di un sintomo di frode. Il presupposto è definito come la totalità delle circostanze che porta una persona ragionevole, prudente e professionalmente preparata a credere che una frode si sia verificata, si stia verificando o si verificherà. Si noti che il presupposto è solo una ragione sufficiente per giustificare un'indagine. Prima di iniziare un'indagine formale è necessario ottenere l'approvazione della direzione [42].

Fase 2 – Raccolta delle prove

Una volta stabilito il presupposto, le prove vengono raccolte nel tentativo di accertare se, in effetti, si è verificata una frode [80]. Vengono raccolte prove per determinare:

- Cosa è stato rubato;
- Chi ha commesso l'atto;
- Come è stato commesso l'atto;
- Quando è stata commessa la frode;
- Perché è stato commesso l'atto;
- Dove si è verificata la frode.

Per evitare di suscitare sospetti e implicare un sospetto innocente, è buona prassi iniziare ad utilizzare tecniche investigative che non sono facilmente riconoscibili, come ad esempio:

- Coinvolgere il minor numero di persone possibile all'inizio;
- Lavorare gradualmente verso il principale sospettato, fino a quando non sarà coinvolto in un'intervista;
- Fare riferimento all'indagine utilizzando parole non minacciose, come audit e inchiesta.

Fase tre: valutazione delle prove

In questo passaggio, le prove raccolte vengono valutate per determinare se siano sufficienti per valutare e denunciare la frode. Non vengono raccolte prove per formulare un'opinione sul fatto che si sia verificata una frode, perché ciò può essere fatto solo in un tribunale. Tuttavia, le prove devono essere valutate per determinare se sono complete e accurate [92]. Se le prove sono ritenute insufficienti, potrebbe essere necessario raccoglierne ulteriori. Inoltre, possono anche essere valutate per determinare la migliore linea di condotta dell'azienda (andare in tribunale, ottenere una confessione dal responsabile, etc...).

Fase quattro: definizione reportistica

La fase finale dell'indagine sulla frode è redigere un report contenente i risultati . Alcune caratteristiche importanti di un rapporto di frode di qualità sono:

- Precisione;
- completezza;
- Imparzialità;
- Chiarezza;
- Rilevanza.

Un rapporto di frode non deve mai contenere una conclusione o un'opinione sul fatto che una frode sia effettivamente accaduta [115]. Quando un caso viene portato in tribunale, il rapporto di frode viene ammesso come prova. Se contiene opinioni e conclusioni, l'avvocato difensore può tentare di usarle per dimostrare pregiudizio verso il cliente.

Le prove

Le prove sono qualcosa che può aiutare a dimostrare o confutare i fatti in presenza di una frode. Per essere legalmente accettabili come prove, questi elementi devono essere:

- Raccolte legalmente;
- Competenti;
- Obiettive;
- Rilevanti.

Prove documentali

Uno dei più importanti tipi di prove raccolte sono le prove documentali, nonché anche il tipo di prova più ampio e più frequentemente raccolto. Ad un occhio addestrato, i documenti possono dire molto su una frode, perchè contengono informazioni preziose che possono condurre ad esempio a testimoni. I documenti forniscono anche una traccia cartacea che mostra ad un investigatore cosa è successo durante ogni fase dell'elaborazione del documento.

Regole per la raccolta e la gestione delle prove documentali

Di seguito sono riportate delle regole generali su come prendersi cura delle prove documentali [116]:

- Conservare tutti i documenti che hanno impatto sull'analisi;
- Conservare i documenti originali ove possibile. Le copie originali sono considerate primarie;
- Non toccare i documenti originali più del necessario. I documenti potrebbero avere impronte digitali, cancellazioni, alterazioni, che possono essere danneggiate o distrutte dalla manipolazione. Potrebbero anche essere necessari in seguito per l'analisi forense;

- Non modificare l'aspetto di un documento;
- Non riparare documenti strappati;
- Non esporre il documento a umidità, luce solare o calore e non lasciarlo incustodito;
- Collocare gli originali in una copertina trasparente che consenta loro di essere visualizzati e manipolati senza danneggiarli. Su ciascuna copertina, segnare la data di ricezione del documento;
- Creare una copia dell'originale e conservare l'originale in un luogo sicuro;
- Mantenere una catena di custodia per ciascun documento dal momento in cui viene ricevuto fino alla sua presentazione in tribunale come prova. Senza questa catena, un documento potrebbe non essere accettato dal tribunale come prova;
- Laddove non sia possibile ottenere il possesso fisico di un documento originale esistente, farne una copia. Le copie sono considerate prove secondarie e sono ammesse come tali quando:
    - L'originale è stato perso o distrutto da qualcuno diverso dalla parte introducendolo come prova;
    - Una parte avversa ha il controllo del documento e non può essere ottenuto;
- Sviluppare un sistema di archiviazione che consente di trovare rapidamente i documenti necessari;
- Creare un database contenente le seguenti informazioni:
    - la data di creazione del documento e la data di ricezione;
    - La fonte del documento;
    - L'oggetto del documento e una breve descrizione del suo contenuto;
    - Un numero che identifica il documento.

Come ottenere le prove documentali

Esistono diversi modi per ottenere il possesso di prove documentali [126]:

- Consenso volontario: molte delle aziende e persone indagate non hanno nulla da nascondere e forniranno agli investigatori la documentazione di cui hanno bisogno. Il consenso può essere orale o scritto, con consenso scritto preferito quando il documento è ottenuto da una società avversa o testimone;
- Citazioni: prove documentali in possesso di terzi possono essere difficili da ottenere senza un ordine del tribunale;
- Ordine di esibizione: sono ordini emessi da un giudice quando vi è una elevata probabilità che nella documentazione richiesta vi siano elementi indiziari di colpevolezza.

Tipi di analisi del documento

I seguenti sono alcuni dei controlli più comuni effettuati sulla documentazione [61]:

- Analisi della scrittura, per determinare se un documento o una firma scritti a mano sono autentici;
- Analisi di alterazione, per determinare se un documento è stato modificato o modificato.
- Analisi dell'inchiostro, per determinare se tutto l'inchiostro di un documento proviene dalla stessa penna o matita, o per determinare l'età dell'inchiostro o del piombo.
- Analisi della carta, per determinare se la carta su cui è scritto un documento ha la stessa trama, spessore, colore e opacità in tutte le pagine.

Derivazioni dall'interazione tra i dipendenti

Le persone dentro e fuori la società sono fonti di prove per gli investigatori, poiché interagiscono tra loro avendo maggiori probabilità di vedere cambiamenti nei loro comportamenti. Di seguito alcuni strumenti attraverso i quali ottenere prove.

Hotline

Come già visto in precedenza, affinchè una hotline abbia successo, deve essere caratterizzata dai seguenti fattori:

- Garanzia di anonimato;
- Capacità di richiamo, in modo che l'investigatore possa ottenere ulteriori informazioni;
- Presenza di Campagne di sensibilizzazione, così i dipendenti vengono informati e periodicamente sulla garanzia di anonimato;
- Supporto del top management.

Interviste

L'intervista è uno degli strumenti più importanti nel basket degli strumenti a disposizione, e devono essere strutturate per ottenere quanto segue [119]:

- Informazioni sugli elementi essenziali della frode;
- Informazioni sul background personale;
- Cooperazione tra vittime e testimoni.

Le tipologie di persone intervistate sono di tre tipi:

- Intervistati cooperativi;
- Intervistati neutrali;
- Intervistati ostili.

Una buona intervista si articola in tre fasi distinte:

- Introduzione: lo scopo del colloquio deve essere chiaramente indicato;
- Corpo: in questa fase la persona viene intervistata per scoprire chi, cosa, quando, dove, perché e come.
- Chiusura: l'auditor ringrazia per la collaborazione.

Prove fisiche

Le prove fisiche sono il tipo di prove meno utilizzate in un'indagine per frode. In altri crimini, comportano l'esame e l'analisi di oggetti come armi da omicidio, oggetti di droga, ecc. Un'indagine per frode a volte può comportare l'esame e l'analisi di [127]:

- Le impronte digitali;
- Serrature rotte;
- Oggetti fisici, come l'inventario rubato;
- Sostanze come grasso e liquidi;
- Tracce, come vernici e macchie; e
- Impressioni, come segni di taglio e tracce di pneumatici.

1.20 Focus: computer forensic

Utilizzo di risorse informatiche e informative aziendali: la policy aziendale

La documentazione normativa di regolazione interna a carattere aziendale, così come disciplinata dal codice civile e dalle leggi speciali, può inoltre essere integrata da una ulteriore regolazione di dettaglio, per effetto di esigenze contigenti e specifiche dell'impresa, in relazione all'attività svolta o all'utilizzo di risorse strumentali. Le risorse informatiche e informative aziendali, ad esempio, sono costituite dal complesso delle informazioni in disponibilità dell'azienda a vario titolo (database ed archivi cartacei relativi a proprietà intellettuale, know how, business, informazioni contabili/finanziarie, informazioni sui clienti, sui fornitori e sui partner d'impresa, documentazione di sistema, procedure operative o di supporto, piani di continuità), risorse software e risorse hardware. Queste risorse comprendono anche le risorse di Rete, cioè posta elettronica, internet, intranet. L'utilizzo, da parte di tutti i componenti dell'organizzazione aziendale, delle risorse informative e informatiche aziendali elencate deve avvenire in conformità alle leggi ed ai regolamenti dello Stato e alle normative aziendali interne, allo scopo non solo di eseguire puntualmente la prestazione lavorativa, ma anche di evitare o ridurre al minimo rischi di indisponibilità, accesso non autorizzato, distruzione o perdita accidentale delle risorse stesse. Simili rischi possono essere sintetizzati nell'espressione "evento illecito" [140], che è ogni evento, sia interno che esterno all'azienda, che determini una lesione o un pregiudizio grave nei confronti di beni/interessi, di cui l'impresa abbia la tutela, la proprietà od anche la disponibilità, per i quali la legge preveda anche l'applicabilità di una sanzione penale. Occorre prevenire i rischi connessi ad un utilizzo di dette risorse per motivi non attinenti allo svolgimento delle mansioni

aziendali o addirittura per motivi dolosamente diretti a compromettere rete, dati, informazioni e apparecchiature. Si devono quindi predisporre idonee e preventive misure di sicurezza, in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche. In particolare la sicurezza fisica è il complesso di sistemi, prodotti e procedure destinato alla protezione delle risorse aziendali, costituite da impianti, ambienti e persone e che sinteticamente costituiscono il patrimonio aziendale. L'esigenza di disporre di adeguati mezzi di protezione è legata all'intensità di frequentazione delle aree di operatività dell'impresa ed al valore dei beni e dei processi produttivi [141]. È diritto dell'imprenditore di svolgere forme di controllo cd. "difensivo" sull'esattezza della prestazione lavorativa e sul corretto uso, da parte del lavoratore, dei beni e servizi aziendali messigli a disposizione per l'espletamento delle mansioni lavorative. Il controllo difensivo consiste in attività conseguenti ad eventi illeciti, volte ad accertare la responsabilità del fatto e la quantificazione del danno, coordinando le iniziative volte a minimizzare i danni subiti dall'impresa ed a contrastare i rischi d'immagine derivanti, nonché segnalando eventuali debolezze del sistema di controllo interno che abbiano favorito il verificarsi dell'evento illecito. Il controllo difensivo, consistente nell'acquisizione di tutte le evidenze (documenti, testimonianze, fotografie, registrazioni, etc...) comprovanti la realizzazione dell'illecito, si conclude con l'elaborazione di una relazione (report), funzionale all'adozione di provvedimenti, cautelativi e/o repressivi, ed eventualmente disciplinari, richiesti dal caso. Policies, linee guida, regolamenti interni ed altri documenti variamente denominati sono così gli strumenti dell'impresa con i quali i vari aspetti della vita lavorativa sono regolamentati, sotto il profilo dello svolgimento fisiologico dell'attività lavorativa, con riferimento al corretto utilizzo dei sistemi aziendali, all'informazione sulle misure di sicurezza adottate e sull'utilizzo dei dati raccolti all'interno dell'azienda.

Riferimenti normativi

Il fondamento normativo che giustifica la legittimità dell'adozione della "policy aziendale" (o altra simile denominazione) risiede nel combinato disposto degli artt. 4 e 8 legge 300/1970 (Statuto dei Lavoratori) , artt. 2, 3, 4, 113 e 114 D.Lgs. 196/2003 (Codice Privacy), e 2087, 2104 e 2555 e.e. Il controllo diretto ad accertare condotte illecite ed individuare responsabilità è lecito e non confliggente con i diritti e le libertà fondamentali e la dignità del lavoratore: l'esigenza difensiva infatti è giustificata dalla salvaguardia del patrimonio aziendale, che comprende beni, servizi e persone e trova fondamento costituzionale nel combinato disposto degli artt. 35 e 41 Cost. laddove si statuisce che la Repubblica tutela il lavoro in tutte le sue forme ed applicazioni e l'iniziativa economica privata è libera e non può svolgersi in contrasto con l'utilità sociale o in modo da arrecare danno alla sicurezza, alla libertà ed alla dignità umana. L'esigenza difensiva manifestata realizzata con il controllo è funzionale alla garanzia della sicurezza dei luoghi di lavoro e alla salvaguardia, tra l'altro, del diritto al lavoro mediante lapreservazione delpatrimonio aziendale da attacchi diretti a comprometterlo. L'illecito commesso nei luoghi di lavoro non può pertanto trovare nessuna "copertura" dietro il diritto alla privacy, in quanto l'illecito mette a rischio o danneggia proprio il patrimonio aziendale che è funzionale all'esercizio dell'impresa da un lato e all'esercizio del diritto al lavoro dall'altro.

Rilevanza ai fini della responsabilità amministrativa degli enti (D.LGS. 231/2001)

La legge 18 marzo 2008, n. 48 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento intero" ha ampliato le fattispecie di reato che possono generare la responsabilità degli enti. L'art. 7 del

provvedimento ha introdotto nel D.Lgs. 231/01 l'art. 24-bis "Delitti informatici e trattamento illecito di dati". I nuovi reati introdotti nella disciplina della responsabilità amministrativa degli enti dalla L. n. 48/08 sono: falsità in un documento informatico pubblico o avente efficacia probatoria, accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.), detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.), diffusione di apparecchiature , dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.), intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.), installazione di apparecchiature atte ad intercettare , impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.), danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.), danneggiamento di informazioni, dati e programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.), danneggiamento di sistemi informatici o telematici (art. 635-quarter c.p.), danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.), frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.). È agevole rilevare come queste fattispecie criminose siano la tipizzazione, sul piano della tutela penale, dei rischi di indisponibilità, accesso non autorizzato, distruzione o perdita accidentale delle risorse informative, che gravano sulle risorse informative e informatiche dell'azienda e dai cui derivano le pesanti sanzioni previste e disciplinate dal D.LGS. 231/2001.

L'unico modo per stornare l'applicazione delle sanzioni a carico dell'ente è la dimostrazione dell'adozione e della efficace attuazione di un "modello di organizzazione, gestione e controllo" idoneo a prevenire la commissione degli illeciti penali considerati. Il D.LGS. 231/200 prevede poi l'istituzione di un

Organismo di controllo, che sia interno all'ente, con il compito di vigilare sul funzionamento e sull'osservanza dei modelli, nonché di curare il loro aggiornamento. Il comma 2, dell'art. 6 del D.LGS. 231/2001 indica le due fasi principali in cui deve articolarsi un sistema idoneo: in primo luogo l'identificazione dei rischi rappresenta la fase di preparazione del sistema, nel corso della quale va analizzato il contesto aziendale (area per area, settore per settore) in modo da evidenziare la probabilità di commissione degli illeciti; in secondo luogo la progettazione del sistema di controllo, che avverrà prima analizzando gli eventuali strumenti di controllo già in essere, per poi valutare successivamente l'opportunità e le modalità del suo adeguamento alle prescrizioni del D.LGS. 231/2001.

Policy aziendale, computer forensics e data retention

La Computer Forensics, di cui si parlerà nel paragrafo che segue, costituisce forse il processo più importante nell'ambito delle attività riconducibili ai c.d. "controlli difensivi", riconosciuti legittimi a seguito di sentenze della Cassazione, oltre che della magistratura di merito, e a seguito di provvedimenti a carattere generale e decisioni del Garante per la protezione dei dati personali. Il controllo difensivo, come si è già detto sopra, è la reazione dell'impresa ad un evento illecito realizzato dal dipendente a danno del patrimonio aziendale o a danno di terzi. Si tratta di un controllo diretto ad accertare condotte illecite e ad individuare i soggetti responsabili, siano essi i lavoratori, siano essi occasionali visitatori. In via prudenziale, ed allo scopo di evitare ricorsi al Garante della Privacy oltre che sanzioni penali, sanzioni processuali (i dati personali trattati in violazione della disciplina in materia di trattamento dei dati personali non possono essere utilizzati), è opportuno, anche se non strettamente necessario, ricorrere alla procedura di cui all'art. 4, comma 2 legge 300/1970. L'informativa diffusa

all'interno dell'impresa mediante gli strumenti variamente denominati "policy", "regolamento interno aziendale", "linee guida" è sufficiente per legittimare la raccolta e l'utilizzo dei dati relativi alle operazioni di controllo. In ogni caso non è richiesto il consenso per l'utilizzo dei dati ai fini di controllo difensivo [141]. La policy aziendale sono un elemento fondamentale per l'efficacia dell'attività investigativa aziendale. Esse infatti contengono i seguenti elementi:

- I riferimenti e richiami agli illeciti informatici, alfine di creare consapevolezza negli utenti;
- le regole a cui il personale e le terze parti che operano con l'azienda devono attenersi nell'uso della strumentazione informatica;
- le modalità e i limiti nella raccolta delle informazioni per le attività interne di gestione e prevenzione frodi, in particolare per quanto concerne la raccolta di prove elementi probatori;
- le modalità di coordinamento e di collaborazione tra le strutture coinvolte nelle attività di indagine;
- le azioni che possono essere intraprese nei confronti di un soggetto coinvolto in un'attività fraudolenta.

In ultimo occorre sottolineare che le policy, per loro stessa natura, necessitano di continuo aggiornamento, in quanto risentono dei mutamenti normativi e dell'organizzazione interna dell'azienda. Le cautele da seguire nell'acquisizione e conservazione dei dati sono realizzate nella procedura di seguito illustrata [142]:

- circoscrivere e dettagliare nella maniera più precisa possibile l'area fisica dell'illecito, il numero dei dipendenti sospettati, gli elementi dell'illecito; formalizzare la richiesta di accesso agli incaricati a ciò proposti, inclusi in un elenco ad hoc, già predisposto nell'ambito della adozione di misure di sicurezza idonee ad evitare o ridurre il rischio di accessi non autorizzati o di trattamenti non consentiti o non conformi alle finalità della raccolta;

- acquisire i dati afferenti ai movimenti dei soggetti sospetti, evidenziando esclusivamente i movimenti pertinenti al fatto illecito;
- adottare soluzioni informatiche idonee ad assicurare il controllo delle attività svolte. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti. Tali soluzioni comprendono la registrazione delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi. I sistemi di audit log devono garantire la completezza, l'immodificabilità e l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad auditing. Il controllo deve riguardare anche gli accessi compiuti dagli incaricati allo scopo di evitare abusi;
- elaborare una reportistica interna che tenga contro esclusivamente del fatto illecito scoperto e quindi funzionale al solo comportamento illecito. Per quanto riguarda la conservazione dei log file, si ritiene che la durata di conservazione debba essere ancorata al momento dell'effettuazione dell'inventario delle consistenze patrimoniali ai fini della dichiarazione dei redditi annuale, per il cui il termine massimo è dato dalla comunicazione, ad opera del Responsabile dell'inventariazione, dell'avvenuta effettuazione dell'inventario e dal rilievo negativo in termini di diminuzione o danneggiamento delle consistenze stesse. La conclusione del controllo delle consistenze patrimoniali dell'impresa costituisce il dato temporale entro cui accertare eventuali comportamenti illeciti di danno o di furto al patrimonio aziendale. Il fondamento giuridico è da rinvenirsi nel testo unico delle imposte sul reddito, laddove impone precisi oneri in sede di

redazione della dichiarazione annuale dei redditi e dell'imposta sul valore aggiunto.

In dettaglio, la data entro cui la conservazione può essere consentita può coincidere con i seguenti termini:

- giorno ed ora della conclusione delle operazioni di inventariazione e della elaborazione del report sulle operazioni compiute;
- giorno ed ora della comunicazione del report sulle operazioni di inventariazione al responsabile dei servizi contabili;
- giorno della approvazione del bilancio;
- giorno dell'invio della dichiarazione dei redditi annuale.

Una ulteriore procrastinazione del termine della conservazione non appare legittimamente proponibile, in quanto con l'invio della dichiarazione dei redditi si congelano tutte le consistenze patrimoniali ai fini fiscali e quindi non avrebbe alcuno scopo la conservazione di dati finalizzati alla tutela del patrimonio aziendale, una volta che i valori patrimoniali sono fissati definitivamente con la dichiarazione dei redditi ed il suo invio telematico.

Computer forensics aziendale: aspetti generali

Uno dei driver principali per la crescita di attività di Computer Forensics Aziendale è il fenomeno dei "white collar crime", nome specifico coniato negli USA nel 1939 da Edwin Hardin Sutherland, per definire i reati commessi da un dipendente di un'organizzazione privata o governativa, che gode di una posizione di fiducia. Genericamente, quindi, si definisce "white collar crime" il reato commesso da una persona di elevata onorabilità e classe sociale nel corso dello svolgimento del ruolo che ricopre durante le funzioni lavorative. Fino a qualche anno fa le aziende investivano in sicurezza IT dotandosi unicamente di sistemi di protezione da

attacchi esterni [143]. L'azienda considerava come minaccia solo la criminalità interaziendale, ovvero le aggressioni provenienti dall'esterno dell'organizzazione ad opera di outsiders. Di recente invece è stato accertato che oltre l'80% degli attacchi agli asset aziendali arrivano dall'interno. Le aziende hanno così iniziato ad investire nella protezione da criminalità intra aziendale, ovvero hanno iniziato a tenere presenti le minacce provenienti dall'interno dell'organizzazione ad opera di insiders. Il concetto di frode indica un atto compiuto per ledere un altrui diritto attraverso l'inganno: nel caso di frode aziendale, il significato è quello di un comportamento non violento che procura guadagno o beneficio, in modo illecito, causando un danno ingiusto, anche indiretto, ad altri. Si tratta quindi di azioni illegali che contemplano anche l'inserimento di istruzioni logiche nei computer aziendali al fine di ottenere benefici, attingendo dai capitali e dai beni prodotti dall'azienda. Le motivazioni ricorrenti per le quali dipendenti e dirigenti compiono frodi di varia natura nelle organizzazioni pubbliche o private di appartenenza, sono quelle viste nei paragrafi precedenti:

- il desiderio di arricchirsi e/o possedere l'oggetto che normalmente non ci si potrebbe permettere, ovvero il desiderio di realizzare con poca fatica le proprie aspirazioni;
- l'insoddisfazione e la frustrazione generate nell'ambiente di lavoro;
- il desiderio di equilibrare inconsapevolmente gli squilibri emozionali di un trattamento di lavoro considerato ingiusto;
- la non percezione delle conseguenze legali ed amministrative (denuncia, licenziamento, ecc) dell'eventuale rilevazione della frode commessa;
- l'idea di poter eludere ogni controllo relativo alle azioni commesse in azienda;
- l'errata consapevolezza che una piccola sottrazione non possa interessare a coloro che gestiscono business di ben più elevata portata;

- la mancanza di controlli sistematici nell'azienda, quindi la percezione che le frodi rilevate, siano state scoperte per puro caso e da ciò l'indiretta consapevolezza che il rischio che si sta per correre è realmente minimo, questo porta alla credere che il livello e la qualità del controllo interno sono facilmente superabili.

La disciplina della Computer Forensics applicata in un contesto aziendale può contribuire ad introdurre metodologie funzionali ad acquisire, preservare ed analizzare i referti (intesi come digital evidence), e competenze su come identificare ed analizzare delle prove che coinvolgono svariate tecnologie (hard disk forensics, network forensics, mobile forensics, ecc.) [122]. Inoltre tutto deve avvenire con la garanzia che l'informazione trattata sia autentica, integra, vera, completa, raccolta legalmente e, quando possibile, con metodologie ripetibili, in modo da poterla utilizzare in giudizio. Il primo passo da compiere da parte dell'azienda per poter garantire la riconducibilità delle azioni sui dati è quello di avere implementato correttamente un processo di Identity Access Management, in modo da garantire che gli accessi alle risorse aziendali avvengano realmente da persone fisiche certe. L'altro elemento indispensabile è la realizzazione di un sistema di log management che garantisca l'integrità dei dati e l'impossibilità che questi possano essere modificati manualmente da un amministratore di sistema. L'azienda deve poi emettere una serie di policy o normative interne che determinino i limiti all'uso promiscuo degli strumenti aziendali, in particolare l'uso degli strumenti elettronici (es. posta elettronica, utilizzo di pc fissi e/o portatili e cellulari/smartphone) assegnati per uso lavorativo, ma concessi in parte anche per uso personale. I dipendenti e i collaboratori devono essere consapevoli ed accettare che in casi gravi e di necessità l'azienda, a tutela degli interessi della stessa, può esercitare investigazioni, anche preventive difensive, sui suddetti strumenti di proprietà dell'azienda stessa. Il passo successivo è quello di

ufficializzare un gruppo di lavoro per la gestione dei casi/incidenti. Questo gruppo di lavoro è sempre composto da due organi, uno operativo e l'altro amministrativo, il primo composto dal fraud manager e se non presente un risk manager o internal audit, che deve essere affiancato da un tecnico esperto in computer forensics, e l'altro formato da hr (risorse umane) e ufficio legale. Questi due organi lavorano in team, in accordo con la rappresentanza sindacale presente in azienda, e comunque sempre nel rispetto della normativa che regola il rapporto di lavoro tra dipendenti e datori di lavoro. La parte operativa, che in azienda deve essere supportata da 4 elementi fondamentali che sono:

- Lettera di contestazione e dichiarazione dei dati personali sensibili presenti negli strumenti aziendali che stanno per essere sequestrate;
- Incarico per attività di computer forensics e autorizzazione al trattamento dei dati personali;
- Procedura operativa per identificazione, acquisizione, analisi e documentazione delle digital evidence;
- Modello di catena di custodia.

Il primo è indispensabile perché l'azienda non rischi di trattare dati personali sensibili del dipendente, in questo senso viene chiesto al dipendente di dichiarare entro un tempo limite quali eventuali dati personali sensibili sono presenti nello strumento aziendale che sarà oggetto di indagine. Il secondo elemento è fondamentale per permettere ad un consulente tecnico in computer forensics di iniziare il lavoro, in questo devono essere anche dichiarati gli obblighi di riservatezza e i limiti di applicabilità. il terzo è un prontuario delle best practice da tener presente come linea guida principale delle attività da seguire durante lo svolgimento della computer forensics. il quarto è indispensabile alla conservazione del reperto, è un documento che serve a tracciare tutti gli

spostamenti e gli accessi alla memoria digitale originale ed è parallela all'intero processo di cristallizzazione della fonte di prova e si estende anche al di là di esso.

Procedura operativa

La procedura operativa deve comprendere I seguenti step [85]:

- L'attività di computer forensics deve essere svolta solo dopo regolare incarico, accordo di segretezza (nda), manleva legale e autorizzazione al trattamento dei dati;
- L'attività di computer forensics deve essere svolta solo da personale certificato e con comprovata esperienza pluriennale;
- L'attività di individuazione e smontaggio dei reperti utili alle indagini deve avvenire in affiancamento con il fraud manager o risk manager o internal audit manager e deve essere ampliamente documentata fotograficamente;
- Il consulente tecnico nei diversi casi: acquisizione live o post mortem, dovrà agire seguendo le best practice internazionali;
- Dopo aver smontato le memorie da analizzare, il sistema deve essere acceso per registrare l'eventuale scarto orario del sistema acquisito, fase che deve essere documentata fotograficamente;
- Dopo aver individuato i media e le memorie utili alle indagini si deve iniziare a compilare il documento di catena di custodia;
- Il consulente tecnico, a meno che non effettui immagini raw in porzioni di file, deve aver precedentemente eseguito la cancellazione sicura dei dischi di destinazione, questa fase dovrà essere documentata (algoritmo di wipe) e riportata ella relazione finale;
- L'attività di acquisizione dei dati da analizzare deve avvenire, quando possibile, in modalità ripetibile, utilizzando write blocker hardware,

calcolando e verificando doppio l'hash e deve essere ampliamente documentata fotograficamente;

- Il reperto sequestrato deve essere custodito, insieme alla catena di custodia in cassaforte e/o in adeguato locale ad accesso riservato, ogni ulteriore accesso o spostamento deve essere riportato sul documento catena di custodia;
- La fase di analisi deve avvenire con software adeguato e ampliamente documentata, anche tramite screenshot, e riportata nella relazione finale;
- Al termine delle attività il consulente tecnico dovrà cancellare in modo sicuro (tramite tecniche di soprascrittura multipla "wipe") tutti i dati relativi al caso lavorato consegnando apposito verbale di cancellazione sicura dei dati;
- Tutte le attività elencate sopra dovranno essere effettuate in accordo con gli organi aziendali coinvolti preposti (hr, fraud manager, risk manager, internal audit, ufficio legale, ecc.).

Eventi oggetto di attività di computer forensics

Le tipologie di eventi oggetto di attività di computer forensics, specificamente quando tale attività venga attuata a livello aziendale, sono principalmente [35]:

- Eventi di violazione di politiche aziendali, ossia eventi che rappresentano una violazione di una regola aziendale formalizzata in una policy;
- Eventi illeciti, eventi cioè che costituiscono violazione di leggi e normative determinando una lesione o un pregiudizio grave nei confronti di beni e/o interessi (di cui l'azienda abbia la tutela, la proprietà o anche la disponibilità).

Violazione di policy

La violazione delle Policy può comportare, potenzialmente, l'attivazione di un'attività d'indagine forense interna, in particolare nei casi di uso improprio di:

- strumentazione elettronica aziendale;
- informazioni aziendali;
- credenziali di accesso ai sistemi aziendali.

Queste o altre tipologie di violazione possono ricadere anche nella generazione di un illecito:

- direttamente, in quanto una particolare violazione di una politica aziendale può configurarsi anche di per sé come "illecito";
- indirettamente, ad esempio nel caso di attacchi dovuti a worm / virus informatici, con danneggiamento dei sistemi informatici o sottrazione di dati. In questo caso la propagazione del malware potrebbe (ed in effetti questo è vero nella maggior parte dei casi) non essere frutto di un atto intenzionale, ma di una non sufficiente attenzione nell'applicazione delle norme interne attinenti all'utilizzo e/o alla gestione della strumentazione informatica.

Eventi illeciti

È complesso definire a priori gli eventi che possono richiedere l'esecuzione dell'attività forense, tuttavia è possibile definire le principali categorie di attività fraudolente, avremo quindi:

- Attività di Hacking eseguite verso i sistemi aziendali, eventualmente sfruttando punti di accesso privilegiati (insider);
- Furto d'informazioni riservate;
- Spionaggio industriale;
- Esecuzione di minacce dirette ai o provenienti dai dipendenti dell'azienda;

- Estorsioni o ricatti
- Frodi finanziarie o monetarie;

In caso di eventi illeciti, un'azienda si può trovare in differenti condizioni rispetto all'esecuzione dell'illecito stesso, ed in particolare:

- i sistemi aziendali hanno subito l'illecito;
- i sistemi aziendali sono stati utilizzati per perpetrare l'illecito (o come tramite dello stesso);
- i sistemi aziendali contengono informazioni relative ad un illecito (interno o esterno).

Per quanto concerne, in particolare, l'ultimo punto, occorre infine considerare che può essere richiesta attività di Computer Forensics anche in caso di indagini riguardanti illeciti tradizionali, come ad esempio in casi di rapine o reati sulla persona, ove l'analisi di evidenze digitali possa aiutare a chiarire il contesto in cui è avvenuto l'illecito.

Modalità di attivazione di una computer forensics

L'attivazione può avvenire a seguito di una richiesta proveniente dall'esterno dell'azienda, ad esempio da forze dell'ordine o società terze che richiedono l'esecuzione di una indagine a seguito di uno specifico evento, oppure in caso di illecito interno. A mero titolo esemplificativo, si può far cenno ai seguenti canali di attivazione:

- Segnalazioni anonime;
- Comunicazione e-mail o cartacea;
- Rilevazione alert legati al monitoraggio di sicurezza di determinati sistemi informatici;
- Segnalazioni provenienti dalle alter strutture o funzioni interne aziendali, come ad esempio la gestione del personale;

- Comunicazione o richiesta delle forze dell'ordine.

Il ruolo dei controlli interni

L'attuazione di controlli interni (continuativi, periodici o a campione) allargati a tutte le strutture aziendali si pone come importante presupposto per l'identificazione di eventi che possono portare al riconoscimento di un illecito. Infatti, un tale evento può verificarsi in un gran numero di differenti attività e processi aziendali [35]. Dovrebbe essere responsabilità di ogni funzione operativa aziendale porre in essere idonei sistemi di controllo per la prevenzione e l'individuazione di tali eventi, in quanto il sospetto di un evento illecito può sorgere nel corso della normale operatività produttiva ovvero a seguito di controlli.

Il ruolo delle segnalazioni degli utenti

Uno dei principali elementi che possono attivare una indagine interna è la denuncia, da parte degli utenti, di presunti illeciti. La segnalazione avvierà la fase preliminare nella quale il personale specializzato verificherà l'effettiva sussistenza dell'illecito. Una volta che questa sia accertata, verranno attivate le fasi successive. Si dovranno, comunque, considerare i seguenti aspetti:

- gli utenti dei sistemi aziendali, siano essi dipendenti o consulenti, dovrebbero essere messi nella condizione di riconoscere un illecito che si verifichi nel loro ambito di lavoro (ad esempio tramite momenti formativi);
- deve essere agevolata l'attività di segnalazione dei possibili illeciti, ad esempio attraverso la realizzazione di punti di contatto (email, call center, etc);
- la gestione delle segnalazioni degli utenti deve essere effettuata in modo strutturato, tenendo traccia di tutte le segnalazioni effettuate e delle

attività di analisi preliminare e di accertamento eseguite. In questo modo è possibile disporre di un archivio storico di tali informazioni, utile per successive attività di business security intelligence.

Riferimenti e richiami agli illeciti informatici

Una buona norma per il corretto utilizzo delle risorse informative aziendali dovrebbe definire le regole per l'utilizzo delle risorse informatiche da parte del personale aziendale, puntualizzando quelle che sono le attività illecite, le responsabilità e le modalità di utilizzo della strumentazione informatica. In particolare, dovrà essere opportunamente introdotto il concetto di reato definendone i comportamenti, come nell'esempio che segue:

Costituisce inoltre un reato la messa in atto di determinati comportamenti configurabili come crimini informatici, in particolare:

- la falsificazione di documenti informatici (art. 491 bis c.p.);
- l 'accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- la diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 quinquies c.p.).

Regole di utilizzo della strumentazione informatica

Occorre anche formulare opportune politiche inerenti l'utilizzo corretto delle risorse informative e informatiche aziendali, corredate di istruzioni operative e di linee guida per gli utilizzatori e per i gestori [4]. Ad esempio, nel caso di utilizzo di posta elettronica e Internet, a prescindere dalle specifiche norme operative, una policy interna potrebbe definire specifiche finalità associate all'utilizzo degli strumenti in oggetto da parte del personale, introducendo le seguenti linee generali di comportamento:

- La posta elettronica aziendale è uno strumento di lavoro che deve essere utilizzato dal personale aziendale al solo fine di svolgere le attività legate alle mansioni lavorative, salvo casi eccezionali di comprovata urgenza e necessità. Internet è uno strumento di lavoro che deve essere utilizzato dal personale aziendale al solo fine di svolgere le attività legate alle mansioni.

Modalità di raccolta delle informazioni

Una fase importante dell'attività investigativa interna riguarda l'identificazione e l'estrazione delle evidenze del sistema informatico attraverso il quale è stata eseguita l'attività illecita. In merito a questo, l'azienda dovrebbe chiarire, in una specifica policy, le informazioni a cui il team incaricato di seguire le attività di analisi della frode può avere accesso, e le modalità di conservazione. Ad esempio, una policy dovrebbe sottolineare che ai fini del conseguimento dei propri obiettivi il personale di (fraud management, internal audit) ha, nell'ambito del gruppo, libero accesso alle funzioni operative, alle norme e procedure aziendali, ai libri contabili ed alle relative evidenze di supporto, ai dati gestionali e di qualsiasi altro genere, ai locali, nonché libertà di effettuare interviste al personale, salvo quanto diversamente stabilito dalla legge [114].

Inoltre, con riferimento alla definizione e all'assegnazione delle utenze per l'accesso ai sistemi informativi ed alla relativa retention delle informazioni con lo scopo di conservazione delle evidenze, una policy dovrebbe richiamare quanto segue:

- I file di log inerenti agli accessi ai dati daparte degli utenti, devono essere tracciati, registrati e conservati ai fini della gestione degli incidenti di sicurezza.

Ai fini della conservazione delle evidenze:

- il periodo di tempo definito deve risultare idoneo a supportare futuri accertamenti e conforme alle normative vigenti;
- le modalità di conservazione dei dati raccolti devono garantire l'inalterabilità delle evidenze nel corso del tempo.

Modalità di collaborazione tra le strutture aziendali

Alcune politiche aziendali hanno l'importante obiettivo di definire e formalizzare le regole di cooperazione tra le strutture interne dell'azienda, al fine di agevolare i processi di riconoscimento di eventi illeciti e l'adozione di contromisure. Uno degli aspetti di maggiore rilevanza riguarda la necessità di una stretta collaborazione tra la funzione di indagine interna e quella ICT.

Indagine interna aziendale: case study

Nel presente paragrafo sarà trattato un caso tipo, evidenziando in particolare le fasi connesse alla gestione delle fonti di prova. Nella presentazione del caso saranno illustrate anche aspetti legati alla strutturazione di un report. In particolare, si illustreranno i passi di indagine preliminare e le risultanze emerse da essa, nonché il processo di indagine vero e proprio composto dalle due fase parallele di cristallizzazione della prova e redazione della catena di custodia, il tutto seguito dalla preparazione del report.

Analisi preliminare: presupposti per l'apertura di una indagine interna

L'analisi preliminare, svolta in generale a cura degli investigatori o auditor, permette in via generale di stabilire l'esistenza dei presupposti per l'apertura di un caso di frode interna. Nel particolare esempio considerato, si tratta di un invio massivo di e-mail verso molteplici caselle aziendali, come spiegato nella seguente sezione del report.

Attività svolta	Note
SEGNALAZIONE DELL'ILLECITO AZIENDALE In data XX/XX/XXXX è stato effettuato un invio massivo di messaggi di posta elettronica (c.d. spam) non per finalità lavorative ma con l'intento di diffondere un messaggio relativo a _____. Per tale motivo veniva richiesto alla funzione di sicurezza aziendale competente di svolgere accertamenti tecnici in modo da poter identificare l'autore dell'invio della email.	La segnalazione è giunta all'attenzione Della sicurezza aziendale, in quanto l'invio del messaggio di Spam era diretto a tutte le caselle e-mail aziendali.

Fin dalle prime analisi, è apparso indispensabile verificare se l'e-mail di spam fosse stata inviata dai sistemi interni aziendali o meno. A tal fine, è stato analizzato il messaggio di posta, al fine di verificare se questo sia stato mandato attraverso i server aziendali oppure se proveniente dall'esterno del perimetro aziendale. È stata effettuata una preliminare analisi delle informazioni disponibili, ovvero l'e-mail di spam oggetto di segnalazione, identificando che i server dai quali era stata inviata erano effettivamente quelli aziendali. Tale evento è stato ritenuto sufficiente per definire l'apertura del caso. In particolare, data la natura dell'evento (spam), una fonte di prova idonea a stabilire l'opportunità di attivazione di un caso è stata facilmente reperita su una delle postazioni di lavoro che ha ricevuto il messaggio. La procedura di estrazione di una e-mail deve in generale preservare non solo il testo del messaggio ma anche informazioni di sistema rilevanti, quali:

- La data e l'ora di spedizione del messaggio (la quale potrebbe non coincidere con la data di ricezione);

- L'account di posta utilizzato per l'invio del messaggio (tenendo conto che questo potrebbe essere falsificato e quindi non costituisce necessariamente un'evidenza valida);
- I server utilizzati per l'invio del messaggio.

Per fare questo è necessario estrarre il messaggio nella sua interezza. In taluni casi (come quello trattato), può ritenersi eccessivo eseguire l'intero backup del sistema, in quanto il dato era contenuto all'interno del database delle mail. Si è quindi deciso di eseguire un'estrazione parziale del contenuto del disco, focalizzandosi sulla mail di spam. Le attività di colui che investiga, in un caso simile, sono le seguenti:

- eseguire o supervisionare l'attività di estrazione della mail dal sistema e verificare che i dati estratti coincidano esattamente con quelli sul sistema (attraverso l'utilizzo di tecniche di Hashing);
- realizzare il verbale relativo all'attività di estrazione nel quale si descrivono passo dopo passo le operazioni eseguite, possibilmente supportando l'attività da foto significative, ad esempio per certificare l'ora di estrazione del messaggio;
- eseguire la cristallizzazione della prova, in questo caso all'interno di un cd rom;
- realizzare la catena di custodia e sigillare la fonte di prova.

Processo di indagine

In una attività investigativa, la ricerca delle evidenze è un processo ciclico, a partire dall'elemento che provoca l'attivazione del caso fino alla formulazione del quadro globale, passando attraverso fasi di ricerca delle fonti di prova, cristallizzazione delle stesse e successiva analisi. Oltre ai vari passi che portano

alla cristallizzazione delle fonti di prova (riconoscimento, acquisizione e conservazione/protezione) si affianca la redazione della catena di custodia. Nel seguito il procedimento è applicato al caso in esame.

Ricerca di fonti di prova

In generale, l'attività di analisi preliminare delle evidenze immediatamente disponibili deve mirare, data la particolare natura del dato informatico e le specifiche modalità di diffusione, anche ad identificare le varie infrastrutture tecnologiche aziendali che possano recare tracce ulteriori dell'accaduto, come illustrato nella sezione del report di seguito mostrato:.

Attività svolta	Note

RICERCA FONTI DI PROVA Per quanto riguarda la metodologia di tracciamento di un 'e-mail, appare di rilievo evidenziare che particolare cura dev'essere posta nel verificare e riscontrare ogni elemento o dato di cui si viene a conoscenza, utilizzando reperti e digital-evidence presenti su altri sistemi informatici aziendali. Difatti, come è noto, tutto ciò che accade in una rete di computer non lascia traccia solo nel sistema in cui si è verificato l'evento ma, quasi sempre, vi sono informazioni registrate su altri sistemi per esigenze diagnostiche e/o di governo del sistema.	Si sottolinea la necessità di raccogliere le evidenze digitali o fonti di prova legate all'attività che ha prodotto l'illecito, allargando quanto più possibile il campo di ricerca

Nel caso in esame, l'e-mail di spam disponeva di un mittente associato ad una casella di posta elettronica impersonale. Analizzando i log dei server di posta, è stato possibile identificare l'ora esatta dell'invio del messaggio di spam e determinare che effettivamente la mail provenisse dal mittente presente nell'indirizzo indicato nella stessa. L'estrazione dei log dal server, costituendo tale dato una possibile fonte di prova, è stata svolta secondo specifiche modalità di computer forensics (opportunamente adattate al diverso contesto operativo). Le caselle impersonali possono tuttavia essere accedute da differenti soggetti e postazioni di lavoro, pertanto l'analisi effettuata sui server di posta non è stata

sufficiente per determinare da quale sistema è stato effettivamente eseguito l'illecito. Si è quindi proceduto ricercando ulteriori informazioni, ovvero incrociando i dati disponibili e cercando chi, nel momento dell'invio della mail di spam, fosse "registrato" come "connesso" all'interno dell'Active Directory aziendale. Tale analisi portava all'identificazione di due sistemi che rispettavano i requisiti descritti e che permettevano di risalire (attraverso l'indirizzo IP) alle postazioni da cui probabilmente proveniva il messaggio di spam. Tali informazioni venivano ritenute sufficienti a procedere con la ricerca di evidenze probatorie direttamente sui sistemi degli utenti (tema delicato, secondo quanto illustrato in precedenza).

Cristallizzazione delle fonti di prova

Alcuni dati, potenziale fonte di prova, potrebbero essere contenuti all'interno del disco delle postazioni di lavoro. Per tale motivo è opportuno procedere con l'analisi dell'hard disk, previa sua duplicazione. L'incaricato dell'indagine ha preceduto quindi con l'acquisizione delle evidenze secondo le modalità forensi definite nelle policy aziendali, con particolare riferimento alla modalità di acquisizione ritenuta più opportuna (in questo caso, appunto, la duplicazione). Seguono alcune parti del report, relativi all'identificazione, all'acquisizione e alla verifica del reperto classificato.

Attività svolta	Note

IDENTIFICAZIONE DELLA POSTAZIONE In data____, con il supporto tecnico di _____, veniva cristallizzato l'hard disk identificato con indirizzo IP_____	Esistono diversi livelli di identificazione. (In questo esempio la Postazione di Lavoro e successivamente il supporto di storage).
IDENTIFICAZIONE DELLA FONTE DI PROVA Trattasi del materiale di proprietà di (azienda _____). In particolare il materiale in analisi risulta così composto: - Numero _____ Hard Disk di _____, etichettato ____, i cui dettagli e relativi serial number sono: HD I : Hard disk [...] - [...] - da [...] GB - SIN: [...]	Vengono Riportate le informazioni contenute anche nella Catena di Custodia relative alle prove, per consentire il riferimento.

ACQUISIZIONE È stata realizzata una forensic image (copia) dell'hard disk originale, consentendo in un secondo momento di effettuare una medesima attività a riscontro delle risultanze investigative. Tale procedura, a differenza della mera copia, consente di operare su una bit stream image dell'originale. È necessario, però , effettuare tale operazione con idonei strumenti che consentano di mantenere inalterata la traccia informatica oggetto dell'analisi. L'immagine è stata eseguita utilizzando il software_____che consente l'acquisizione, senza possibilità di modifica dell'originale, di un hard disk o di qualsiasi altro supporto di memorizzazione collegato al sistema. Tale software, prodotto da _____, destinato all'uso professionale ed investigativo da numerose agenzie e forze dell'ordine in tutto il mondo, è considerato in linea con gli standard internazionali per le analisi delle tracce informatiche. 128	L'acquisizione deve essere effettuata secondo le modalità più opportune e in conformità alle best practice del settore.

Attività svolta	Note
VERIFICA L'hard disk contrassegnato come _____ non risulta danneggiato e pertanto è stato possibile calcolare le firme di HASH nella modalità normalmente utilizzata, ovvero sia sul supporto originale che sulle immagini, per poi verificarne la coincidenza. File Integrity: Verifica Completata, O Errori Acquisition Hash: 3A1F4503744A50E3739F59C862935747 Verify Hash: 3A1F4503744A50E3739F59C862935747 Si evidenzia che le firme calcolate risultano uguali.	È necessario effettuare una verifica di congruenza tra l'originale è il duplicato, prima di procedere alle attività di analisi

Redazione della catena di custodia

Alla cristallizzazione di ogni fonte di prova, si affianca la redazione della catena di custodia. Segue un esempio per uno specifico elemento probatorio.

REDAZIONE DELLA CATENA DI CUSTODIA PER LA SPECIFICA FONTE DI PROVA Per documentare la "Chain of Custody" sono state effettuate delle fotografie informato digitale di tutte le attività tecniche, precisamente: La postazione cristallizzata (esterno ed interno) Clone ed acquisizione dell'hard disk tramite il dispositivo Logicube: 	In questo caso, il report sostituisce la catena di custodia

Analisi delle fonti di prova

Le informazioni digitali acquisite sono state analizzate con l'obiettivo di identificare eventuali tracce che potevano ricondurre alla creazione del messaggio di posta elettronica, oggetto delle indagini interne. in particolare, veniva ricercata all'interno delle e-mail inviate dall'utente titolare della postazione di lavoro la presenza del messaggio di spam "originale". Nel caso in cui il messaggio fosse stato cancellato, sarebbe comunque possibile, grazie a strumenti specifici di computer forensics, identificare porzioni di file utili a fornire elementi probatori, come specificato anche nel report esemplificativo di seguito indicato.

Attività svolte	Note
ANALISI DEI REPERTI ACQUISITI L'accertamento tecnico, eseguito sul materiale sopra descritto, era mirato all'individuazione, su tale supporto di memoria, di eventuali informazioni (anche non visibili con normali tecniche di consultazione dello stesso), che potessero contribuire a chiarire la posizione di _____, in relazione all 'incarico ___.	Nel report deve essere riportato il processo di analisi delle evidenze probatorie.

Preparazione del report

Il report deve essere redatto utilizzando le informazioni raccolte e preferibilmente secondo un template aziendale. Il template standard dovrebbe incorporare diverse sezioni:

- Una prima sezione (dati sintetici), dove si riportano gli aspetti di maggiore rilevanza riguardanti il caso ed il contesto di riferimento identificando, ad esempio, le strutture interessate, la figura richiedente l'attività di computer forensic o il soggetto leso e quindi una breve descrizione dell'evento;
- Segue la descrizione delle attività di analisi vera e propria, nella quale viene illustrato il caso, sono ripercorse le attività svolte e si riporta la ricostruzione dell'accaduto. La presentazione dei fatti deve essere metodica e rigorosa, in modo tale che l'analisi effettuata sia ripetibile a partire dalle indicazioni fomite, e porti ai medesimi risultati. La ripetibilità dell'analisi e la trasparenza nelle attività svolte attribuisce al report l'effettiva validità in sede giudiziaria;
- Nel capitolo relativo alla conclusioni e proposte si devono identificare le responsabilità, i danni accertati legati all'evento illecito analizzato ed eventuali considerazioni aggiuntive;
- La sezione Allegati consentirà di integrare l'analisi presente nel report con informazioni aggiuntive e di dettaglio riguardanti i vari aspetti dell'analisi forense (ad esempio il verbale di acquisizione della prova, le analisi effettuate dal laboratorio, ecc.).

Si osservi come, nelle parti conclusive, sia presente la possibilità di fornire indicazioni alle strutture interessate, anche ai fini di mitigare il rischio di un ripetersi dell'illecito accertato, o di renderne più facile l'identificazione. Nel caso in esame potrebbe suggerirsi, ad esempio, un irrobustimento di alcuni log infrastrutturali, come si evince dalla seguente porzione del report:

Attività svolte	Note

INDICAZIONI ALLE STRUTTURE INTERESSATE Come emerso durante le attività investigative, il sistema di data retention non consente una diretta correlazione tra l'utente autorizzato ad inviare un'e-mail da una casella di gruppo ed il messaggio in oggetto. Alla luce di quanto sopra, si richiede l'immediata cancellazione dei contenuti illeciti ed un controllo su eventuali connessioni esterne in Peer to Peer con la supervisione dell'ufficio Sicurezza Aziendale . Pur essendo il contenuto della mail in oggetto non particolarmente critico, appare necessario definire e circoscrivere gli ambiti relativi al data retention, evitando in tal modo il ripetersi di un fenomeno fuori controllo che potrebbe risultare dannoso per l'azienda.	Indicazioni alle strutture interessate, che possono essere di natura generale, relative a possibili cambiamenti di approccio o all'esecuzione di attività di prevenzione specifiche.

In conclusione, si noti come la redazione di report relativi ai casi di illecito secondo un formalismo comune e con l'utilizzo di un template standard, favorisce le attività di analisi su casi futuri e vada nella direzione di predisporre strumenti e metodologie a supporto di una più efficace attuazione della business security intelligence. Tale prassi favorisce, inoltre, il tracciamento dei casi mediante sistemi informatici, e permette di predisporre strumenti per l'assistenza al personale addetto nella generazione della documentazione

2. FRAUD MANAGEMENT NELL'INFORMATION AND COMMUNICATION TECHNOLOGY

La seconda parte di questa stesura approfondisce il tema delle frodi nell'area dell'Information e Communication Technology. Nello specifico verrano presi in considerazione alcuni settori industriali nei quali si caratterizzano in modo peculiare le modalità di attuazione, ed in cui sono altrettanto particolari le soluzioni implementate per la prevention, la detection ed il contrasto delle frodi. Come si vedrà, l'Information and Communication Technology costituisce in questi contesti il punto di attacco e lo strumento di difesa allo stesso tempo. I settori analizzati sono i seguenti:

- Banche ed istituzioni finanziarie, che, trattando denaro quale oggetto principale della propria attività, ed essendo questo ed altri beni finanziari al giorno d'oggi declinati all'atto pratico mediante transazioni digitali, si caratterizzano come ambito privilegiato di azione per attività fraudolente;
- Telecomunicazioni, in quanto il passaggio dalle tecnologie analogiche a quelle digitali da una parte, e le politiche commerciali aggressive adottate dai diversi player dall'altra, rendono tale mercato una delle aree privilegiate per l'attuazione di attività fraudolente, caratterizzate da complessità e rapidità sempre crescenti;

- Assicurazioni, ed in particolare il ramo auto che vede una percentuale molto elevata di sinistri denunciati in modo fraudolento la cui parte più rilevante non è scoperta dalle compagnie;
- Gaming, un mercato in rapida crescita e di notevole interesse per il tema in oggetto in quanto la possibilità di nascondere la propria identità nel contesto dell'online gaming in particolare, rende tale ambito un terreno ideale per attività fraudolente e criminali;

Tale vista per settore è inoltre integrata con l'analisi dei principali servizi di pagamento (Online, Mobile, Carte di credito), trasversali ai settori di mercato, al fine di evidenziarne le principali caratteristiche in termini di tipologia e di possibili modalità di contrasto.

Unire le esperienze maturate in settori così diversi è uno degli obiettivi di questa stesura: la criminalità è veloce a trasferire le modalità operative da un settore ad un altro quando queste si dimostrano efficaci, per questo la condivisione delle esperienze nel contrasto può aiutare a rendere più efficaci le tecniche di contrasto messe in campo.

2.1 Frodi e banche

Nel mondo delle Istituzioni Finanziarie, le frodi possono essere raggruppate in due categorie principali [145]:

- Le frodi aziendali, condotte da soggetti interni o esterni a danni dell'istituzione stessa;
- Le frodi sui servizi, condotte da soggetti esterni ai danni delle Istituzioni Finanziarie. Le principali modalità avvengono mediante la falsificazione di identità, il furto di identità e la manomissione o alterazione degli strumenti di pagamento.

Le frodi aziendali

L'ambito bancario offre per la sua particolarità diverse possibilità per perpetrare una frode. Accanto alle normali frodi, tipiche di ogni azienda, quali ad esempio la non corretta gestione degli appalti di fornitura, le frodi di carattere amministrativo, l'uso illecito di strumenti e attrezzature da parte dei dipendenti, etc., possono essere effettuate diverse tipologie specifiche ai danni della banca, dei clienti, di terzi [145].

Una delle possibili frodi riguarda la non corretta applicazione di pratiche commerciali da parte dei dipendenti a danno sia dei clienti, sia della banca (a favore o meno della controparte).

Per la rete commerciale è possibile mettere in atto pratiche non corrette nei confronti della clientela per raggiungere il budget commerciale: un possibile caso riguarda l'esecuzione di disinvestimenti da prodotti anche più favorevoli per il cliente per indirizzarli su uno specifico prodotto. Per il medesimo fine, analoga pratica può essere condotta ai danni della banca, ad esempio concedendo fidi e mutui sopravvalutando ad arte le garanzie prestate [147]. Il beneficio ottenuto per chi esercita queste pratiche scorrette può derivare da un incentivo economico e di carriera. Altre attività che possono essere messe in atto dai dipendenti possono riguardare ad esempio il cambio di un assegno di un'altra banca per contanti, il cambio di banconote false, il cambio di assegni contraffatti, la compravendita di titoli per contanti, le operazioni per cassa etc, senza dimenticare la disponibilità di sistemi informativi che consentono l'accesso a grandi quantità di dati, consentendo a molti dipendenti di effettuare con facilità estrazioni che possono essere cedute a terzi. In particolare, chi gestisce i sistemi informativi dispone di una posizione privilegiata per l'attuazione di tali frodi, nonostante la stringente regolamentazione di settore e i controlli posti in essere a protezione dei dati.

Le frodi sui servizi

l'appetibilità delle istituzioni finanziarie per i frodatori risiede principalmente nel fatto che trattano il denaro come oggetto principale della loro attività. Non c'è quindi da meravigliarsi che siano stati sviluppati, nel corso dei secoli e soprattutto nel corso degli ultimi anni, con le moderne tecnologie informatiche, innumerevoli metodi e sistemi di frode. Le principali tecniche di conduzione di frodi sui servizi sono [146]:

- La manomissione o alterazione dello strumento di pagamento, il cui caso più diffuso è ad esempio la clonazione delle carte di pagamento. Le perdite legate al fenomeno solo in UK nell'ultimo decennio ammontano ad oltre 500M€/anno [150]
- Falsificazione o furto dell'identità fisica: cioè il ricorso a documenti falsi o contraffatti per aprire nuovi rapportidi pagamento, che possono essere poi utilizzati dai truffatori per monetizzare. Per condurre tali frodi si utilizzano generalmente documenti sottratti a terzi oppure della documentazione falsa;
- Furto di identità digitale: la sottrazione dell'identità digitale della vittima, l'insieme di codici pin e password utilizzate per l'autenticazione da remoto, al fine di effettuare operazioni di pagamento. Caso più diffuso è la sottrazione dei dati di accesso all'internet banking (ad esempio mediante tecniche di phishing, social engineering, oppure il ricorso a virus informatici denominati trojan);

Soluzioni per la prevenzione, la detection e il contrasto delle frodi in ambito bancario

Relativamente alle frodi sui servizi, sta diventando di primaria importanza il tema del furto di identità, sia essa documentale che digitale. Le soluzioni adottate per

combattere le frodi si possono generalmente dividere in soluzioni preventive e soluzioni reattive [150].

Soluzioni preventive

Comprendono tutte le soluzioni che dovrebbero permettere di bloccare un tentativo di frode prima che vada a buon fine. Fanno parte di questa categoria le soluzioni di:

- Fraud Prevention: sono i sistemi che sono in grado verificare se da un certo dispositivo si stia manifestando un comportamento anomalo, indice di un tentativo di frode;
- Meccanismi di autenticazione: sono soluzioni che proteggono l'accesso ai servizi, in particolare di e-banking, quali le diverse soluzioni di strong authentication (ad esempio token, certificati digitali, sistemi biometrici, come grafometria e voce);
- Formazione/Awareness: le diverse iniziative che le banche mettono in campo nei riguardi della clientela e di tutti i livelli organizzativi interni, al fine di aumentare la consapevolezza ed il livello di attenzione sulle minacce e i relativi rischi di frode, sono uno degli aspetti fondamentali da tenere presente in un piano globale di prevenzione delle frodi;
- Verifiche documentali: insieme di controlli finalizzati ad individuare false identità, complete o parziali, che possono essere create a partire da documenti.

Soluzioni reattive

Comprendono tutte le soluzioni che permettono di identificare eventi anomali, indice di utilizzo fraudolento del servizio:

- Monitoraggio Transazioni: soluzioni che, in funzione di vari parametri (dati transazione, comportamento dell'utente, geolocalizzazione, analisi del device, etc…) permettono di definire un livello di rischio di una transazione e conseguentemente attuare determinate azioni (dal richiedere un'autenticazione più forte fino al blocco della transazione stessa);
- Information Discovery: sono sistemi che, esplorando e analizzando liberamente dati strutturati e non strutturati, provenienti dalle fonti più disparate (ad esempio i dati delle transazioni, contratti di attivazione, customer care, fonti aperte da social network) permettono attraverso l'uso di tecniche di data mining, di correlare fra loro vari fenomeni in modo da identificare eventi anomali;
- Monitoraggio accessi a basi dati: il monitoraggio dell'accesso alle informazioni strutturate presenti in azienda può permettere di individuare comportamenti anomali che possono essere indicatori di frode e meritano un'analisi di dettaglio da parte degli organi di controllo della banca;
- Collaborazione con le forze dell'ordine: il continuo scambio di informazioni tra la banca e le forze dell'ordine è uno strumento indispensabile per aumentare l'efficacia delle varie attività di prevenzione e di repressione.

Riferimenti normativi

Sono presenti numerosi riferimenti normativi, sia a livello Europeo che a livello di normativa italiana. A livello Europeo, particolare rilevanza hanno le recenti "Raccomandazioni per la sicurezza dei pagamenti internet", emanate dalla Banca Centrale Europea (BCE), che rispondono alla necessità di incrementare la fiducia dei consumatori verso tale mezzo di pagamento ed il conseguente utilizzo, rendendo omogenei i livelli di sicurezza delle operazioni di pagamento effettuate su internet. Le raccomandazioni chiedono alle istituzioni finanziarie di

incrementare i presidi di sicurezza su ambiti di governance, su quelli di controllo e monitoraggio e su meccanismi e soluzioni di prevenzione frodi. Meno recente, ma sempre attuale, è la Direttiva Europea 2007/64 (PSD) [150], che si pone l'obiettivo di facilitare la creazione di un mercato unico dei pagamenti in euro normando il mercato dei sistemi e dei servizi di pagamento elettronico, favorendo lo spirito innovatore e declinando i nuovi strumenti in opportunità di business, incrementando la tutela dell'utente, migliorando la trasparenza delle condizioni e l'accessibilità alle informazioni, standardizzando i diritti, gli obblighi e i requisiti informativi in capo sia all'utente sia ai prestatori di servizi di pagamento, favorendo un'azione per rendere maggiormente efficienti i servizi ai clienti finali (ad esempio la riduzione dei tempi di esecuzione delle transazioni), ed infine migliorando al contempo le dinamiche di mercato (ad esempio la pressione sui prezzi, l'apertura a nuovi player).

A livello nazionale, si segnalano le recenti disposizioni di vigilanza prudenziale per le banche (circolare n° 263 del 2/7/2013) di Banca D'Italia, che mirano a promuovere il rafforzamento della capacità delle Istituzioni Finanziarie di gestire i rischi aziendali [146]. Tra i vari elementi viene richiesto che le procedure operative e di controllo debbano, tra l'altro, minimizzare i rischi di attuazione di frodi o di casi di infedeltà dei dipendenti.

Il DLgs. 231/2007, art. 55, comma 9, invece, disciplina la fattispecie di chi, al fine di trarre profitto per sé o per altri utilizza indebitamente, non essendone titolare, carte di credito o di pagamento per l'acquisto di beni o alla prestazione di servizi e di chi falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo, che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi. Con il DL n. 93 del 14 agosto 2013 convertito nella legge 119 il 15 ottobre 2013, sono state introdotte, tra le altre, alcune novità in tema di frode informatica con sostituzione di identità digitale e falsificazione di

carte di credito. Le fattispecie di reato citate, infatti, entrano a far parte dell'elenco dei reati presupposto che fanno scattare la responsabilità amministrativa degli enti ai sensi del d.lgs. 231/2001 [147].

Il ROI delle misure antifrode nelle banche.

Tra il 1943 ed il 1954 lo psicologo statunitense Abraham Maslow studiò approfonditamente il comportamento umano e teorizzò la famosa "piramide dei bisogni", secondo la quale l'individuo si realizza soddisfacendo via via bisogni sempre più sofisticati. Maslow indivuiduava così vari stadi, che devono essere soddisfatti in modo progressivo [64]. Il bisogno di sicurezza è al secondo stadio, ovvero appena al di sopra dai bisogni fondamentali, quelli fisiologici. Quindi è come dire che dopo che ci siamo assicurati di respirare e di alimentarci, della sicurezza non possiamo fare a meno e, come tutti i bisogni primari, è considerata una commodity, qualcosa che è naturale debba esserci. Inoltre, come tutto ciò che è normale debba esserci, ci si aspetta che abbia un costo non alto, e questa rappresenta una prima criticità, quella culturale [59]. La difficoltà principale nello stimare il ritorno dell'investimento risiede nell'aspetto che è forse quello che stupisce di più: pochi fra i soggetti frodati sono stati in grado di indicare il danno tempestivamente. Valutare un ritorno di investimento necessita di numeri: con semplicità, il ROI= return of investment. Il costo dell'investimento è certo o quantomeno evidente, mentre il valore ottenuto, che si manifesta in una riduzione del danno subito, senza considerare il danno reputazionale, non può avvalersi di dati sistematici. Una seconda criticità è quella attitudinale. L'investimento in prevenzione è un investimento nella riduzione del rischio, ed il rischio è intrinsecamente controintuitivo. Non si può imporre il cambiamento all'inclinazione individuale, ma si può agire su alcune leve di consapevolezza. La

terza criticità è quella della semidecidibilità. Definendo il rischio con una semplice (e semplicistica) formula [33]:

R = P x I,

ovvero il prodotto della probabilità di accadimento di un evento moltiplicata per l'impatto che si avrebbe nel caso in cui si verificasse, risulta chiara la rilevanza della componente probabilistica. La semidecidibilità non è risolubile, è parte intrinseca del concetto di rischio che annovera l'incertezza negli eventi futuri, anche possedendo ampie serie storiche. Il fatto di non essere risolubile però non significa che un rischio non sia calcolabile. Valutare il ritorno dell'investimento è quindi fattibile: basta rimuovere le quattro criticità, l'ultima delle quali è la leva numerica.

Criticità	Indicazioni
Cultura	Informazione quantificata e circostanziata. Un numero, anche se impreciso, colpisce.
Formazione	Non viene sempre erogata e quando si parla di rischio c'è un'obiettiva difficoltà: gli argomenti sono complessi.
Attitudine	Quando si subiscono incidenti, informare con il reporting.
Semidecidibilità	Calcolare anche in modo semi-quantitativo le probabilità di accadimento e gli impatti, in modo tale da avere comunque un numero, anche di scoring, con il quale poter valutare il ROI. Cultura e attitudine agiscono sulla comprensione e accettabilità delle valutazioni.

Valutare il ritorno dell'investimento

La prima difficoltà che si incontra nel valutare il ritorno degli investimenti è quella di non disporre di dati economici esaustivi che quantifichino i danni ed i costi relativi. Per superarla è necessario considerare elementi quantitativi conosciuti a scopo di confronto con i quali creare una matrice di valutazione applicabile. A titolo di esempio, estratto semplificato di un'esperienza reale, viene qui descritto il processo di valutazione "as is" del rischio inerente delle componenti del sistema informative riguardo alle frodi per mezzo di furti di informazione perpetrati tramite accesso non autorizzato ai dati [21]. Il processo si sviluppa in più fasi, di cui la prima può essere scomposta in tre passi:

1. In prima istanza si può definire la scala dei criteri con la quale posizionare l'applicazione dal punto di vista della criticità;
2. Successivamente, si procede con l'attribuzione a ciascun criterio dei "pesi" con i quali l'algoritmo di scoring ponderato valuterà il posizionamento di rischio dell'applicazione in esame;
3. Infine, tramite valutazione degli elementi oggettivi disponibili, si può ottenere uno scoring che rappresenta il punteggio di rischiosità. E' un elemento quali-quantitativo, ma oggettivo.

Anche la seconda fase prevede diversi passaggi. Innanzitutto, al posizionamento di rischiosità, ottenuto con la prima fase, si può associare una valutazione degli impatti conseguenti ai rischi valutati. Sarà quindi possibile ipotizzare un intervento di prevenzione che incida sul posizionamento attuale (ad esempio censendo e crittografando completamente tutte le informazioni riservate e svolgendo sempre e con periodicità definita i penetration test) e valutare la riduzione conseguente dello scoring di rischio. Questa valutazione sarà quindi ripetuta per diversi interventi ipotizzabili. Il rapporto fra lo scoring risultante nell'ipotesi di attuare gli interventi individuati e lo scoring iniziale rappresenta una valutazione dell'efficacia

attesa dell'investimento in prevenzione. Moltiplicata per la griglia di impatti offre una valutazione oggettiva, seppur stimata, dei benefici attesi. L'ultima fase è di ulteriore miglioramento del risultato raggiunto. Se si dispone di informazioni quantitative attendibili e complete anche esterne la stima può, infatti, beneficiare di ulteriori elementi di valutazione.

E' però disponendo di serie storiche che si può stimare il ROI in un modo in cui il rischio può essere espresso matematicamente, costruendo la distribuzione di probabilità e valutando l'esposizione di impatto intercettando la curva di distribuzione al valore di confidenza desiderato (ad esempio, l'esposizione al 99,9% di confidenza) [45].

A questo punto moltiplicando l'esposizione al livello di confidenza desiderato per il rapporto di rischiosità pre e post interventi si otterrebbe quanto l'investimento in prevenzione abbatterebbe l'esposizione al rischio, quantificando in tal modo, in generale economicamente non solo in termini di danno materiale subito ma anche in termini di costi indotti quali inefficienze e riduzione di livelli di servizio anche contrattualmente garantiti, il ritorno dell'investimento.

2.2 Il rischio operativo e frode in banca – il caso Intesa San Paolo Personal Finance

In questo paragrafo sarà analizzata una realtà particolare del mondo bancario, quella di Intesa San Paolo Personal Finance, rispetto all'evoluzione che ha subito nel corso degli ultimi decenni, passando da una realtà orientata principalmente al concetto di rischio di credito a quello di un approccio organico nella gestione dei rischi. Questo processo è avvenuto in maniera graduale, partendo dai primi anni novanta, in cui il mondo bancario si è rivolto con rinnovata attenzione al problema della gestione e misurazione del rischio di credito, passando da una situazione in cui le banche perdevano soldi da clienti inadempienti, ad una in cui la domanda

alla quale rispondere è “Cosa e quanto si perde?” e “Perchè i clienti non pagano?” [146].

Negli anni duemila si è definitivamente preso coscienza di questo, ed una prima risposta è stata quella di classificare le vari tipologie di rischi, cercando delle regole condivise per evitare le perdite. Viene di seguito elencata una classificazione dei rischi in questo settore di mercato:

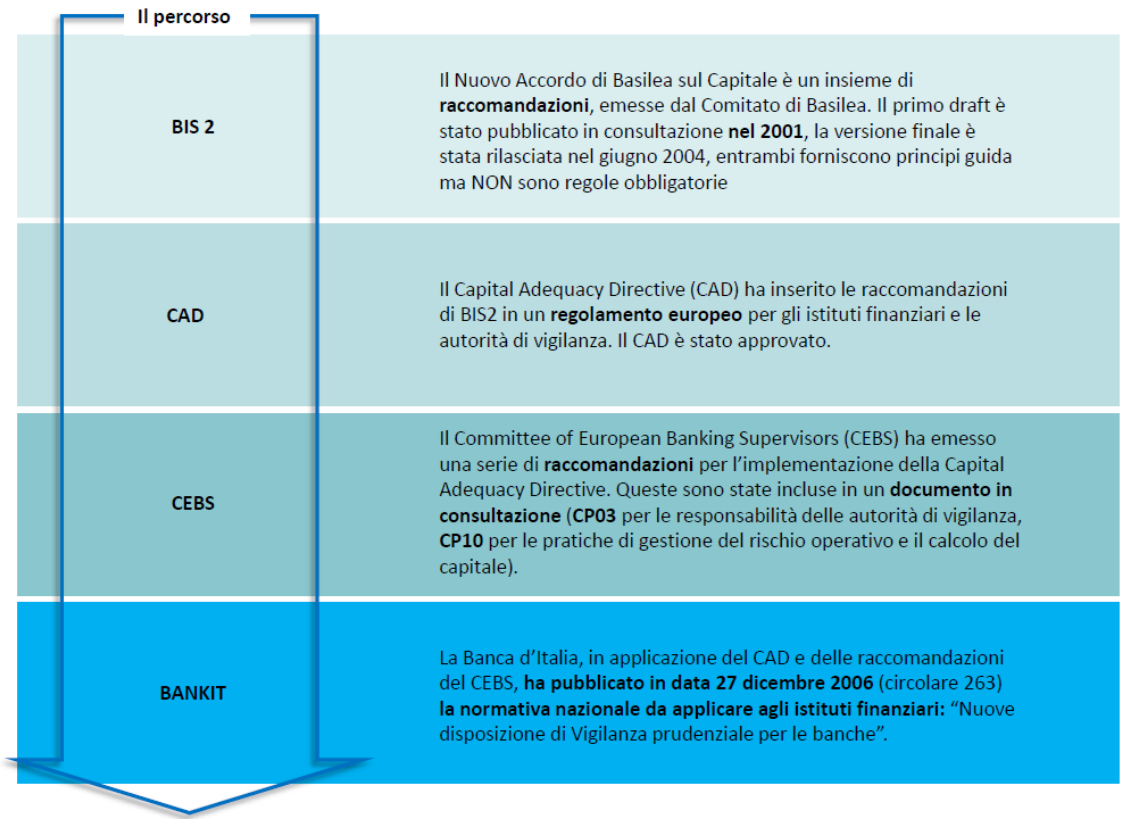
- Rischio di credito: per rischio di credito si intende la possibilità che una variazione inattesa del merito creditizio di una controparte, nei confronti della quale esiste un’esposizione, generi una corrispondente variazione inattesa del valore di mercato della posizione creditoria;
- Rischio operativo: per rischio operativo si intende il rischio di subire perdite derivanti dall’inadeguatezza o dalla disfunzione di processi, risorse umane e sistemi interni, oppure da eventi esogeni. Rientrano in tale tipologia, tra l’altro, le perdite derivanti da frodi, errori umani, interruzioni dell’operatività, indisponibilità dei sistemi, inadempienze contrattuali, catastrofi naturali. Nel rischio operativo è compreso il rischio legale, mentre non sono inclusi quelli strategici e di reputazione;
- Rischio legale: il rischio di perdite derivanti da violazioni di leggi o regolamenti, da responsabilità contrattuale o extra-contrattuale ovvero da altre controversie;
- Rischio Strategico: il rischio di perdite dovuto a cambiamenti del contesto operativo o a decisioni aziendali errate, inadeguata attuazione di decisioni, scarsa reattività a variazioni del contesto competitivo, ad esempio inversione del ciclo economico;
- Rischio reputazionale: il rischio attuale o prospettico di flessione degli utili o del capitale derivante da una percezione negativa dell’immagine

dell'azienda da parte di clienti, controparti, azionisti dell'azienda, investitori o autorità di vigilanza;

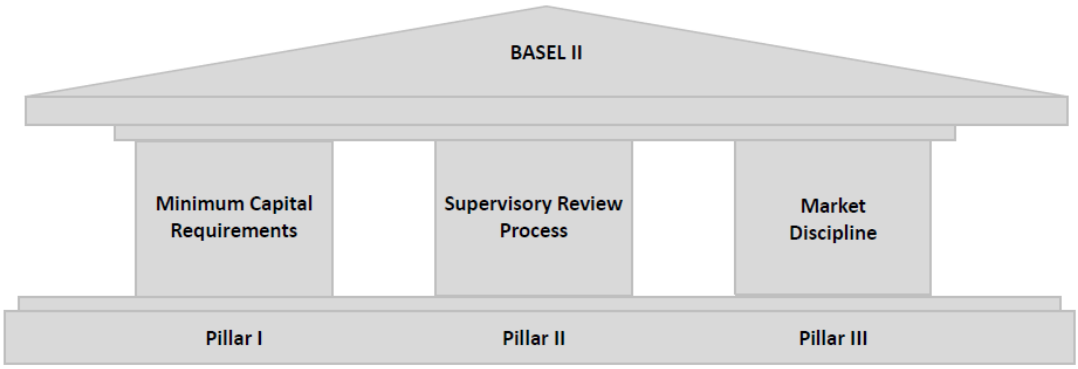
- Merito creditizio: definibile, in sintesi, come l'apprezzamento della solvibilità di un debitore. In altre parole, un soggetto che vanta un reddito costante e sufficientemente elevato avrà maggior merito rispetto ad un disoccupato od un precario; così come chi dispone di un notevole patrimonio acquisirà maggior merito creditizio rispetto ad un nullatenente. La normativa, introdotta col D. Lgs. 141/2010, impone alla banca una severa analisi del merito creditizio;
- Perdita attesa: è il valor medio della perdita che una banca si attende di subire con riferimento ad un credito o portafoglio di crediti, in un certo arco temporale. Normalmente la perdita attesa è espressa come funzione di tre elementi:
    - la probabilità di insolvenza del debitore (Probability of Default, PD);
    - la perdita in caso di insolvenza (Loss Given Default, LGD);
    - l'esposizione al momento dell'insolvenza (Exposure at Default, EAD).

Quindi, si ha: $EL = EAD \times PD \times LGD$

Il supporto delle regolamentazione ha seguito il seguente percorso negli anni duemila:



Il Nuovo Accordo sul Capitale (BIS 2), recepito nelle istruzioni di Vigilanza emanate da Banca d'Italia il 27 dicembre 2006 [145], è strutturato in tre sezioni, mostrate dalla seguente figura:



Il Primo Pillar introduce il concetto di metodologia per il calcolo del requisito patrimoniale a fronte dei rischi di mercato, credito ed operativi, il secondo quello di processo di controllo dell'adeguatezza patrimoniale, soggetto a verifica dell'Autorità di Vigilanza ed il terzo gli obblighi di informativa al pubblico

sull'adeguatezza patrimoniale, l'esposizione ai rischi e le caratteristiche dei sistemi di gestione e controllo. La normativa prevede tre metodi di calcolo del capitale a rischio operativo, caratterizzati da diversi livelli di complessità nella misurazione dei rischi e nei requisiti organizzativi e di controllo [98]:

- BIA: con il Basic Indicator Approach (BIA), il capitale di rischio si ottiene moltiplicando il margine di intermediazione per un determinato coefficiente di rischio (15%): RI*15%;
- TSA: con lo Standardised Approach (TSA) il capitale di rischio si ottiene moltiplicando il margine di intermediazione, suddiviso per business line, per un set di coefficienti di rischio (BIS 2 definisce un coefficiente per ogni business line, minimo 12% massimo 18%): RI*12-18%;
- AMA- con l' Advanced Measurement Approach (AMA), il capitale di rischio è ottenuto attraverso un sistema interno di misurazione basato su elementi quantitativi stabiliti dal nuovo accordo. Per l'utilizzo di tale metodo è necessaria l'autorizzazione della Banca d'Italia: Internal operational risk measurement system.

L'evoluzione e la recente crisi finanziaria hanno evidenziato l'urgenza di sviluppare una gestione del rischio preventiva basata su una più solida governance, anche in considerazione del fatto che esistono rischi tra loro correlati che necessitano di essere analizzati insieme perché attivati dagli stessi fattori di rischio. Ecco chenegli ultimi anni il progetto di Enterprise Risk Management (ERM) [95] si è affermato come nuovo paradigma per la gestione dei rischi nelle banche, nelle assicurazioni e nelle aziende industriali. È un processo che interessa tutta l'azienda, che con il contributo di ogni funzione finalizza un "appetito" al rischio che ha un valore economico. Il concetto di enterprise si esplica quindi nel riconsiderare l'intero ciclo di credito per prevenire un danno economico e generare una crescita sostenibile del mercato.

Le motivazioni del cambiamento, e quindi l'adozione di un approccio risk based, sono state motivate dalla presa d'atto di una situazione che nel 2013 ha visto:

- un requisito patrimoniale per rischi non di credito ma operativi di circa 2 miliardi di euro per perdite inattese;
- Il gruppo ha spesato negli ultimi anni circa 300 milioni di euro di perdite per rischi operativi su base annua per perdite attese.

In ambito rischio operativo e frode, la mission dell'enterprise risk management è:

- definire le metodologie, i processi, le procedure e gli strumenti per la prevenzione ed il controllo dei rischi operativi e delle frodi sia nella fase di istruttoria, di delibera delle pratiche e nella fase di post vendita, ovvero più in generale lungo tutto il ciclo di credito provvedendo al costante aggiornamento ed alla implementazione degli strumenti e delle procedure adottate;
- controllare i rischi operativi e le frodi in tutte le fasi del processo creditizio, al fine di identificare tempestivamente le posizioni e i canali/territori caratterizzati da un alto profilo di rischio, definendo le azioni correttive da porre in essere;
- curare la gestione dei rischi operativi consuntivati e delle frodi subite, in termini di analisi dettagliate dei fenomeni come base della curva di apprendimento costante, e in termini di coordinamento degli interventi da mettere in atto, attivando eventualmente gli organi esterni competenti (per le frodi ad esempio le forze dell'ordine) e coordinandosi, ove necessario, con le funzioni aziendali legale, compliance, controlli interni e audit.

Calando nel particolare il senso dell'Enteprise Risk Management nel settore retail di Intesa San Paolo Personal Finance, per gestire il rischio è necessario avere un modello di servizio/processo strutturato e industrializzato che risponda in tempi e modi adeguati alle esigenze del cliente finale. Il passaggio al modello industriale

impone logiche di analisi di massa, basate su sistemi di scoring/rating, che superano necessariamente le logiche di selezione individuale (pratica per pratica), che vengono mantenute per la gestione delle eccezioni.

Scoring

Le fasi del processo di scoring sono riconducibili ai seguenti passi [146]:

- Analisi multivariata del portafoglio passato: si individuano le variabili discriminanti e si effettua la distinzione tra soggetti "buoni" e "cattivi";
- Definizione dei punteggi per ogni variabile considerate: si associano punteggi per classi di ciascuna variabile;
- Somma dei punti di ogni variabile per definire un punteggio complessivo: il punteggio complessivo è organizzato in fasce di rischio omogenee;
- Individuazione della "cut off strategy": definizione del confine tra pratiche accettate e respinte;
- Disegno della griglia finale: definizione dell'errore accettabile.

Analisi del portafoglio passato

La costruzione dello score avviene attraverso un'analisi multivariata del portafoglio passato:

- Si estrae un campione rappresentativo, si esaminano centinaia di variabili per ciascuna delle posizioni estratte prendendo poi quelle che più di tutte risultano essere discriminanti, ovvero che meglio distinguono tra buoni e cattivi;
- La definizione di buono e cattivo è un'altra chiave del sistema di score. Tipicamente in questo ambito (retail/consumer) si definisce cattivo il soggetto che ha evidenziato un picco di rate arretrate pari a tre o più mesi,

mentre è buono il soggetto che ha evidenziato un picco pari a zero/un mese di insoluto.

Definizione dei punteggi per ogni variabile considerata

Applicando alle variabili discriminanti di cui al punto precedente una metodologia statistica (ad esempio una regressione logistica) si ottiene come risultato un insieme di punteggi associati a ciascuna classe di ciascuna variabile.

In figura 3 viene mostrato un esempio di variabile e di relativa attribuzione di punteggi. Un modello può essere costituito anche da quindici variabili, ciascuna delle quali suddivisa in n classi:

Variabile	Descrizione variabile	Binning	Descrizione binning	Score points	WOE	Bad Rate	% Pop
ANZIANITA_CC	Anzianità conto corrente	low <= ANZIANITA_CC < 54	Fino a 4 anni e mezzo Di anzianità	72	-0,57	3,8	29
		54 <= ANZIANITA_CC < 84	Da 4 anni e mezzo fino a 7 anni di anzianità	77	-0,32	2,9	13
		84 <= ANZIANITA_CC < 132	Da 7 anni a 11 anni Di anzianità	86	0,18	1,8	17
		132 <= ANZIANITA_CC < 204	Da 11 anni a 17 anni Di anzianità	95	0,67	1,1	21
		204 <= ANZIANITA_CC < high	Da 17 anni in su Di anzianità	105	1,25	0,6	19

Variabile

Classi

Punteggi

Figura 3: fattori presenti nel modello

Somma dei punti di ogni variabile per definire un punteggio complessivo

Dalla combinazione dei punti di ogni classe delle variabili del modello si ottiene, con somma algebrica, un punteggio complessivo. Questo punteggio finale organizzato in fasce omogenee è testato e validato ed è valido se restituisce un andamento come segue:

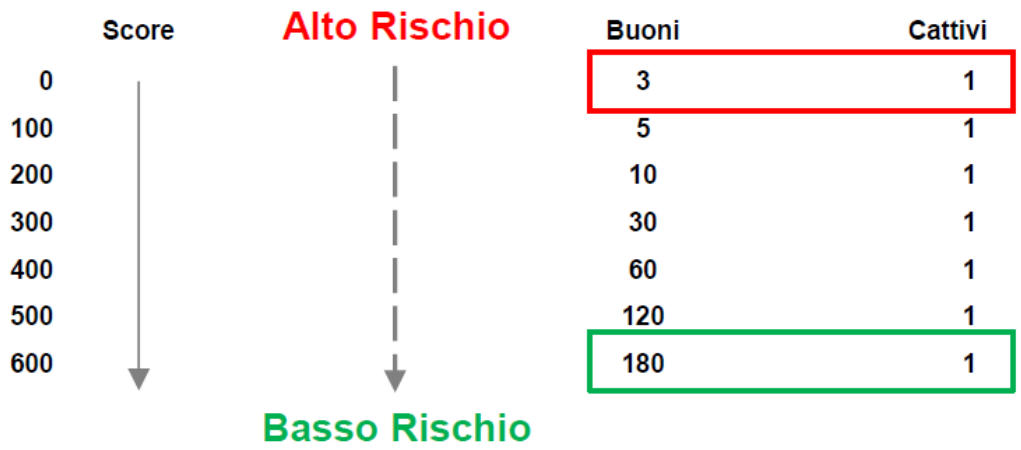


Figura 4: punteggio di rischio

Individuazione della "cut off strategy"

L'applicazione dello score è una politica aziendale. Non si potranno mai generare macchine perfette e uniche, visto che le stesse dipendono da tanti elementi che caratterizzano l'azienda che le usa. La scelta aziendale è la «cut off strategy» (o strategia di taglio), che determina l'appetito al rischio aziendale e consiste nello stabilire dove posizionare la divisione tra le pratiche accettate rispetto a quelle rifiutate. Di seguito un esempio:

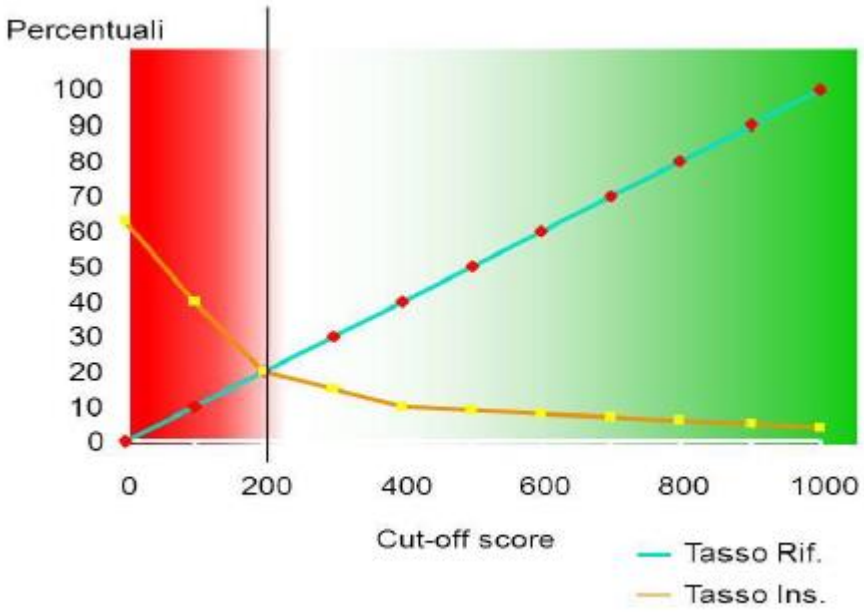


Figura 5: esempio di cut-off scoring

Disegno della griglia finale

Trattandosi di una griglia, a seconda della dimensione delle suddivisioni, si ottiene necessariamente l'effetto rappresentato in figura 6, ovvero è calcolato il rischio di perdere buone pratiche e di accettare pratiche cattive.

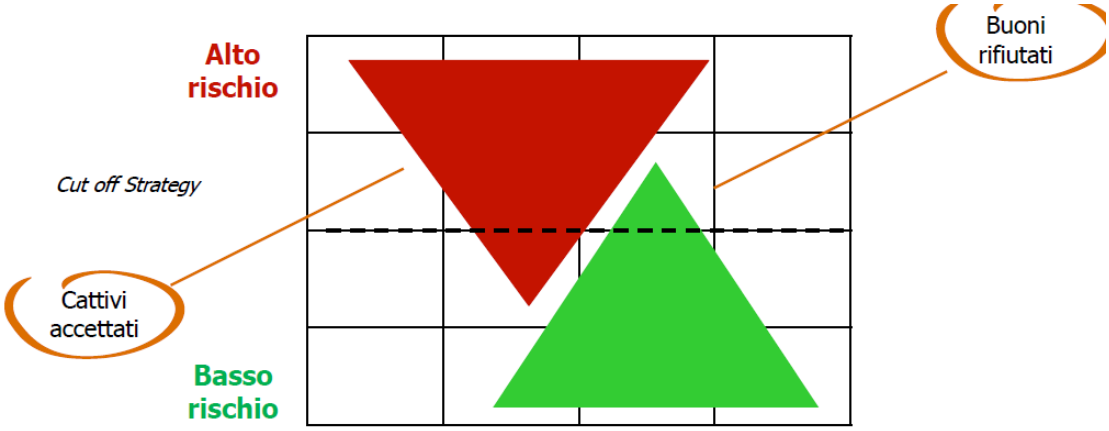


Figura 6: griglia decisionale

L'applicazione della metodologia descritta otimizza tempi e costi rispetto ad una lavorazione di tipo manuale. Altro beneficio correlato, consiste nel fatto che si processano simultaneamente molte più evidenze (positive e negative) che generano una sintesi pesata. Ne consegue un aumento della capacità computazionale e del livello di accuratezza delle analisi in fase di istruttoria diminuendo i tempi. La logica esposta di fatto abbandona la logica dei vincoli, meglio noti come policies che determinano l'evento al verificarsi anche di una sola condizione dimenticandosi di tutti gli altri elementi che possono concorrere alla valutazione del merito.

Focus sul segment Retail

In questo paragrafo verranno esaminati dapprima casi di frodi verificatisi prima dell'introduzione delle misure di prevenzione, poi il ciclo del presidio dei rischi

operativi fino all'attività puntuale che svolge la figura del fraud analyst in Intesa San Paolo Personal Finance [145].

Prima dell'introduzione delle misure di prevenzione, i casi di frode nell'erogazione di mutui e prestiti erano tendenzialmente frequenti.

Le casistiche erano da riferirsi a:

- Mutui erogati a deceduti: la banca a seguito di evidenti morosità in fase di attivazione del processo di recupero apprende che i clienti sono deceduti diversi mesi prima della stipula del mutuo stesso;
- Mutui erogati tramite intermediario rivelatosi infedele: la banca viene a conoscenza che un proprio intermediario è indagato per truffa. Viene appurato che lo stesso ha acceso mutui a prestanome analfabeti e nullatenenti e gli immobili sono di valore pressoché nullo;
- Mutui erogati su immobili fatiscenti: La banca, a seguito di controlli a campione, rileva gravi irregolarità su numerosi mutui concessi su uno stesso immobile, rivelatosi poi fatiscente. La banca mette a perdita la somma monetaria corrispondente ed avvia le procedure legali necessari all'accertamento delle responsabilità.
- Mutui erogati su case gravate da abuso edilizio: a seguito di richieste di sospensione mutuo, la banca viene a conoscenza che il tribunale ha sequestrato i terreni e gli immobili, ed apre procedura di indagine.

I soggetti che possono commettere frodi possono essere:

- Cliente: falsifica la documentazione anagrafica e quella reddituale, per accedere al finanziamento pur non avendo i requisiti perché in difficoltà economiche;
- Prestanome: contrae debiti per centinaia di euro accettando, solitamente su proposta di bande organizzate, che il proprio nome compaia in luogo

di un'altra persona, con il fine di ottenere somme di denaro immediato, in genere in contanti, ignari delle conseguenze.

- Intermediario infedele: Provvede a modificare diverse informazioni sulla pratica del cliente o in alcuni casi presenta pratiche il cui cliente è inesistente o utilizza un prestanome. In alcuni casi falsifica la documentazione per consentire al cliente di ottenere credito chiedendo commissioni aggiuntive, ottenendo sul proprio conto o su quello di parenti la cifra di finanziamento richiesto.
- Bande Criminali organizzate: Servendosi di prestanome o di dipendenti infedeli, provvedono ad inviare a più banche richieste di finanziamenti false, modificando i dati anagrafici e reddituali collegati ad entità reali o inventate, per accedere ad ingenti somme di denaro senza aver intenzione di restituire gli importi, lasciando le conseguenze legali a prestanome o comunque contando sulla difficoltà di essere intercettati.

Il ciclo del presidio dei rischi operativo e frode

Il presidio dei rischi è un processo complesso che si articola in diverse fasi, ugualmente rilevanti e fortemente integrate che consente di far leva su più azioni, per consentire un buon trade off tra esigenze di business e contenimento dei rischi di credito, operativi e frodi.

Per preservare la banca da possibili situazioni di rischi operativi e frodi risulta necessario attivare nelle diversi fasi del processo controlli sistematici e differenti. In particolare la banca deve occuparsi di tre macro aree:

- Prevention: definizione di metodologie, algoritmi e strumenti per la prevenzione ed il controllo dei rischi operativi e delle frodi;

- Detection: ovvero il controllo delle frodi in tutte le fasi del processo creditizio ed individuazione delle aree di miglioramento della fraud prevention;
- Analysis e misurazione rischio fonte d'affari: la gestione delle frodi subite e sventate, la messa in atto di nuovi interventi nonché la misurazione del rischio canale collegato alla fonte d'affari che canalizza le richieste di finanziamento.

Fraud prevention

L'obiettivo della prevention è implementare, laddove fattibile, tecniche di prevenzione idonee ad evitare potenziali schemi di frode al fine di mitigarne gli impatti. In Intesa San Paolo Personal Finance vengono adottate le tecniche di seguito descritte:

Reti neurali

Affinché il processo di Fraud Detection & Prevention garantisca un risultato costante, è necessario l'utilizzo di strumenti dinamici/adattivi per la costruzione di regole di intercettazione sempre al passo con l'evoluzione del fenomeno tramite l'implementazione di modelli. Il processo di apprendimento dai dati permette di definire pattern sconosciuti e dipendenze tra i dati disponibili. Inoltre la modellizzazione basata su reti neurali è molto veloce rispetto alla maggior parte degli approcci noti.

Analisi Emozionale

In un individuo le emozioni sono difficilmente manipolabili. Partendo da questo assunto ci si può concentrare su alcuni elementi che possono indicare lo stato emozionale di un individuo. Il primo è l'analisi sensoriale della voce, che ha

l'obiettivo di costruire un classificatore capace di discriminare gli stati emotivi di un soggetto a partire dai dati raccolti attraverso gli incontri in agenzia.
La Voice Stress Analysis (VSA) è condotta attraverso i seguenti step:

- estrazione di caratteristiche del segnale audio associato alla voce del richiedente registrata in agenzia;
- codifica delle informazioni e comparazione con casi di frode accertata o presunta;
- Individuazione real-time di situazioni potenzialmente a rischio frode.

Il secondo è la firma grafometrica, che permette l'identificazione certa ed univoca del firmatario del contratto bancario: acquisire la firma autografa su appositi dispositivi in grado di registrare l'immagine della firma, i dati dinamici e i parametri biometrici di essa, come ritmo, velocità, pressione, accelerazione e movimento aereo. La misurazione di questi cinque parametri permette di identificare in modo certo e univoco la persona che firma. L'identità biometrica rappresenta un elemento di sicurezza, considerando che non può essere falsificata o delegata ad altri.

Fraud detection

Obiettivo della detection è l'individuazione tempestiva della frode in atto e il conseguente blocco tempestivo di comportamenti dannosi in tutte le fasi del processo creditizio. La mitigazione dei rischi operativi e frode in Intesa San Paolo Personal Finance viene effettuata tramite l'analisi del merito creditizio e di un team dedicato di fraud analyst.

- Analisi del merito creditizio: l'analisi passa per il check delle fasi del processo di istruttoria e dell'individuazione delle griglie di scoring per il rischio frode. L'esito dei motori decisionali indirizza le successive azioni e

controlli, inviando (attraverso un apposito stato attributo del sistema) le pratiche ad alto rischio al controllo manuale del team di frau analyst.

- Team di fraud analyst: è stato creato e formato, attraverso corsi di formazione continuativi, un team di detection dedicato per l'attività di controllo e presidio dei rischi operativi attraverso l'analisi puntuale della documentazione collegata alla pratica, delle posizioni sospette e intercettate dalla griglia di scoring.

Fraud analysis

Appurato che l'esposizione al rischio di frode deve essere verificata periodicamente al fine di identificare schemi ed eventi potenziali che la banca deve mitigare, è necessario implementare un sistema di reporting e di flussi comunicativi che fungano da input alle attività di investigazione e che aiutino ad attivare azioni correttive.

Reporting

Monitoraggio continuo delle segnalazioni di comportamenti "fraudolenti" provenienti da qualunque ufficio della società, che confluiscono in report gestiti da un unico ufficio che si occupa di raccogliere, catalogare e tentare di risolvere e accertare le irregolarità. Tutta la documentazione connessa al monitoraggio viene costantemente rivista ed aggiornata in modo da essere allineata con le dinamiche aziendali.

Rischio canale

Si individuano una serie di indici sintetici del portafoglio collegato alle filiali canale banking e ai convenzionati canale non banking per risalire la relativa catena distributiva e condividere periodicamente gli esiti del monitoraggio con gli stakeholder.

Knowledge database

Consiste nella verifica delle frodi ripresentate. È noto, sulla base del Know how interno, che le frodi non sono eventi isolati ma spesso si ripresentano nel tempo seppur con lievi differenze. L'insieme dei tratti caratteristici di ogni frode passata, subita o sventata, risulta di estrema utilità nell'attività di fraud detection. In ogni pratica in esame si verifica l'eventuale presenza di informazioni anagrafiche collegate a soggetti fraudolenti memorizzati nel Knowledge Database.

Il presidio dei rischi in Intesa Sanpaolo Personal Finance: Le fasi del processo e i controlli di rischio operativo in essere

Viene di seguito mostrato il flusso operativo in Intesa San Paolo Personal Finance:

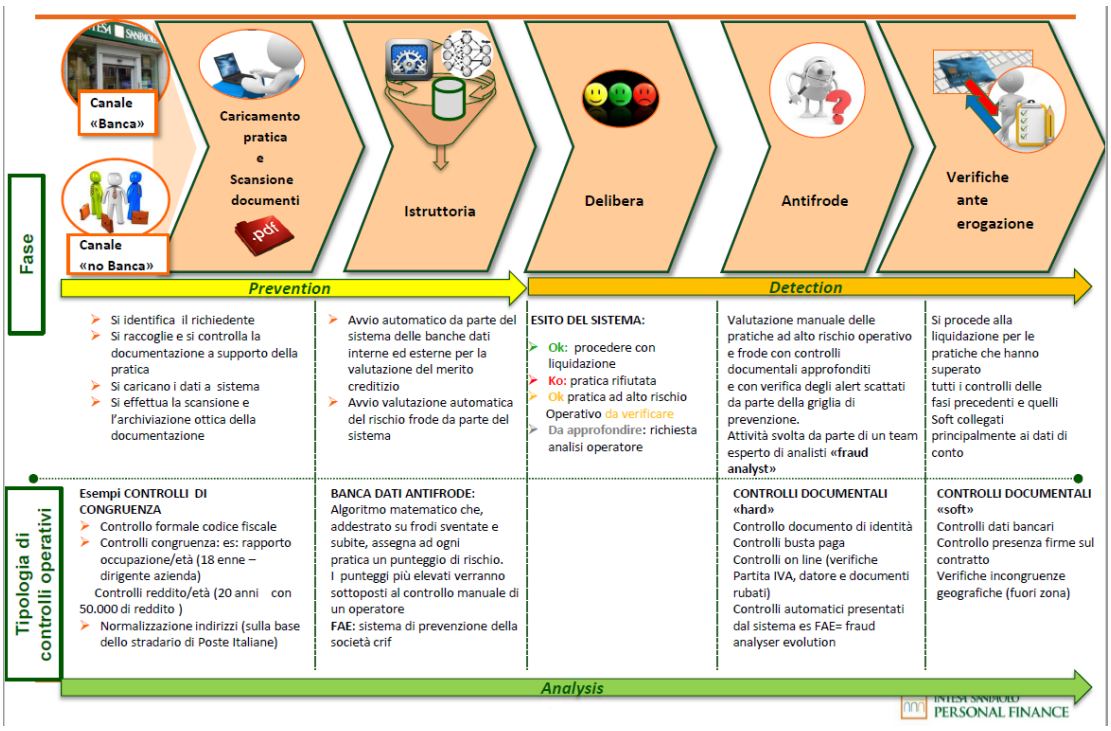


Figura 7: fasi del processo in Intesa San Paolo

Caricamento Pratica

In questa fase, l'addetto:

- Raccoglie le esigenze del cliente;
- Svolge gli adempimenti in materia di trasparenza;
- Acquisisce la documentazione necessaria;
- Ha la responsabilità della qualità dei dati caricati e dei riscontri previsti circa documenti e identità dei soggetti coinvolti;
- Non effettua alcuna valutazione ai fini del merito creditizio e nessuna discrezionalità sul mandare avanti o meno la pratica nel processo valutativo;

- Inserisce note di presentazione commerciale della richiesta per contestualizzarla.

Il Sistema:

- Per contenere i rischi operativi collegati alla fase di caricamento, assiste l'operatore con campi codificati il più possibile e con controlli automatici di rischio operativo tra cui: normalizzazione indirizzi, verifiche telefoni fissi e mobili, congruità dei valori;

I controlli principali sono impostati a sistema come:

- warning: gli utenti addetti al caricamento vengono semplicemente avvisati dell'incongruenza con quanto previsto dai parametri, ad esempio nel caso di inserimento non corretto di un dato;
- bloccanti: gli utenti addetti al caricamento non possono procedere all'inserimento del dato tranne in alcuni casi specifici in cui possono forzare il salvataggio dei dati (ad esempio, nel caso in cui il richiedente si presenti con permesso di soggiorno scaduto, è possibile inserire la data di scadenza riportata sull'attestazione/certificato rilasciato dalla questura di residenza in quanto valido come sostituzione degli atti ufficiali).

I controlli possono essere:

- formali: si intende la correttezza del dato imputato in termini di dimensione, natura (testo o numero) e formattazione (lunghezza minima e massima, formato data, etc...);
- di congruenza: si intende la correlazione delle informazioni socio-demografiche inserite e la congruenza/coerenza del contenuto del dato con gli altri dati inseriti (es. controllo maggiore età inibendo inserimento pratiche di minorenni);
- di obbligatorietà: si intende la possibilità di gestire, parametricamente, specifici algoritmi di controllo quali la presenza di almeno un recapito

telefonico fisso che a sua volta sia formalmente corretto, ossia non sia stata inserita per cinque volte consecutive la stessa cifra.

In ultimo, l'addetto scansiona tutto il materiale permettendo così la:

- dematerializzazione singola dei documenti già in fase di caricamento;
- creazione di un repository centralizzato contenente tutta la documentazione collegata alla pratica;
- implementazione di check list documentali consultive in fase di caricamento e nelle fasi successive;
- disponibilità del fascicolo documentale digitale in tutte le fasi del processo di credito.

Istruttoria

Il Sistema effettua interrogazioni automatiche a:

- banche dati interne (archivio storico della banca che raccoglie l'elenco dei nominativi non graditi per situazioni diverse, tra cui elevata morosità storica non più presente nelle banche dati esterne);
- esterne (es. CRIF, SEK PROTESTI) ovvero archivi pubblici e non, con informazioni comportamentali relativi al sistema creditizio italiano che raccolgono l'elenco di tutti i clienti che negli ultimi tre anni hanno avuto delle insolvenze;

Successivamente recupera le informazioni socio-demografiche inserite in fase di caricamento della pratica e attiva il processo di valutazione attraverso l'interazione automatica con il motore decisionale (in ISPF viene chiamato "Strategy One"). Gli alberi decisionali si distinguono per il merito creditizio da un lato, e per il rischio operativo e frode dall'altro. Per entrambi si applicano modelli statistici che sintetizzano le informazioni raccolte nelle fasi precedenti e esprimono la

probabilità di incorrere in una pratica con problematiche correlate a tematiche di rischio operativo e frode di insolvenza da parte dei soggetti richiedenti.

Gli esiti sono di quattro tipi:

1. Pratica Accettata: la pratica rientra nei parametri di accettazione definiti da Intesa Sanpaolo Personal Finance;
2. Pratica Rifiutata: la pratica non rientra nei parametri di accettazione definiti da Intesa Sanpaolo Personal Finance ed è stata esclusa negli accordi di esercizio opzione di liquidazione con garanzia;
3. Pratica Approvabile: la pratica non rientra nei parametri di accettazione definiti da Intesa Sanpaolo ma in forza agli accordi stipulati tra le parti, è possibile esercitare l'opzione di liquidazione con il versamento di una somma a garanzia concordata;
4. In attesa di esito: una parte residuale delle pratiche presentate non viene deliberata in automatico dal sistema ma viene sottoposta all'attenzione di un analista ISPF.

Delibera

La fase di delibera si divide tra attività automatica su tutte le pratiche la cui istruttoria ha determinato un esito positivo senza alcun dubbio, e una fase manuale dove l'operatore prende in carico solo le pratiche con esito incerto e provvede ad analizzare le caratteristiche d'insieme per determinare la sostenibilità della pratica.

Nel dettaglio seguente i possibili output del Sistema:

- rosso: la pratica viene respinta automaticamente dal sistema (autorifiuto);
- giallo: associato ad esito incerto del merito creditizio (richiede intervento manuale dell'addetto di valutazione crediti);

- verde: la pratica viene approvata automaticamente dal sistema (auto approvazione);
- verde con check fraud acceso: alla pratica viene attribuito un attributo "DV" (Da Verificare) che richiede l'intervento manuale di una figura preposta ai check documentali, il fraud analyst;
- verde senza check fraud acceso: la pratica è pronta per la fase dei controlli ante liquidazione.

La figura del fraud analyst in Intesa San Paolo Personal Finance

Il fraud analyst valuta il rischio operativo e di frode attraverso l'analisi di:

- alert scattati (sulla base delle policies e degli esiti della griglia frode);
- congruità dei dati caricati a sistema con i dati dei documenti allegati alla pratica nonché la validità dei documenti stessi.

L'obiettivo del team di specialisti fraud analyst è quello di intercettare attività fraudolente e criminali attraverso:

- Un'analisi investigativa della documentazione relativa alla pratica oggetto di analisi;
- Determinare le relazioni sfumate tra le pratiche presenti nel Sistema;
- Analizzare il rischio geografico e la congruità tra luogo di richiesta finanziamento e la località di residenza e domicilio del cliente;
- Analizzare le similarità presenti nella richiesta con altre in corrispondenza di schemi di frode subite e presenti sui database interni e/o esterni;
- Valutare il rischio di atipicità nella configurazione temporale degli eventi ricollegabili alla richiesta.

Verifiche ante erogazione

In questa fase il sistema ferma la pratica in un apposito stato evidenziando il tipo di controlli necessari prima di poter far avanzare di stato la pratica, quindi prima di liquidare. L'addetto quindi:

- verifica la coerenza di tutti gli elementi legati alla liquidazione (ad esempio: data decorrenza prima rata, coordinate bancarie, corretta apposizione delle firme e piena compilazione del modulo contrattuale);
- Effettuare le verifiche di conformità se non fatte in fase di caricamento (ad esempio: tutti i dati presenti sul contratto siano stati riportati correttamente sul sistema);
- Controlla la presenza dei dati bancari (IBAN);
- Verifica e smarca i controlli di rischio operativo di tipo «soft» (alert) presentati dal sistema eventualmente scattati (ad esempio il controllo fuori zona, che scatta quando il luogo della richiesta e quello di residenza e lavoro non coincidono).

Focus: il segmento Retail

Intrapreso il percorso di evoluzione della gestione del rischio attraverso l'individuazione e gestione dei cosiddetti rischi emergenti, l'attività di sviluppo si è concentrata principalmente sul rischio operativo, frode e canale dove spesso le definizioni dei tre insiemi sono correlate o comunque contraddistinte da confini molto labili. L'obiettivo è la tutela della Società/Gruppo Intesa San Paolo Finance da possibili situazioni di rischio collegate alla fonte d'affari (appunto rischio canale) attraverso l'implementazione di un sistema di monitoraggio, basato su misurazione puntuale delle performance, analisi dei trend e reportistica di sintesi delle fonti di affari, per l'analisi del comportamento di tutti i livelli della catena

distributiva, attraverso l'analisi due processi, "captive" ed "extra captive", per la gestione delle irregolarità riscontrate sulle singole fonti di affari.

I benefici sono:

- Miglioramento delle performance della rete distributive;
- Miglioramento del presidio dei rischi legati anche alla provenienza della pratica;
- Migliore standardizzazione del set informativo utilizzato per la rappresentazione dei fenomeni sul territorio/canale.

Le macroaree scelte per la gestione del rischio canale sono:

- Impianto di reporting: consiste nella creazione di un sistema di reporting mensile in grado di evidenziare in modo strutturato l'andamento (in termini di performance) dei canali (captive e extra captive) e di generare alert di rischio sui vari livelli della filiera distributiva.
- Processo di gestione degli alert: definizione di processi "captive" ed "extra captive", che consentano di gestire e chiudere in positivo o negativo le evidenze di rischio riscontrate lungo le filiere distributive, con al tavolo tutte le realtà coinvolte (dalle strutture aziendali di controllo alle strutture commerciali di coordinamento delle reti distributive stesse).
- Knowledge Database: costruzione di un DataBase come strumento dove sono raccolte e catalogate tutte le note di irregolarità (evidenze di pratiche canalizzate dall'intermediario/filiale con caratteristiche anomale). Un sistema di regole collegato che generi alert che consentono di rivedere i rapporti a rischio unitamente agli indicatori quantitativi provenienti dal sistema di reporting. Le uscite del processo sono ad esempio la messa sotto osservazione, la sospensione dell'operatività o la chiusura del rapporto.

Impianto di reporting

La struttura distributiva è stata suddivisa come mostrato in figura 8:

Figura 8: suddivisione dell'area retail in Intesa San Paolo

Le seguenti dimensioni di analisi sono state prese in considerazione:

- Orizzonte temporale di osservazione: Produzione degli ultimi 24 mesi rolling. Alcune osservazioni sono relative al recente passato ovvero il trend degli ultimi 12 mesi;
- Dinamica del fenomeno: si osserva l'andamento degli indicatori con evidenze ad 1, 3, 6, 12 mesi per cogliere il «trend» dei fenomeni osservati;
- Riferimenti spaziali e gerarchici: i vari indicatori, oltre ad essere espressi in valori assoluti, sono osservati anche in termini relativi con il confronto con il totale portafoglio di riferimento e con il livello della catena distributiva superiore;
- Uniformità della misurazione: per consentire il raffronto omogeneo tra segmenti diversi gli indicatori sono stati standardizzati tra captive ed extra captive e lungo tutta la catena distributiva.

Gli indicatori osservati sono suddivisi in quattro tipologie ed articolati secondo le seguenti dimensioni di analisi:

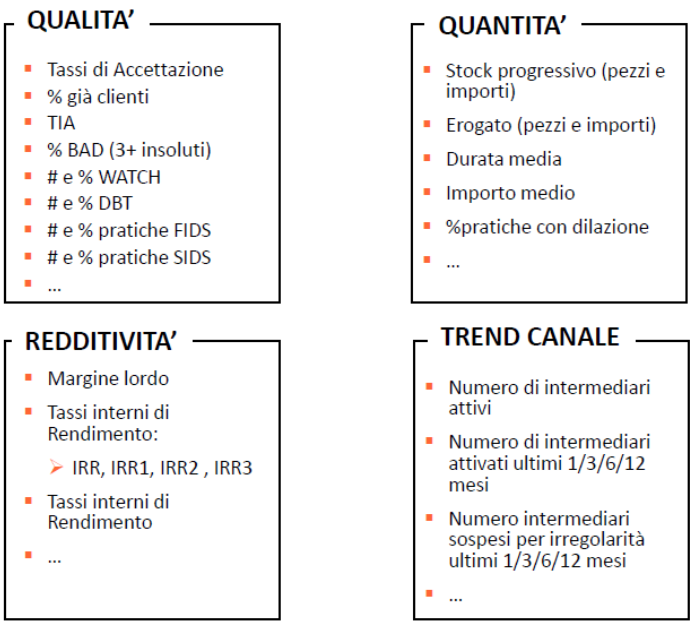


Figura 9: dimensioni di analisi

Perimetro e struttura dei report

I report sono differenziati per segmento captive ed extra captive, seguendo le stesse logiche.

I seguenti punti sono presenti nella reportistica dedicata al segmento captive:

- Sintesi: fornisce un'overview dei best e worst del territorio per direzioni e per aree;
- Confronto direzioni: una vista con i principali indicatori per un confronto tra direzioni e con il totale portafoglio;
- Confronto aree: stessa vista delle direzioni con i principali indicatori per un confronto tra le aree di ogni direzione e con il totale direzione;
- Tasso di accettazione: per portafoglio e per direzioni il tasso di accettazione e la distribuzione tra nuovi e già clienti gruppo;

- Filiali best e worst: evidenza delle migliori 20 e peggiori 20 filiali per soglie di quantità minime combinate con gli indicatori di rischio in un caso migliori nell'altro peggiori;
- Produzione filiali: per portafoglio e per direzioni la distribuzione in percentili del numero di filiali in base ai pezzi prodotti con evidenza anche dei valori medi e massimi;
- Rischio acido: elenco filiali con alert di rischio attivo sulla produzione recente, con tutte le informazioni disponibili nel database per le analisi delle singole posizioni;
- Rischio globale: elenco filiali con alert di rischio attivo sugli stock complessivi con tutte le informazioni disponibili nel database per le analisi analisi delle singole posizioni;
- Dettaglio filiali: elenco di tutte le filiali con tutte le informazioni disponibili nel database per le analisi delle singole posizioni e valori di ciascun indicatore esposti per confronto immediato con area e direzione.

I seguenti punti sono presenti nella reportistica dedicata al segmento extra captive:

- Sintesi: il colpo d'occhio dei best e worst del territorio per distretti e coordinamenti;
- Confronto reti: una vista con i principali indicatori per un confronto tra rete diretta e indiretta;
- Confronto distretti/coordinamenti: stessa vista delle reti con i principali indicatori per un confronto tra le «aree territoriali» di ogni rete e con il totale di riferimento;
- Tasso di accettazione: il tasso di accettazione e la distribuzione dei macro prodotti per portafoglio e per distretti/coordinamenti;

- Filiali/agenzie convenzionate best e worst evidenza delle migliori 20 e peggiori 20 realtà per soglie di quantità minime combinate con gli indicatori di rischio in un caso migliori e nell'altro peggiori;
- Produzione filiali/agenzie: per portafoglio e per direzioni la distribuzione in percentili del numero di filiali in base ai pezzi prodotti con evidenza anche dei valori medi e massimi;
- Rischio acido: elenco filiali con alert di rischio attivo sulla produzione recente con per ciascuna riga tutte le informazioni disponibili nel db per analisi delle singole posizioni;
- Rischio globale: elenco filiali con alert di rischio attivo sugli stock complessivi con tutte le informazioni disponibili nel database per le analisi delle singole posizioni;
- Dettaglio filiali/agenzie: elenco di tutte le filiali/agenzie con tutte le informazioni disponibili nel database per le analisi delle single posizioni e valori di ciascun indicatore esposti per confronto immediato con livelli catena superiori;
- Dettaglio convenzionati: elenco convenzionati con le stesse logiche del punto precedente di filiali e agenzie.

Di seguito un esempio di report prodotto:

	Rete Diretta Indicatori	Data Aggiorn.	Totale Portafoglio	Rete diretta	Coord. Emilia Romagna	Filiale Bologna 1	Convenzionato Praxis Srl
Qualità	T.ACCETTAZIONE	Ult. Mese	84,12%	85,19%	87,65%	90,50%	93,33%
	...	Ult. 3 Mesi	82,95%	84,00%	85,42%	88,54%	92,10%
	...	Ult. 6 Mesi	82,38%	83,81%	84,55%	88,58%	92,20%
	...	Ult. 12 Mesi	81,53%	83,71%	84,49%	89,27%	92,28%
	TIA 6	Ult. Mese	5,69%	2,05%	2,34%	2,84%	0,03%
	TIA 12	Ult. Mese	8,86%	3,71%	3,99%	4,33%	0,03%
	BAD 3+	Ult. Mese	3,99%	1,78%	1,69%	1,61%	1,26%
	FIDS	Ult. Mese	0,91%	0,19%	0,22%	0,27%	0,43%
	SIDS	Ult. Mese	0,18%	0,05%	0,02%	0,02%	0,00%
Quantità	TOTALE EROGATO #	Totale	489.668	100.481	20.615	8.742	2.769
	TOTALE EROGATO €/mil	Totale	€ 1.675.820.061,86	€ 544.082.611,99	€ 123.641.246,48	€ 47.006.701,72	€ 9.293.838,80
	DURATA avg	Ult. Mese	23	31	31	33	35
	...	Ult. 3 Mesi	24	32	32	33	35
	...	Ult. 6 Mesi	26	32	32	32	35
	...	Ult. 12 Mesi	26	32	33	32	34
	IMPORTO avg	Ult. Mese	€ 2.540,80	€ 5.139,93	€ 5.335,66	€ 4.490,02	€ 3.455,57
	...	Ult. 3 Mesi	€ 2.801,48	€ 5.226,32	€ 5.605,71	€ 4.820,20	€ 3.467,87
	...	Ult. 6 Mesi	€ 2.987,70	€ 5.422,03	€ 5.857,79	€ 5.196,47	€ 3.399,59
	...	Ult. 12 Mesi	€ 3.116,94	€ 5.439,25	€ 6.080,83	€ 5.364,09	€ 3.413,34
Redditività	MARGINE avg PA	Ult. Mese	2,84%	2,76%	2,72%	-	-
	MARGINE avg PF	Ult. Mese	5,17%	5,29%	0,51%	-	-
	MARGINE avg PP	Ult. Mese	6,66%	6,48%	6,38%	-	-
	MARGINE avg VD	Ult. Mese	6,46%	7,96%	9,05%	-	-

Esempi di trend

Confronto su indici di rischio «acidi»

Confronto su indici di rischio «robusti»

Confronto su indici di rischio «frode»

Esempi di trend

Alcuni indicatori di redditività

Figura 10: Esempio di report

Processo di gestione degli alert

Il processo di gestione degli alerts i attua nelle seguenti fai:

- Produzione reporting rischio canale a cadenza mensile e distribuzione dati in rete: mensilmente Il sistema di reporting sarà reso disponibile ai coordinatori territoriali/responsabili di filiale/agenzia ed alle altre strutture di sede interessate. Trimestralmente i responsabili di filiali/agenzie e coordinatori territoriali dovranno fornire riscontro sui casi in alert all'ufficio gestioni controparti.
- Valutazioni e Feedback dei coordinatori del territorio: entro 10 giorni lavorativi i coordinatori territoriali, previa analisi da parte dei responsabili delle filiali/agenzie, valutano le posizioni in Alert, inserendo gli esiti e inviando, ove necessario, le argomentazioni e i business case per l'eventuale mantenimento sotto osservazione dell'operatività nei successivi 6 mesi;

- Analisi di Gestione Controparti dei feedback della Rete: entro i 15 giorni lavorativi successivi al ricevimento degli esiti, l'ufficio gestione controparti provvederà a:
    - sospendere le posizioni in alert con parere favorevole della rete (5gg);
    - sottoporre al Comitato Ristretto le posizioni rimaste aperte per le quali i coordinatori territoriali esprimono disaccordo rispetto all'Alert.
- Chiusura post concordanza in comitato ristretto: Al primo Comitato Rischi e Credito utile post incontro del punto precedente le posizioni ancora pending vengono decise;
- Chiusura rapporti segnalati o attivazione del periodo sotto sorveglianza: Per tutti i casi definiti a valle della contribuzione del sistema di reporting (ad eccezione eventuale delle posizioni in delibera del comitato se la data utile è successiva a 30 giorni) a tale scadenza saranno aggiornati informaticamente da Gestione Controparti;
- Controllo semestrale delle posizioni in osservazione: Le evidenze dei business case delle posizioni che si manterranno aperte avranno un check point a 6 mesi.

Quindi in conclusione, l'analisi identifica agevolmente le aree territoriali in alert rispetto al totale portafoglio, dopodiché fa scattare un'analisi approfondita dei singoli casi solo dove necessario per poter porre in essere le azioni volte a cambiare le logiche del rapporto di intermediazione.

L'attività di intelligence sui singoli casi in alert, che di fatto si sposta sullo specifico portafoglio del partner/territorio, determina i comportamenti fraudolenti, per i quali si attivano misure drastiche sul rapporto in essere fino alla chiusura del rapporto per esterni e provvedimenti disciplinari per interni, e le performances del

portafoglio in chiave credito, per le quali si devono porre in essere azioni correttive concrete sul nuovo business per recuperare il pregresso e creare valore sulle nuove erogazioni.

2.3 Frodi e telecomunicazioni

Le società che offrono servizi di telefonia, fissa e mobile, negli ultimi quindici anni hanno fatto registrare una progressiva evoluzione nella relazione con il cliente, che ha portato ad una sempre crescente attenzione verso il concetto di customer care [75]. Parallelamente, però, il mercato delle telecomunicazioni ha dovuto anche fare fronte a modalità sempre piu' complesse, rapide e aggressive nel perpetrare frodi: ciò ha comportato quindi la necessità di una adeguata attività di monitoraggio e contrasto delle stesse.

In particolare, il passaggio dalla tecnologia analogica a quella digitale segna nel mercato delle Telco l'inizio di un'evoluzione dei fenomeni fraudolenti che spostano l'attenzione dal campo dei rischi tradizionali (come i casi di abuso) a forme più complesse e talvolta difficilmente prevedibili, che vanno dalle false sottoscrizioni alle frodi finanziarie fino a quelle tecnologicamente piu' sofisticate basate su tecniche di hacking [81].

Le cause dell'insorgere di nuovi fenomeni fraudolenti sono molteplici:

- La forte competizione nel mercato delle telecomunicazioni, aggressività e velocità delle politiche commerciali;
- Le politiche commerciali sempre più orientate a catturare nuovi clienti attraverso un'ampia disponibilità di promozioni, traffico gratuito e scontistiche;
- La sempre crescente domanda di minuti di traffico a basso costo da parte di nuovi carriers interessati alla gestione di traffico telefonico;
- Le vulnerabilità, anche provvisorie, di servizi e prodotti appena immessi sul mercato o su processi di gestione, dovuti ad un ridotto time to market;
- Lo scenario tecnologico sempre più complesso, dovuto anche alla convergenza fisso-mobile e all'ingresso nel mercato di internet e degli operatori virtuali;

- Il sempre più approfondito know how tecnologico e di mercato che i frodatori dimostrano di possedere;
- Il crescente interesse del mondo della criminalità organizzata per le frodi nelle telecomunicazioni, che mette in campo notevoli investimenti allo scopo di organizzare frodi come forme di business;
- La presenza di siti specializzati nazionali ed internazionali su internet con informazioni dettagliate sulle vulnerabilità presenti e sulle varie modalità di sfruttamento delle promozioni.

In tutti i casi rileviamo, come fenomeno più significativo osservato negli anni, l'affacciarsi sullo scenario il mondo del crimine organizzato, che si è andato progressivamente sostituendo ai singoli individui.

Categorizzazione delle frodi in ambiente telco

Le frodi nel mondo telco possono presentarsi in modo complesso, come combinazione di due o più tipologie di azioni fraudolente. [89]

Tentare, tuttavia, una categorizzazione è essenziale per la definizione delle più idonee strategie di contrasto e per la predisposizione dei processi operativi adeguatamente dimensionati anche in termini di risorse e professionalità specifiche.

Tale categorizzazione è necessaria anche per poter comunicare in maniera efficace con altri operatori del settore antifrode, allo scopo di condividere i fenomeni in atto e i relative potenziali rischi utilizzando una terminologia comune.

Ad alto livello, possiamo distingure le attività fraudolente in due macro tipologie [68]:

- Fraud type primario, relativo al modo illecito con cui il frodatore viene in possesso del bene o servizio telefonico (la SIM, l'handset, il servizio , la tariffa o la promozione, ecc.);

- Fraud type secondario, relativo alla modalità di utilizzo illecito del bene stesso.

Più in dettaglio le categorie in cui possiamo raccogliere le tipologie di frodi nel mondo delle telecomunicazioni, comunemente utilizzate tra gli operatori Telco e convenzionalmente riconosciute a livello internazionale dalla GSM Association, sono le seguenti:

- Subscription fraud;
- Technical fraud;
- Distribution fraud;
- Prepaid fraud;

Subscription fraud

Si tratta di una frode di tipo primario, sempre ricorrente, nella quale il frodatore, nel momento in cui si attiva come cliente, fornisce dati personali (come il nome e cognome, indirizzo, numero conto bancario/IBAN, professione, etc.) totalmente falsi oppure appartenenti ad una persona realmente esistente ma inconsapevole. Tale frode può ulteriormente differenziarsi in ulteriori tipologie che hanno come oggetto specifico, ad esempio:

- I dati personali di persone che risultano essere complici (proxy fraud);
- I dati bancari falsi o di persone ignare (Direct Debit Fraud);
- I dati di carte di credito rubati (Credit Cards – Stolen/Compromised) o duplicate (Credit Cards – Counterfeit) o veri appartenenti ad altra persona che disconoscera' il pagamento (Credit Card-Not-Present Transactions).

In generale, la subscription fraud è favorita da dinamiche commerciali nell'acquisizione di nuovi clienti laddove le aziende tendono a semplificare il più possibile le procedure di attivazione dei contratti, perchè velocizzando e

riducendo i controlli si crea l'opportunità per i frodatori di ottenere un contratto con modalità illecite allo scopo di non pagare i servizi richiesti.

Technical fraud

Le frodi tecniche vengono perpetrate utilizzando strumenti informatici con cui si forzano funzionalità di sicurezza degli operatori o si sfruttano bug temporanei del software o problemi tecnici dei servizi degli operatori. Tali frodi sono spesso veicolate da Internet, che diventa anche il più efficace strumento per la divulgazione di informazioni tecniche utili a mettere in atto la frode stessa. Queste frodi rientrano nel mondo dei crimini informatici (art. 640/Frode informatica, art. 615/Accesso abusivo ad un Sistema informatico o telematico, art 615/Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici).

In questa macro-tipologia di frodi rientrano diversi sottoinsiemi tra cui, ad esempio [93]:

- Mailbox Hacking:accesso non autorizzato alla casella vocale della segreteria telefonica di un cliente;
- IMEI Reprogramming: modifica o sovrascrittura del codice IMEI di telefoni rubati o smarriti allo scopo di sfuggire alle blacklist degli operatori;
- SIM Card Cloning: duplicazione della Sim originale attivata dall'operatore allo scopo di utilizzarla successivamente per beneficiare di servizi vari senza il pagamento dei costi dovuti. Tale frode è possibile soltanto sulle SIM di vecchia generazione ormai poco presenti sul mercato;
- Spamming (SMS&IP services): consiste nell'invio massivo di messaggi di tipo sms indesiderati ad un numero considerevole di persone, allo scopo di invitarli, in maniera ingannevole, a contattare un numero di telefono tipicamente di tipo premium (il fornitore del servizio premium coincide col frodatore);

- Phishing, in particolare smishing e vishing (rispettivamente phising via sms o chiamate Voip): tramite tecniche di spoofing del CLI (falsificazione del numero mittente), gli utenti ignari credono di essere invitati ad esempio dal proprio operatore telefonico a fornire dati personali, dati finanziari o comunque codici riservati, che verranno poi utilizzati per perpetrare frodi ai loro danni;
- Mobile Malware: utilizzo di software malevolo (virus, worms, trojan horses, ecc.) da diffondere sui device mobili, ad esempio, allo scopo di catturare dati personali o informazioni sull'utilizzo dei servizi telefonici, effettuare chiamate o inviare sms in maniera automatica verso numeri premium.

Distribution fraud

Le distribution fraud consistono in attività illecite, o contrattualmente vietate, attuate da personale che opera nei processi di logistica, distribuzione e vendita di servizi e prodotti di telefonia. Tra queste, alcuni esempi:

- Dealer fraud: frode perpetrata da dealer, addetto al punto vendita o da frodatori esterni, che stipula contratti fittizi a nome di persone ignare o inesistenti allo scopo di ottenere SIM e telefoni;
- False Agent / Remote Activation Fraud: attivazione di nuove line/contratti con procedure veloci (chiamata di numeri dedicati) da parte di falsi dealers o agenti ma da parte di frodatori;
- Theft & Handling Stolen Good: appropriazione indebita di beni destinati alla distribuzione e vendita (sim, telefoni) per essere rivenduti su canali commerciali non dell'operatore.

Prepaid fraud

Le frodi sulle SIM prepagate possono essere messe in atto ricaricando il credito mediante l'utilizzo di carte di credito rubate o clonate, utilizzando codici PIN di ricarica precedentemente trafugati da parte di personale infedele operante presso fornitori che producono le cartine di ricarica, oppure abusando di sistemi informatici su cui si ha accesso per ragioni di lavoro.

Tra queste alcuni esempi sono:

- Manual Recharging: il frodatore, che fa parte del personale interno dell'operatore, può sfruttare l'accesso al sistema delle preapagate per accreditare ricariche su SIM proprie o di terze persone che non ne hanno diritto;
- Roaming Fraud: il frodatore riesce ad utilizzare dall'estero una SIM ricaricabile con credito esaurito approfittando di problemi tecnici temporanei sulla rete del gestore sfruttando quindi una vulnerabilità temporanea della rete per generare volumi di traffico rilevanti, anche verso numerazioni premium internazionali che consentono di accumulare credito;
- Scratch Card Abuse: la frode consiste nel rivendere una carta di cui è stato già utilizzato il codice di ricarica della tessera la cui confezione verrà poi ricostruita per sembrare nuova.

Gli abusi e gli arbitraggi nelle Telco

Gli abusi e gli arbitraggi non sono classificabili come vere e proprie frodi, piuttosto come forme illecite di utilizzo di servizi senza che i comportamenti che li caratterizzano possano essere considerati illegali. Abusi e arbitraggi consistono infatti nell'utilizzo e nello sfruttamento in maniera impropria di servizi, tariffe e promozioni che l'operatore mette sul mercato, violando termini contrattuali o

sfruttando a proprio vantaggio delle vulnerabilità, anche temporanee, legate a lacune tecnologiche, errori di programmazione del software o bug dei sistemi informatici [66].

Un caso tipico di abuso nel mercato italiano viene realizzato combinando lo sfruttamento di specifici servizi con determinati piani tariffari che prevedono l'assegnazione di credito sulla SIM che riceve traffico. In questo modo i frodatori vengono spinti a generare traffico non pagato veicolandolo verso la SIM su cui è stato precedenetemente attivato il piano di autoricarica. Il credito illecitamente ottenuto con queste modalità viene quindi monetizzato effettuando chiamate verso numerazioni premium o rivendendo le SIM cariche di credito a terze persone.

Altro fenomeno sotto grande attenzione del fraud management è la trasformazione del traffico, che si mette in atto utilizzando SIM (ottenute fraudolentemente, con contratti regolari o SIM intestate a terzi) sulle quali sono state attivati piani tariffari particolarmente vantaggiosi. Queste SIM vengono installate in dispositivi denominati SIM BOX (che possono, ad esempio, essere configurate all'interno di centralini), che ridirigono il traffico originato da una rete fissa verso rete mobile attraverso tali SIM. In questo modo il frodatore non riconoscerà il costo dell'interconnessione entrante all'operatore di telefonia mobile di destinazione, in quanto la chiamata non apparirà più generata da rete fissa, ma dalla SIM "ponte" presente nella SIM BOX, che sfrutta le promozioni precedentemente attivate.

Soluzioni adottate per la prevenzione, la detection e il contrasto delle frodi

L'ambito Telco presenta molteplici aspetti e dimensioni di analisi, sia per le caratteristiche e le modalità di accesso al mercato più tradizionali (es. sottoscrizione di contratti), sia per le caratteristiche di sfruttamento delle offerte

commerciali tipiche del mondo telefonico, sia per caratteristiche decisamente più orientate allo sfruttamento a tutto tondo dei canali alternativi (es. Internet) e di politiche commerciali aggressive. Un efficace sistema di presidio e contrasto delle frodi si basa su una strategia di prevenzione, monitoraggio e reaction a tutti quei fenomeni fraudolenti che possono avere impatti negativi sulle revenues aziendali o sul brand. Deve quindi esistere in azienda un modello di governance dei rischi organizzato per coinvolgere in modo puntuale non soltanto la struttura di fraud management, ma anche tutte le altre funzioni aziendali che concorrono al ciclo di vita dei prodotti e dei servizi [90].

Fase di prevention

La prima azione di prevention consiste nell'analisi da parte delle unità organizzative di sicurezza e fraud management dei rischi frodi evidenziabili in una offerta o in un servizio di telefonia mobile, sia in termini tecnici che strettamente commerciali, sin dalle prime fasi di sviluppo del servizio o dell'offerta. Si tratta, quindi, di un aspetto di governance che implica un rapporto di stretta collaborazione tra le aree di sicurezza/fraud management e le aree di marketing e che comporta un coinvolgimento del management per una attenta valutazione del rischio associata al rilascio delle nuove proposition commerciali.

Inoltre, grande attenzione andrà posta alla prevenzione delle frodi perpetrate da personale infedele interno all'operatore o da rivenditori/agenti, che sfruttano la possibilità di accedere ai sistemi dell'operatore per compiere attività illecite (ad esempio accredito punti fedeltà, ricariche, promozioni a soggetti a loro vicini). Lo sviluppo di applicazioni destinate al personale dovrà quindi prevedere opportune funzionalità di logging e tracking allo scopo di consentire una adeguata attività di investigation in caso di incidente. Tutti gli operatori dovranno essere poi esaurientemente informati in merito a quanto previsto dalle procedure aziendali

per una corretta gestione del cliente e di tutta la sua documentazione, sia cartacea che elettronica. Nella fase di prevention rientrano anche gli aspetti tecnici e procedurali volti ad una verificare i dati forniti dai clienti in fase di acquisizione.

Fase di detection

Nel corso della commercializzazione dei servizi, la detection viene garantita con il monitoring di parametri che consentono, da parte di esperti fraud analyst, l'individuazione dei rischi emergenti. In caso di anomalie, gli analisti provvedono ad effettuare approfondimenti ed eventualmente a confermare la presenza di un incident.

Nel mercato delle telecomunicazioni, in particolare, per effettuare una efficace attività di detection, è di basilare importanza innanzitutto mantenere la mappatura della molteplicita' dei servizi offerti aggiornata, in modo da poter intercettare anche i piu' deboli segnali di una frode emergente e di garantire una costante valutazione del rischio commerciale. I Fraud Management System, che monitorano il traffico telefonico e consentono la gestione dei casi, rivestono un ruolo fondamentale in questa attività. Tali sistemi elaborano il traffico generato dai clienti e, sulla base di regole e parametri definiti dagli analisti, generano i cosiddetti "casi". I parametri e le regole utilizzate dai Fraud Management System per il traffico telefonico sono molteplici (chiamata, controlli su black list, etc...), sono definiti dinamicamente e si basano tipicamente sul superamento di soglie di traffico [94].

Dal momento che i fenomeni fraudolenti sono soggetti a rapide mutazioni e ad una notevole variabilità, i sistemi tradizionali di controllo basati esclusivamente sul superamento di soglie di traffico sono affiancati da moduli a tecnologia più evoluta come le reti neurali, con una intrinseca capacità di apprendimento dai casi di analisi pregressa. Naturalmente anche i piu' evoluti sistemi di controllo devono

essere costantemente aggiornati, corredandoli di nuove features messe a disposizione dai fornitori. I sistemi aziendali per l'attività antifrode non sono tuttavia in grado di individuare, da soli, i fenomeni fraudolenti nel caso in cui la frode venga perpetrata sfruttando problemi tecnici che hanno come effetto la mancata produzione di dati utili al monitoraggio. Anche l'utilizzo di tecniche di controllo basate sull'analisi economica dei servizi sarà quindi utile per evidenziare la generazione di costi anomali per l'azienda sfuggiti ai metodi di detection tradizionale. Infine, tra le attività svolte in fase di detection, dopo l'acquisizione di un cliente, sussistono i controlli antifrode effettuati in automatico, sull'eventuale presenza del cliente in blacklist e su altri tipi di informazioni socio-demografiche e comportamentali, allo scopo di definire un indice di rischio ed eventualmente attivare il fraud analyst per ulteriori approfondimenti o per il passaggio ad una fase di reaction. Risultano quindi molto utili le verifiche documentali, che sono anche finalizzate ad individuare false identità, complete o parziali.

Fase di Reaction

La fase di reaction comporta l'applicazione di procedure per la gestione dei fenomeni di frode e l'eventuale escalation dei casi piu' rilevanti al Management. Nel caso di frode accertata dall'analisi, la reaction consiste tipicamente nella sospensione o blocco immediato dei servizi oggetto di frode, nella sospensione o blocco di SIM e IMEI, con una richiesta di supporto alle tecnologie per eventuali interventi sulla rete o all'area legal, nel caso in cui si debbano bloccare dei pagamenti ad altre entita' coinvolte (ad esempio un altro operatore). Successivamente, la gestione dell'incidente prevede l'individuazione dei meccanismi che hanno originato la frode e, se necessario, la denuncia alle autorità competenti. Questo avviene attraverso un processo di condivisione all'interno di un gruppo di lavoro che coinvolge diverse funzioni aziendali, di volta in volta

interessate all'incidente, tra cui il finance, marketing, legal, customer care, technology, allo scopo di approntare in breve tempo un piano di azioni da condividere con il Management [105].

2.4 La gestione delle frodi nelle comunicazioni – Il caso Wind

Il ruolo della funzione di Fraud Management

La vision della funzione di Fraud management all'interno di Wind S.p.a. è quella di creare una cultura aziendale del rischio in cui tutte le forme di perdita delle entrate siano proattivamente affrontate con un programma end-to-end di prevenzione, monitoraggio e reazione volto a tutelare la redditività dell'azienda e la qualità dei prodotti/servizi offerti ai clienti contro ogni tipo di errore/inefficienza e di frode/abuso [148]. Per fare ciò, va definito, è stato implementato un sistema interfunzionale di prevenzione e di controllo in grado di ridurre al minimo i rischi di perdita dei ricavi e di qualità del servizio a causa di inefficienze/errori nei processi/sistemi aziendali. Gli obiettivi quindi sono:

- Definire un insieme adeguato ed efficace di policy, regole e metodi per la prevenzione ed monitoraggio del ciclo di vita dei Prodotti/Servizi offerti;
- Sviluppare un processo integrato di gestione dei rischi di frode, che definisca compiti e responsabilità chiare e precise tra le diverse funzioni aziendali per l'esecuzione dei controlli e la risoluzione dei casi rilevati;
- Garantire una visione unitaria e strategica dei rischi, problemi, impatti ed azioni risolutive, garantendo una visibilità a livello aziendale;
- Garantire la conformità dei processi alla normativa vigente (ad esempio 231/01, Privacy, etc...).

I seguenti fattori sono stati identificati per implementare la vision sopra descritta [149]:

- Identificazione dei rischi: L'analisi continua dei rischi è fondamentale per prevenire e contenere gli effetti sui ricavi. L'obiettivo è garantire adeguatezza e completezza di misure e metodi di prevenzione e controllo, partecipando al processo di creazione dei prodotti/servizi.
- Sistema di controllo: E' necessario monitorare con continuità e tempestività l'offerta lungo l'intero ciclo di vita. L'obiettivo è quello di dotare Wind S.p.a di strumenti di controllo avanzati, basati su regole e strategie decisionali modificabili rapidamente e su funzioni di monitoraggio quasi real time, attraverso la generazione di allarmi ed esecuzione di azioni automatiche.
- Policy e Procedure: Il modello del processo di fraud management deve essere fortemente integrato con i processi di business aziendali. L'obiettivo è la realizzazione di un processo basato su un approccio olistico e proattivo alla gestione dei rischi e su metodi e procedure in grado di rendere efficiente ed efficace la cooperazione tra le funzioni per l'analisi e la risoluzione dei problemi.
- Organizzazione e Risorse: La funzione di Fraud Management deve supportare il business ma, al tempo stesso, essere parte integrante del sistema di controllo interno aziendale. L'obiettivo strategico è definire un modello organizzativo che assicuri alla funzione indipendenza ed autonomia (rispetto alle funzioni owner dei processi di business) e vicinanza al Management, e creare un centro di competenza su rischi, contromisure e best practice in materia di sicurezza e frodi;
- Visione Unitaria: Il Management deve avere sensibilità e chiara consapevolezza del livello dei rischi, dei controlli e dei piani d'azione esistenti. L'obiettivo strategico è realizzare un modello di reporting ed un flusso informativo che assicuri visibilità, a livello aziendale, dei rischi e dei danni potenziali per il business e rapidità delle decisioni.

Per prima cosa, è stata effettuata una mappatura dei processi in scope al fraud management rispetto al processo di creazione di revenue, mostrata in figura 11 (in verde i processi in scope):

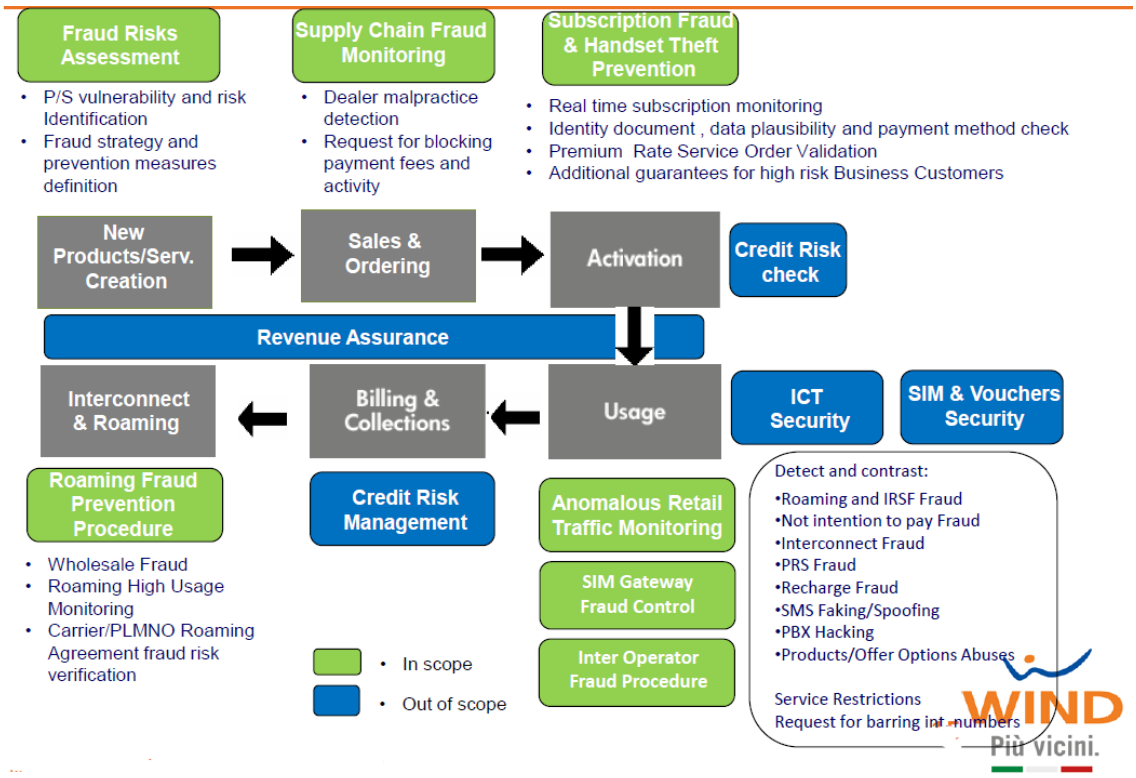


Figura 11: Processi in scope

In secondo luogo, si è proceduto alla strutturazione interna della funzione Fraud Management, organizzata in:

- Governance: si occupa della definizione di linee guida, processi e procedure per la gestione antifrode, monitoraggio delle attività svolte e supporto al miglioramento delle stesse per il raggiungimento della mission di funzione;
- Gestione Operativa delle frodi: gestione end to end dei fenomeni di frode, al fine di minimizzare preventivamente il rischio di frodi e di rilevare e gestire i casi di frode in corso.

Nel particolare, il processo della parte Governance si articola nelle seguenti fasi:

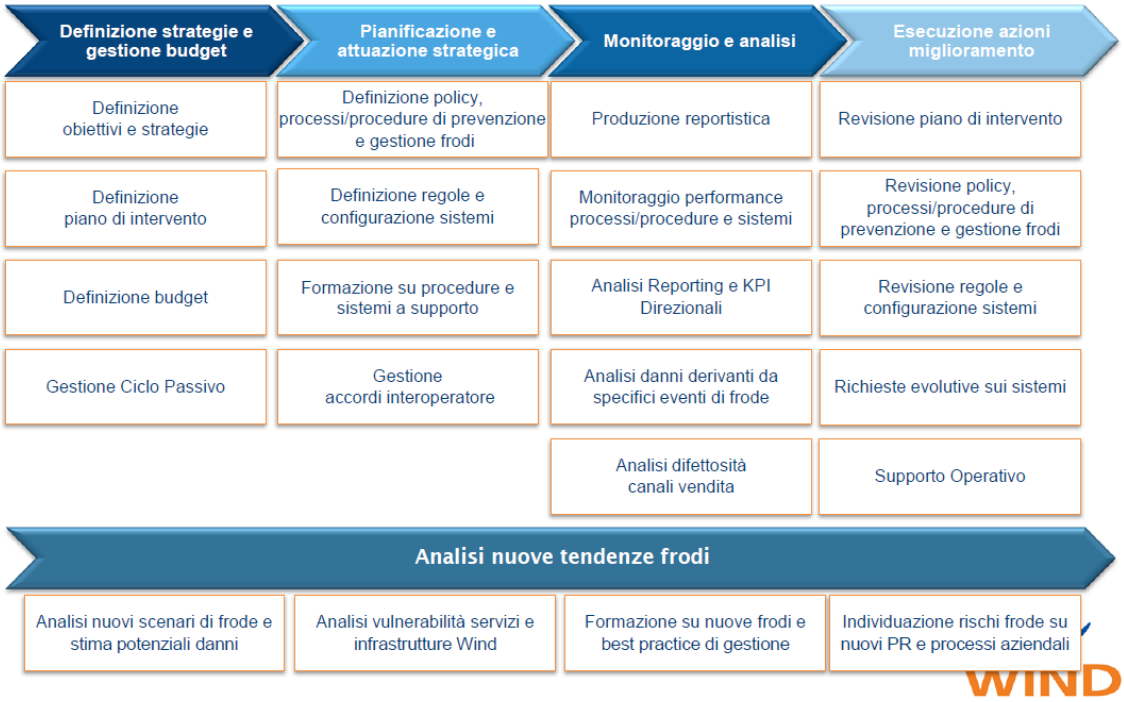


Figura 12: Processo di Governance

Mentre quello operativo:

Figura 13: Processi Operativo

Il governo del rischio frode richiede la costruzione di un processo fortemente trasversale deve interfacciarsi con molte funzioni aziendali, sia nella fase di commercializzazione che in quella di erogazione del servizio figura 14:

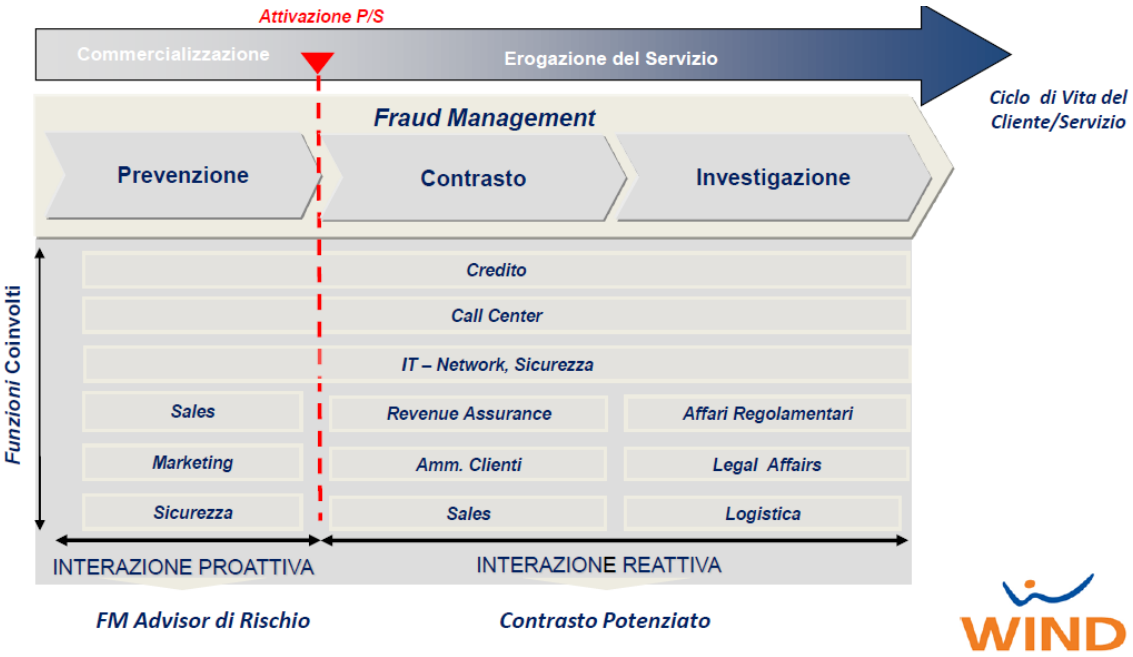


Figura 14: Interfunzionalità tra aree aziendali

Nella fase di prevenzione, la funzione Fraud Management svolge un ruolo di Advisor sui seguenti processi aziendali:

Processi:	Obiettivo Interazione:	Dipartimenti:
Attivazione Servizio	Definire e sviluppare controlli anti-frode in fase di acquisizione del cliente	Credito Sales Call Center
Sviluppo Nuovi Prodotti/Servizi	Condividere delle policy/contromisure anti-frode che minimizzino il rischio frode in accordo con le esigenze di vendita del marketing	Marketing IT-Network Sicurezza
Campaign Management	Condividere delle policy/contromisure anti-frode che minimizzino il rischio frode in accordo con le esigenze di vendita del marketing	Marketing
Logistica	Condividere policy e contromisure anti-frode sui processi logistici al fine di minimizzare i rischi	Logistica

WIND

Figura 15: Ruolo di Advisor tra processi aziendali

In quella di contrasto ed investigazione, interagisce con i seguenti dipartimenti nelle aree di analisi descritte figura 16

Dipartimenti	Aree di Analisi
Credit Management	• Review dei criteri e delle procedure di interazione con i processi di Fraud Management
Revenue Assurance	• Definizione flusso informativo per la comunicazione di eventi rilevanti relativi a revenue lekeage (scarti, traffico a zero, ecc.)
International Wholesale e Roaming Affari Regolamentari	• Formalizzazione procedura operativa per la gestione dei contenziosi (es. storno costi ITC per casi di frode) • Definizione flusso informativo per la comunicazione eventi rilevanti
Call Center	• Review dei criteri e delle procedure di interazione con i processi di Fraud Management (Dialer da Satellitare, Disconoscimenti, Sospensioni, ecc.)
IT e Network	• Definizione di modalità di supporto per l'analisi e la risoluzione di scenari di frode complessi • Definizione flusso informativo per la comunicazione eventi anomali/rilevanti in ottica antifrode
Amm. Clienti	• Review dei criteri e delle procedure di interazione con i processi di Fraud Management
Sales	• Definizione di controlli anti-frode e flussi di comunicazione per la gestione di comportamenti di malpractice in fase di vendita

WIND

Figura 16: Interazione tra dipartimenti aziendali – aree di analisi

Il modello risultante creato per soddisfare i requisiti di funzionalità interne alla funzione e di interoperatività aziendale è il seguente:

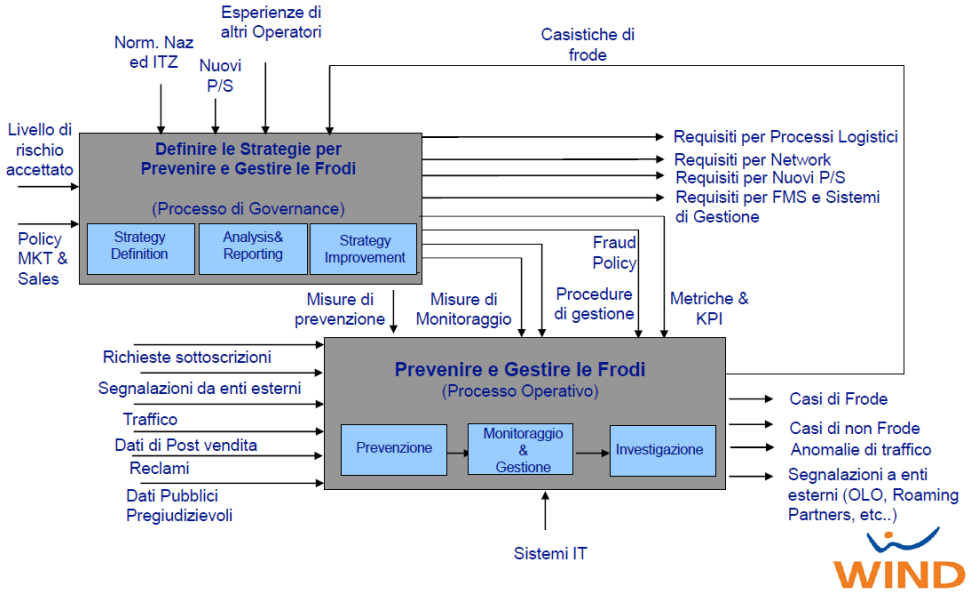


Figura 17: Modello di fraud Governance

Fattori critici di successo del processo di Fraud Management

I seguenti fattori sono fondamentali per il raggiungimento degli obiettivi [149]:

- Risorse: La disponibilità di risorse con skills e conoscenze specialistiche idonee (skills di customer service e credit control, skills di analisti di processo, skills di "data miner", skills di Network ed IT, known su casistiche di frode, tecniche di detection, processi di business e logistici, offerta prodotti/servizi, IT e Network Security, internet, metodologie di analisi dei dati);
- Informazioni: La qualita' delle informazioni disponibili sui fenomeni di frode (profili comportamentali dei frodatori, casistiche di frode, esperienze altri gestori, quadro normativo e legislativo, statistiche) e la definizione dei parametri definiti per il rilevamento delle diverse tipologie di frode;

- Processi: la visibilita' end to end sui prodotti/servizi offerti ed il sistematico coinvolgimento del fraud management nel lancio dei nuovi, la tempestivita' con cui si svolge l'azione di rilevamento e gestione della frode e la capacità di monitoring continuo del processo;
- Sistemi: la disponibilità' di sistemi di antifrode in grado di assicurare ampia flessibilita' nella variazione delle regole che definiscono i parametri per la rilevazione delle frodi e di tools di supporto alle attività di analisi dei comportamenti fraudolenti.

Nel processo antifrode sono stati identificati i seguenti Kpi, raggruppati per le seguenti aree:

- Efficienza: confronto tra le quantità di risorse produttive ed i risultati:
    - Tempo medio di lavorazione di un caso
    - Costo medio per caso di frode
    - % falsi positive
- Efficacia: misurazione dei risultati del servizio (outcame):
    - % casi di frode rilevati su totale casi generate
    - Impatto effettivo su impatto potenziale
    - Danni evitati
- Qualità: livello di affidabilità e precisione del servizio:
    - Incidenza attivazioni "bad" su attivazioni totali
    - % reclami su casi di frode gestiti
    - Incidenza reclami per frode su reclami totali

La cooperazione con gli altri operatori telefonici

A livello internazionale, la GSMA è stata costituita nel 1995 come come ente per supportare e promuovere gli operatori mobili. Risale alla sua storia un memorandum d'intesa firmato nel 1987 da 13 operatori in 12 paesi che si sono

impegnati ad implementare il GSM per i servizi mobili. Ad oggi circa 800 operatori in tutto il mondo sono membri GSMA. L'adesione associata è aperta alle società attive nell'ecosistema mobile, ed includono produttori di telefoni e dispositivi, società di software, fornitori di apparecchiature, nonché organizzazioni di settori industriali come servizi finanziari, sanità, media, trasporti e servizi pubblici. È strutturata in Working Groups che operano sotto la supervisione del Products & Services Management Committee (PSMC), e sono stati creati per:

- Facilitare lo scambio di informazioni e best practice;
- Sviluppare e mantenere documentazioni tecniche/operative per facilitare lo sviluppo efficace ed il rollout di servizi mobili interoperabili a livello globale;
- Proteggere i sistemi, le reti e gli utilizzatori dei servizi offerti su tecnologia GSM;

I Working Groups esistono in ambito roaming, interworking and interconnect, security e fraud, devices and SIM, web technologies and IPR. Nel 2014 il PSMC ha deciso di riorganizzare tutti i working groups, così il "Fraud Forum and Security Group" sono stati integrati in un unico gruppo, il Fraud and Security Group (FSG), il cui organigramma viene mostrato di seguito:

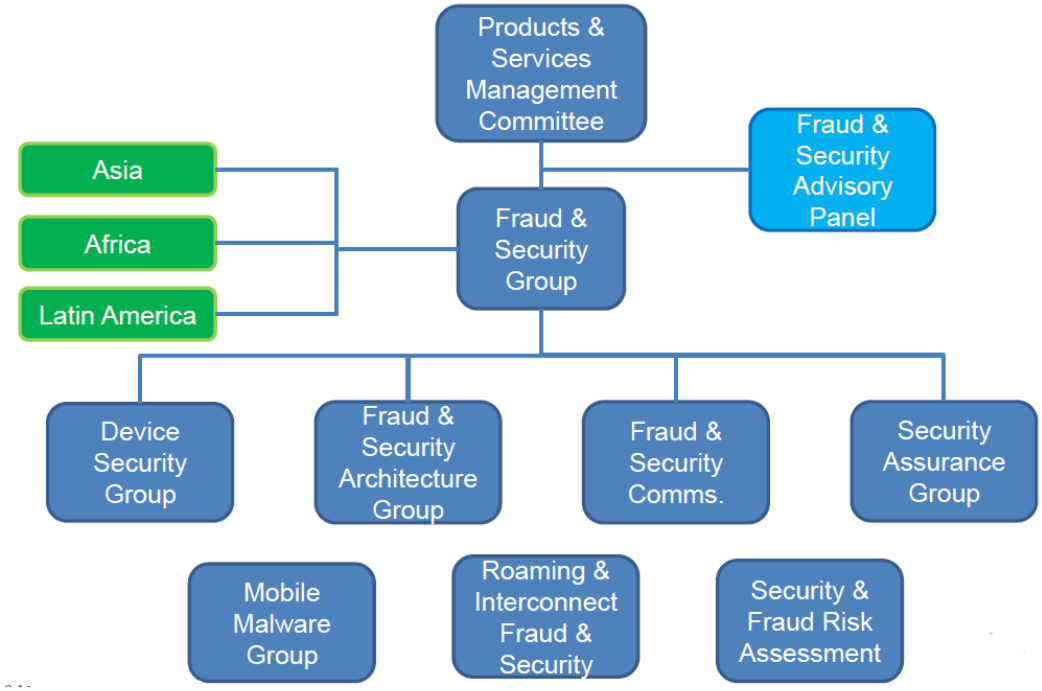


Figura 18: Organigramma GSMA

In ambito nazionale invece, è stata emanata una direttiva da parte dell'AGCom, la 418/07Cons, inerente le disposizioni in materia di trasparenza della bolletta telefonica, sbarramento selettivo di chiamata e tutela dell'utenza.

Considerato l'elevato numero di denunce presentate alle Autorità per presumibili frodi riguardo ad addebiti in bolletta di chiamate non effettuate, e delle controversie che queste generavano tra utenti e operatori riguardo, si è reso necessario, al fine di facilitare la prevenzione e la rapida individuazione di fenomeni fraudolenti sulle reti di comunicazione elettronica, prevedere che gli operatori si impegnassero a sviluppare apposite forme di intervento rapido e di scambio di informazioni tra gli stessi, istituendo allo scopo un tavolo tecnico, presieduto da un rappresentante designato dall'Autorità [149].

Inoltre, sempre in ottemperanza alla Direttiva AGCom 418/07/Cons gli Operatori italiani hanno provveduto, tra l'altro, a mettere a punto un Protocollo d'Intesa per la cooperazione nella prevenzione e contrasto delle frodi con i seguenti obiettivi:

- realizzare un processo operativo interoperatore per il monitoraggio e la risoluzione congiunta dei tentativi di frode;
- creare un Comitato Tecnico Antifrode, CTA, che gestisca le regole e modalità operative da rispettare per la loro gestione congiunta.

I principali tipi di fenomeni fraudolenti trattati nell'ambito del processo di cooperazione sono:

- Frodi dovute ad intromissione di terzi su utenze di clienti ignari;
- Frodi da sottoscrizione falsa;
- Fenomeni fraudolenti con utilizzo di prodotti ricaricabili con credito ottenuto attraverso attività fraudolente;
- Fenomeni fraudolenti da servizi ingannevoli (ad esempio spamming di SMS ingannevoli con inviti a chiamare NNG o altre numerazioni associate a servizi fittizi, ecc.);
- Frodi deducibili dalla presenza di caratteristiche anomale nel traffico.

Processo Interoperatore

Le fasi del processo operativo interoperatore sono le seguenti [148]:

- Segnalazione: L'operatore di accesso è tenuto a segnalare gli eventi presumibilmente fraudolenti rilevabili sulle numerazioni d'origine del traffico. L'operatore titolare di Numerazioni Non Geografiche (NNG) è tenuto a segnalare gli eventi di traffico anomalo terminanti sulle proprie numerazioni non facilmente rilevabili a livello di reti d'accesso;
- Verifica: Gli operatori destinatari delle segnalazioni sono tenuti a:
    - eseguire le verifiche del caso;
    - fornire il riscontro all'operatore segnalante;

    - inviare una segnalazione ad eventuali altri operatori coinvolti nello scenario di traffico anomalo rilevato;
    - comunicare le eventuali azioni cautelative intraprese per la risoluzione del caso.
- Risoluzione: La risoluzione richiede azioni congiunte a carico sia dell'operatore d'origine sia di quello/i di destinazione. Le azioni sono differenziate in funzione del tipo di evento e riguardano:
    - La gestione tecnica della frode:
        - sbarramento traffico;
        - inibizione accesso alle NGG fraudolente;
        - chiusura numerazioni NNG.
    - La gestione economica:
        - blocco pagamenti vs servizi/prodotti
        - note di credito

A fronte di una segnalazione l'operatore segnalante pone in essere, sulla propria rete, tutte le azioni cautelative idonee a mitigare i rischi. Nel caso in cui il traffico fraudolento sia diretto verso NNG (Numerazioni Non Geografiche), tali azioni possono consistere in:

- inibizione parziale o totale dell'accesso alla/e NNG interessata/e dalla propria rete;
- sospensione cautelativa dei pagamenti dei corrispettivi di interconnessione verso l'operatore titolare della numerazione, ove applicabile;
- storni/note di credito sulle fatture verso i clienti inerenti gli importi di traffico impropriamente fatturati;
- presentazione esposto/denuncia all'Autorità Giudiziaria.

L'operatore destinatario ha delle responsabilità che sono definite in funzione del tipo di frode. Qualora il traffico sia terminante su NNG, si ha la:

- sospensione del pagamento della reverse a favore del Service Provider;
- richiesta al Service Provider di rimuovere le eventuali irregolarità rilevate sul servizio, pena la risoluzione del relativo contratto o la chiusura della NNG o del gruppo di NNG interessate;
- chiusura della/e NNG e, nei casi più gravi (ad esempio in caso di servizi fittizi con evidenti profili e finalità ingannevoli), disdetta del contratto col Service Provider.

Qualora il traffico sia su SIM con profilo di autoricarica, si ha:

- la sospensione cautelativa della SIM destinataria del traffico presumibilmente fraudolento;
- l'invio di una segnalazione all'operatore titolare della NNG nei casi in cui si rilevasse un fenomeno di "scarico" del credito illecito verso NNG;
- l'invio di una segnalazione all'operatore mobile interessato nei casi in cui si rilevasse un fenomeno di autoricarica a catena, ossia di "scarico" del credito illecito verso SIM di altri operatori per presumibili finalità di autoricarica.

Comitato Tecnico Antifrode

Lo scopo del Comitato Tecnico Antifrode è quello di gestire le regole e modalità da rispettare per la gestione congiunta della procedura interoperatore. E' composto dai rappresentanti degli operatori firmatari del protocollo di intesa per l'adesione alla procedura interoperatore antifrode. Alle sedute del CTA partecipano, con funzioni consultive, anche i rappresentanti dell'AGCom e degli operatori che aderiscono unicamente agli impegni previsti nel processo di gestione tecnica delle frodi. È presieduto da un Presidente, scelto tra i membri, che resta in carica 2 anni ed è affiancato da un Vice Presedente, appartenenti ad operatori diversi [148].

Le decisioni riguardanti la modifica delle norme che regolano gli aspetti tecnici sono demandate ad un organo specializzato, il Forum delle frodi, composto dai soli delegati dei membri che operano nell'ambito dell'attività antifrode. Nell'ambito delle Forum delle frodi sono costituiti sottogruppi di lavoro tematici per l'approfondimento di argomenti riguardanti specifiche aree di interesse. Attualmente sono operativi due sottogruppi focalizzati rispettivamente sulla telefonia fissa e mobile, che si riuniscono con cadenza quadrimestrale.

2.5 Frodi e assicurazioni

Il fenomeno delle frodi colpisce in modo significativo il settore assicurativo, in particolare nel ramo auto. Alta è la percentuale di sinistri denunciati in modo fraudolento e di questi molti non vengono scoperti dalle compagnie [58], Pagano, M., Immordino, G.Corporate fraud, governance, and auditing2012Review of Corporate Finance Studies.

Il governo italiano ha ritenuto di dovere intervenire indicando nelle compagnie e nell'IVASS (Istituto per la Vigilanza sulle Assicurazioni) i soggetti principali per la lotta alle frodi. Dal punto di vista normativo il Governo italiano ha emanato una serie di provvedimenti [150]:

- Legge 27/2012 – "Decreto Liberalizzazioni", che prevede misure contro le frodi in fase di liquidazione e prevede l'obbligo per le imprese di assicurazioni di trasmettere una relazione annuale sulla propria attività antifrode. Tale relazione è stata poi strutturata attraverso il Regolamento ISVAP 44/2012;
- Legge 134/2012 - "Decreto Sviluppo", che ha apportato modifiche al Codice di Procedura Civile (art.342 e s.), che incidono sull'Appello e Ricorso per Cassazione;
- Legge 135/2012 – "Spending Review" che istituisce l'IVASS per sostituire

l'ISVAP con stretto collegamento con la vigilanza bancaria (CONSOB);

Legge 221/2012 – "Crescita Bis", che da competenze antifrode all'IVASS, prevede contratti di durata annuale e divieto di tacito rinnovo, le polizze base r.c. auto, aree di consultazione internet per gli assicurati, libera collaborazione tra intermediari, piattaforme comuni per gestione e stipulazione contratti;

Le compagnie stanno reagendo a questi stimoli impegnandosi verso la ricerca e l'implementazione di nuovi processi e strumenti antifrode. Possiamo distinguere le frodi assicurative in quattro categorie:

- Configurazione contrattuale fraudolenta: l'intero affare si sviluppa su presupposti fasulli. L'assicurato omette dei rischi, dichiara un valore troppo elevato dell'oggetto assicurato oppure cerca di assicurarsi per un danno già avvenuto;
- Simulare un evento assicurato: il sinistro avviene successivamente alla firma del contratto, ma l'evento non rientra in garanzia. Per essere indennizzati si dichiara un sinistro coperto da contratto;
- Lo sfruttamento in malafede del sinistro: l'evento assicurato si realizza effettivamente, ma l'entità del danno dichiarato è troppo alta o è stata volutamente esagerata;
- La premeditazione: provocare dolosamente un sinistro per simulare la realizzazione di un rischio assicurato mediante un'accurata preparazione (falsificazione di documenti o altro);

Il primo tipo di frode riguarda la fase contrattuale e le altre le fasi di dichiarazione e gestione di sinistri. La maggior parte delle frodi sembrano essere di tipo esterno alle compagnie, ma nella realtà dei fatti possono essere coinvolte anche figure direttamente o indirettamente legate alle assicurazioni. Il primo tipo di frode considerato può coinvolgere l'agente che stipula il contratto per conto della

compagnia, nel secondo è possibile prevedere il coinvolgimento del perito che deve valutare il sinistro, mentre nel terzo possiamo addirittura supporre il coinvolgimento del perito e della persona addetta a riparare il danno. Nel quarto caso infine si può verificare il coinvolgimento di figure con conoscenze legali che aiutano il frodatore a preparare dei documenti legali che supportino la frode.
Di tutti questi fattori si deve tener conto nello sviluppo delle politiche e delle metodologie di contrasto alle frodi.

Soluzioni Software e metodologie di contrasto delle Frodi

Le soluzioni software in campo antifrode impattano su persone, processi e informazioni. L'obiettivo finale della lotta alle frodi consiste nel ridurre le perdite e mantenere una redditività in linea con i desideri aziendali [117]. Implementando una soluzione efficiente ed efficace, per l'azienda si determina una azione deterrente, quindi se il sistema dei controlli opera in maniera precisa e mirata rispetto alle esigenze si attua un innalzamento della probabilità di individuazione per il soggetto frodante, creando così i presupposti per cui non esistono piu margini convenienti in operazioni malevole. Un processo antifrode maturo è in grado, mediante gli strumenti adatti, non solo di gestire il normale rilevamento ma anche di generare prevenzione. L'approccio strategico sistemico e integrato con i processi aziendali, come ad esempio assunzioni e liquidazioni, e' l'unico possibile per raggiungere obiettivi di cambiamento e di controllo sui fenomeni fraudolenti. Un generico software per il contrasto delle Frodi e' uno strumento che innanzitutto deve dimostrare di essere fattivamente utile alle strutture operative nelle azioni di intelligence sui vari casi. Una moderna soluzione software deve analizzare enormi moli di dati strutturati e non, sia su banche dati interne alle aziende che esterne (ad esempio white list e black list), limitando al minimo la generazione di falsi positivi. Emerge preponderante il fatto che la qualità dei dati

è un prerequisito importantissimo ed un fattore critico di successo per determinare l'efficacia di qualunque piattaforma applicativa. Bisogna creare dei ranking e segmentazioni sui dati aziendali e sui dati esogeni di sistema, quindi innescare azioni di detection ed intelligence e di individuazione dei fattori di rischio [99]. Un altro obiettivo è la diminuzione della latenza tra l'evento fraudolento e la sua rilevazione. Questa attività è molto agevolata dalla qualità dei dati raccolti e che costituiscono la base su cui poi lavorare. Non esiste un'unica soluzione, esistono diverse tecnologie che oggi grazie ad un buon livello di maturità possono essere proficuamente usate e implementate per creare software complessi che siano in grado di gestire le varie fasi di contrasto alle frodi. Ovviamente un'analisi dei bisogni e della realtà dell'azienda è il primo passo per poi procedere alla realizzazione, all'avviamento ed infine al tuning. Di solito una soluzione applicativa antifrode si integra con i sistemi di gestione dei sinistri, ed ha valide features di parametrizzazione delle regole per determinare specifici ranking e indicatori di rischio. Inoltre durante il ciclo di vita del sinistro deve produrre valore aggiunto in ogni cambiamento di stato della pratica. Per esempio oltre alle classiche applicazioni standard relazionali o di business intelligence (online/ batch) debitamente progettate, si possono citare le reti neurali e la nuova realtà dei big data [117]. Queste due componenti sono in grado di creare un'identificazione attiva di relazioni tra dati complessi che aiutano a comprendere fenomeni nascosti o non facilmente visibili agli operatori. La creazione di modelli analitici predittivi è in grado di identificare nuovi tipi e modalità di frode e nuovi trend. Sono sicuramente da esplorare e approfondire gli impatti e i punti di contatto con l'infrastruttura informatica tradizionale in termini di separazione degli ambienti dei compiti (segregation of duties), e tensione alla conformità.

Sicuramente nel sistema di controllo il liquidatore e la sua awareness crea intrinsecamente valore aggiunto, perchè scopo ultimo di una pur sofisticata

soluzione software antifrode, è di fornire all'operatore degli elementi su cui decidere e poter approfondire.

I processi antifrode con una valida piattaforma software oltre ad agevolare la conformità aziendale (obblighi verso l'IVASS), permettono la generazione di valore, la riduzione dei rischi operativi, trasformando un evento critico in una maggiore efficienza ed efficacia intrinseca di tutto il sistema azienda.

2.6 Frodi e gaming

Secondo gli ultimi dati dell' Osservatorio Gioco Online del Politecnico di Milano la spesa complessiva in giochi a distanza è stata sostanzialmente stabile rispetto all'anno precedente: 749 milioni di euro, con un aumento di 14,5 milioni, ovvero l'1,9%. Sono cresciute ulteriormente le occasioni di gioco via Internet grazie alla capillare diffusione di smartphone e tablet, ormai a disposizione di circa 20 milioni di italiani, ed è aumentata l'offerta di giochi con l'introduzione delle slot online [96]. Tale mercato è sempre stato e continua ad essere particolarmente interessante per i singoli frodatori e per il crimine organizzato poiché al suo interno, così come in tutto il mondo internet, si può facilmente nascondere la propria identità: ciò rende tale contesto il terreno ideale per attività fraudolente e criminali, con un particolare rilevanza del riciclaggio di denaro proveniente da attività illegali.

Riferimenti normativi per l'online gaming

La necessità pertanto di regolare le attività di gioco, specificatamente rispetto a crimini quali il riciclaggio, è stata riconosciuta a livello internazionale ed affrontata con una serie di direttive, regolamenti e leggi, anche specifici a livello di singolo stato oltre che, ad esempio, di comunità europea.

Rispetto alla realtà italiana, il D. Lgs. 231/2007 e s.m.i. è la vigente normativa di riferimento relativamente all'antiriciclaggio e contempla il gioco online nell'art. 14, co.1, come offerta, attraverso la rete internet e altre reti telematiche o di telecomunicazione, di giochi, scommesse con vincite in denaro. Nel considerare il gioco effettuato sfruttando le reti di comunicazione, il decreto detta una serie di regole e misure a carico non solo dei gestori dei giochi on line, ma anche dei gestori della rete di telecomunicazione e dei conti gioco utilizzati per il gioco stesso. Tali misure, di natura IT ed organizzativa, hanno lo scopo di dare evidenza di eventuali azioni mirate, specificatamente, al riciclo del denaro proveniente da attività criminali [150].

Tra le misure IT, a titolo esemplificativo si elencano le necessità di:

- Identificare il giocatore prima di consentirgli di partecipare al gioco, fornirgli le credenziali di accesso ed autenticarlo successivamente sulla piattaforma;
- Tracciarne i riferimenti relativi all'IP, la data e l'ora della connessione alla casa da gioco on-line;
- Registrare le movimentazioni sul conto di gioco.

Il D. Lgs. 231/2007 è inquadrato all'interno di una più ampia regolamentazione, anche a livello europeo, al fine di realizzare la collaborazione tra stati membri per tracciare anche possibili movimenti di riciclaggio che coinvolgano attori distribuiti in più nazioni.

Le frodi nell'online gaming

Considerando il panorama completo del mondo del gaming, i comportamenti fraudolenti hanno natura e caratteristiche varie ed eterogenee che dipendono dal particolare tipo di gioco, che vanno dalla falsificazione dei biglietti delle lotterie istantanee fino alla collusione tra più giocatori nell'ambito dell'online gaming. In

particolare è evidente come il tema delle Frodi ICT sia di particolare rilevanza per il contesto dell'online gaming e più in particolare per i giochi in cui è prevista l'interazione dell'utente con altri giocatori (ad esempio il poker online). Pur essendo consapevoli della varietà dei processi definiti e implementati dagli operatori, di seguito si descrivono le tipiche fasi previste per online gaming:

- Conto Gioco: il giocatore apre un proprio conto gioco solitamente attraverso il sito web dello specifico concessionario. Tale operazione può prevedere da parte dell'operatore la richiesta all'utente di produrre documentazione per accertare la propria identità;
- Deposito: l'utente dispone di un portafoglio elettronico associato al proprio conto gioco su cui deposita le somme di denaro con cui intende giocare. Le modalità di deposito sono varie e vanno dall'utilizzo di denaro contante presso ricevitorie autorizzate all'uso di strumenti di pagamento online (carte di credito, carte di debito, paypal,etc…);
- Gioco: l'utente utilizza la disponibilità del proprio portafoglio elettronico, ad esempio, per pagare l'iscrizione ad eventi di gioco (iscrizione a tornei di poker on line), per fare le puntate (scommesse on line, puntate nell'ambito del poker) e per acquistare dei giochi online (lotterie istantanee, giochi di abilità);
- Prelievo: l'utente può prelevare solo la disponibilità derivante dalle proprie vincite.

I comportamenti fraudolenti sono distribuiti in tutte le fasi descritte e partecipano alla composizione della frode. Alcuni fenomeni sono comuni ad altre industries mentre altri sono intriseci alla particolare tipologia di gioco. Consideriamo come esempio più significativo le frodi relative al poker online, sottolineando però che quanto espresso per il seguente esempio può essere esteso ad eventuali ulteriori

giochi online ed in particolar modo ai giochi che prevedono una interazione dell'utente con altri giocatori [149]:

- Preparazione della frode: il frodatore pianifica l'atto fraudolento coprendo le proprie tracce e aprendo il conto gioco fornendo generalità fasulle o rubate. Tale fenomeno, che si configura come frode di sottoscrizione e può essere assimilato alle frodi nell'ambito degli operatori telefonici (soprattutto su servizi mobile), è tipicamente contrastato attraverso controlli di sicurezza che mirano ad accertare la reale identità dell'utente verificando l'eventuale utilizzo di documenti rubati o contraffatti, richiedendo ulteriori riscontri utilizzando differenti canali di comunicazione (fax, telefono) e gestendo la creazione del conto gioco attraverso differenti stati di attivazione (ad esempio in un primo momento il conto gioco è inibito al prelievo);
- Creazione disponibilità e incasso della somma: il frodatore ricarica il proprio conto gioco attraverso strumenti di pagamento affetti da specifiche tipologie di frode quali, ad esempio, carte di credito clonate, o account Paypal rubati. Altro tipico fenomeno nell'ambito del deposito del credito è l'utilizzo di fondi illeciti per ricaricare il conto gioco del frodatore. In questo senso alla frode verso gli altri giocatori e verso l'operatore si aggiunge il fenomeno del riciclaggio di denaro.

Per contrastare tali fenomeni gli operatori possono adottare prodotti e servizi, che operano un controllo sull'utilizzo del conto gioco monitorando i comportamenti sospetti, segmentando la clientela in cluster profilati secondo la criticità rilevata, elaborando grandi quantità di dati per identificare fenomeni non evidenti o emergenti e imponendo opportune soglie e blocchi preventivi per arginare eventuali fenomeni fraudolenti [46].

Come detto il frodatore non può solitamente utilizzare il conto gioco come semplice canale per depositare denaro e prelevarlo in quanto comunemente l'utente può prelevare solo quanto vinto. Dopo le frodi di sottoscrizione e quelle relative ai sistemi di pagamento, nella fase di gioco si sostanziano i comportamenti fraudolenti di gioco. Di seguito si descrivono alcuni esempi significativi nel poker online:

- Collusione: tale fenomeno prevede due o più giocatori che giocano allo stesso tavolo e imbrogliano gli altri avversari che sono all'oscuro di tale coalizione. La collusione comporta la condivisione di informazioni con altri giocatori al tavolo da poker, al fine di ottenere un vantaggio sleale, aumentare le loro possibilità di vincere la mano in gioco e ottenere un passaggio di denaro prelevabile (in quanto frutto di vincita) per una eventuale finalità di riciclaggio.
- Chip Dumping: perdita intenzionale di denaro da parte di un giocatore a favore di un altro giocatore ai fini di truffa; tale comportamento è una particolare forma di collusione che, indipendentemente dalla probabilità di vincita, permette il passaggio di denaro prelevabile, in quanto frutto di vincita, da un giocatore all'altro.
- BOT: intelligenza artificiale: sono programmi software che simulano un giocatore autonomo. Tale software può partecipare a più tavoli da gioco prendendo decisioni attraverso l'applicazione di algoritmi predefiniti. L'efficacia dei BOT e la loro abilità nel vincere è con il tempo diventata sempre maggiore. In molti i casi I BOT sono programmati per personificare un giocatore con cui operare collusione e chip dumping.

Ulteriori comportamenti fraudolenti si basano su sofisticati metodi di intercettazione del codice sorgente del gioco per modificarlo e trarne profitto

(alcuni esempi sono: utilizzo delle user interface (UI), disegno di Debugger e Reverse engineering) [58].

Le contromisure che gli operatori adottano per prevenire, identificare e combattere le frodi nel gaming on-line sono frutto di un compromesso che in questo settore così agguerrito è talvolta una scommessa di business. La presenza di controlli di antifrode fornisce una maggiore sicurezza all'operatore e al giocatore stesso che percepisce di trovarsi in un ambiente più sicuro. L'operatore guadagna la fiducia del giocatore e la propria immagine sul mercato viene associata a valori di sicurezza, tutela e professionalità.

D'altra parte le contromisure possono prevedere per loro natura una fruizione meno agevole e immediata del servizio, i blocchi di sicurezza possono agire in modo cautelativo rallentando l'esperienza di gioco di utenti in buona fede, i controlli in ingresso possono scoraggiare giocatori nell'iscriversi a questo piuttosto che a quell'operatore che lascia entrare più facilmente. Il gioco on-line è caratterizzato da una forte presenza di comunità digitali di giocatori che si confrontano su forum e chat in merito ai differenti operatori e ai diversi servizi. I frodatori frequentano tali comunità e qui cercano di danneggiare gli operatori più accorti tentando di orientare gli altri giocatori ad operare su piattaforme e prodotti meno sicuri e più vulnerabili alle frodi.

Ogni operatore considera tali aspetti nell'adozione di strumenti e processi antifrode, e la scelta finale in parte è determinata dalla tipologia di clientela a cui l'operatore si rivolge. Una clientela più tradizionale, esperta e moderata sarà meno attratta da operatori che enfatizzano la facilità di iscrizione, l'assenza di soglie e blocchi e l'enfasi alla totale libertà di comportamento.

Misure IT per il gaming on line

La tecnologia in continua evoluzione ci riporta all'immagine di "Achille e la tartaruga", ovvero ad un inseguimento continuo tra frodatori e creatori di metodi di lotta alle frodi [49].

Appare quindi chiaro che allo sviluppo di normative sempre più stringenti si deve affiancare l'uso di tecnologie sempre più avanzate, quali ad esempio:

- Tracciamento e autenticazione degli utenti che accedono alle sale virtuali, tramite strumenti di Identity and Access Management che permettano l'incrocio dei dati rilevati e che siano in grado di esportare i log degli accessi secondo le esigenze della creazione di un database unico dei giocatori, che fornisca informazioni utili alle autorità competenti;
- Protezione mediante strumenti quali sistemi anti spyware dai tentativi di intercettazione del traffico finalizzato al furto delle identità dei giocatori per trarne vantaggio;
- Tracciamento dell'indirizzo IP dei giocatori, per cercare di individuare geograficamente gli utenti che mettono in atto comportamenti malevoli;
- Monitoraggio e analisi delle sessioni di gioco e delle chat al fine di identificare comportamenti collusivi e schemi di gioco predefiniti riconducibili all'utilizzo di automi (BOT);
- Protezione e personalizzazione della moneta elettronica attraverso certificati elettronici che assicurino la tracciabilità delle movimentazioni di denaro. Standard tecnologici condivisi a livello internazionale per favorire la sinergia e l'omogeneizzazione dei sistemi e dei processi antifrode e limitare l'ostacolo creato dall'eterogeneità normativa tra i singoli stati;
- Tracciamento dei tempi di permanenza e dei passaggi di denaro nei portafogli elettronici, che assicurino la rilevazione di allarmi in caso di possibili comportamenti contrari alla normativa antiriciclaggio;

- Raccolta e analisi, mediante sistemi di Datawarehouse, dei dati provenienti dai sistemi di autenticazione previsti dalla legge con i dati degli operatori che supportano i giocatori on line e con le chat obbligatorie, in modo da rendere sempre più semplici e più veloci l'identificazione di comportamenti illeciti e la relativa comunicazione alle autorità competenti.

2.7 Le frodi ict tipiche di alcuni canali

Verranno di seguito analizzati I metodi di pagamento per alcuni dei canali frequentemente utilizzati.

2.8 Pagamenti on-line

I servizi di ICT offerti dalle aziende hanno subito una rapida evoluzione al fine di aumentare la soddisfazione del cliente, anche per merito di una sempre maggiore diffusione della globalizzazione del mercato attraverso Internet [60].

Tramite questo nuovo insieme di servizi on-line, aventi come scopo principale quello di consentire alle persone di effettuare operazioni fino a qualche anno fa fattibili unicamente di persona, è diventato quindi possibile e sempre più usuale effettuare i cosiddetti pagamenti on-line che possiamo definire come l'insieme delle operazioni effettuate tramite il canale internet che consentono di effettuare movimentazione di denaro.

Alcuni esempi di pagamenti online sono:

- L'acquisto diretto di beni (pagamento tramite carta di credito su portali di ecommerce, bonifico bancario tramite Internet Banking, ricariche telefoniche);

- L'acquisto indiretto di beni tramite servizi intermediari (pagamento tramite Paypal);
- Il trasferimento di denaro tra soggetti privati (money transfer tramite Wester Union, bonifico bancario tramite Internet Banking).

Prevenzione, detection e contrasto delle frodi nel canale "Pagamenti on Line"

La sempre maggiore diffusione dei metodi di pagamento online ha parallelamente favorito lo sviluppo delle frodi ed atti criminali finalizzati alla sottrazione di denaro o dell'identità del pagatore o del venditore.

E' stato quindi necessario ideare e implementare soluzioni per la prevenzione, la detection ed il contrasto delle frodi nei pagamenti on-line. Per i pagamenti online si fa riferimento, mutuando la definizione dal mondo delle carte di pagamento, al caso di "Card-Not-Present" [88].

Si possono suddividere le possibili soluzioni in due categorie primarie, in relazione al soggetto da tutelare [96]:

- Sicurezza Utente Finale;
- Sicurezza Retailer;

Soluzioni per la sicurezza dell'utente finale

- PayPal: permette di utilizzare un canale esterno al sito di e-commerce per effettuare il pagamento. L'utente ha necessità di definire un proprio profilo in PayPal ed otterrà quindi delle credenziali di accesso, che possono contemplare anche la strong authentication;
- Verified-By-VISA/Mastercard Secure Code. Permettono di utilizzare un ulteriore livello di autenticazione, fornito dai circuiti di carte di credito. Visa e MasterCard hanno introdotto questi sistemi per rendere più sicure le

transazioni online. I titolari delle carte devono registrarsi sui siti degli issuer con Verified by Visa o MasterCard SecureCode, quando devono effettuare dei pagamenti online. Il titolare sfrutta un dispositivo token o imposta una propria password personale da utilizzare per i pagamenti online con carta di credito. Tali sistemi permettono agli istituti finanziari di verificare l'autenticità del titolare della carta per conto del retailer;

- Certificati SSL-EV. Installati nei web server del sito di e-commerce, permettono all'utente di verificare l'autenticità di un sito web;

Chiaramente a questi metodi tecnici vanno affiancate da alcune norme di comportamento legate alle principali modalità di truffa. A titolo esemplificativo riportiamo:

- Chi vende a prezzi sensibilmente inferiori alla media della concorrenza deve destare necessariamente sospetti, in quanto nessuno vende rimettendoci del denaro;
- Va sempre verificata presso il sito dell'agenzia delle entrate la partita IVA del negozio on-line, che deve essere obbligatoriamente dichiarata sul sito;
- La reputazione on line: inserendo su google le parole chiave "nome negozio opinioni" è possibile verificare, sui vari siti di comparazione prezzi quale sia il parere degli utenti sul negozio presso il quale si desidera effettuare un acquisto.
- I metodi di pagamento sono uno dei più importanti campanelli d'allarme: i negozi on-line che accettano esclusivamente pagamenti anticipati con bonifico bancario, vaglia veloce e ricariche prepagate e rifiutano il contrassegno devono essere assolutamente guardati con sospetto: dietro un IBAN a volte non si nascondono conti correnti bancari, dunque intestati a persona certa e rintracciabile, ma carte prepagate.

Soluzioni per la sicurezza retailer

- Fraud Prevention: sono soluzioni che, in Real Time, permettono di verificare se da un client sta iniziando un tentativo di frode. Sono sistemi che grazie ad informazioni di intelligence e monitorando le modalità di accesso al sistema sono in grado di prevenire le minacce di frode e disinnescare minacce che ancora non si sono presentate all'interno del perimetro della società;
- Monitoraggio Transazioni: sono soluzioni che, in funzione di vari parametri (quali analisi comportamentale dell'utente, geolocalizzazione, analisi del device, reputazione, etc…), permettono di definire un livello di rischio di una transazione e conseguentemente svolgere determinate azioni (dal richiedere un'autenticazione più forte fino al blocco della transazione stessa);
- Information Discovery: sono sistemi che, esplorando e analizzando liberamente dati strutturati e non strutturati, provenienti dalle fonti più disparate (quali ad esempio i dati delle transazioni, contratti di attivazione, Customer Care, fonti aperte da social network, …), con tecniche di data mining, permettono di correlare fra loro fenomeni, in modo da riconoscere frodi, che in genere non sono facilmente riscontrabili [120].

Principali normative di riferimento per i pagamenti online

Nell'ambito dei pagamenti online punto di riferimento fondamentale è il progetto SEPA (Single Euro Payments Area) che mira ad estendere il processo d'integrazione europea ai pagamenti al dettaglio in euro effettuati con strumenti diversi dal contante, con l'obiettivo di favorire l'efficienza e la concorrenza all'interno dell'area dell'euro [150].

In ottica della realizzazione del progetto SEPA la Comunità Europea ha emesso la Direttiva 2007/64/CE "relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/ 65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva 97/5/CE", recepita in Italia dal Decreto Legislativo 27 gennaio 2010 , n. 11. La Banca d'Italia si è attivata negli anni con una serie di provvedimenti per l'attuazione delle norme Europee e Nazionali. Primo atto e punto di riferimento è il documento "Attuazione del Titolo II del Decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento (Diritti ed obblighi delle parti)".

Il 24 luglio 2013 la Commissione Europea ha varato una nuova direttiva sui servizi di pagamento con cui l'Europa intende creare un mercato unico dei pagamenti digitali, abbassando i costi, aumentando la sicurezza per consumatori e dettaglianti ed imponendo modifiche alle commissioni interbancarie. Tale direttiva dovrà essere attuata dagli Stati Membri.

Una particolare attenzione alla prevenzione delle frodi è stata posta dai cinque principali brand delle carte di pagamento (VISA, MasterCard, American Express, JCB e Discovery). Dopo alcuni tentativi isolati di Visa e di Mastercard, sul finire del 2004, i citati brand hanno fondato il Payment Card Industry Security Standard Council (PCI SSC), che ha emanato, e continua ad emanare, una serie di standard inerenti la gestione delle carte di pagamento a cui tutti i soggetti coinvolti nella memorizzazione, elaborazione e trasmissione di tali informazioni devono attenersi. La PCI DSS è il più importante di questi standard e include requisiti applicabili a qualsiasi azienda che tratti i PAN (Primary Account Number – numero identificativo) delle carte, sia per gestire direttamente i pagamenti dei propri clienti (Merchant) sia per fornire servizi a chi li gestisce (Service Provider) [25]. Lo standard PCI DSS è un mix piuttosto uniforme di aspetti tecnologici, organizzativi

e procedurali, i cui requisiti possono essere schematicamente riassunti nelle seguenti categorie:

- Sviluppo e gestione di una rete sicura;
- Protezione dei dati dei titolari delle carte;
- Manutenzione di un programma per la gestione delle vulnerabilità;
- Implementazione di rigide misure di controllo dell'accesso;
- Monitoraggio e test regolari delle reti;
- Gestione normativa per la sicurezza delle informazioni.

In questo standard è posta un'enfasi sulle verifiche tecnologiche, prevedendo ad esempio che le attività di Penetration Test siano effettuate seguendo una metodologia riconosciuta e vengano previste delle attività di follow-up al fine di verificare i rientri dalle vulnerabilità emerse a seguito delle verifiche. Questa maggior attenzione alle verifiche tecnologiche, unitamente a controlli più rigidi per quanto riguarda la gestione degli accessi logici che fisici, è tesa a migliorare il livello di sicurezza nella gestione dei dati delle carte di pagamento, andando così a prevenire eventuali frodi dovute all'intercettazione dolosa o involontaria di tali dati. Oltre ad assolvere tutti i requisiti di gestione dell'infrastruttura di rete e di sicurezza fisica e logica, è necessario effettuare periodicamente attività di natura procedurale, riassunte nel Self Assessment Questionnaire (SAQ). Le attività di verifica da parte del PCI Council sono in costante aumento, e possono avere coneguenze come multe ed esclusioni dal circuito al fine di preservare i dati della carte di pagamento da frodi. Oltre alla PCI DSS, il PCI SSC ha pubblicato altri standard che indirizzano due aree critiche per la gestione delle frodi e della sicurezza nel trattamento delle carte di credito. Il primo è il Payment Application Data Security Standard (PA-DSS), che affronta il tema della sicurezza delle applicazioni per il pagamento con carta di credito. In seguito, PCI-SSC ha pubblicato uno standard per la realizzazione dei terminali attraverso cui può

essere inserito un PIN (PCI-PED) ed uno standard per la sicurezza fisica e logica nella produzione di carte di credito, che copre ad esempio la possibilità di sottrarre carte o informazioni di personalizzazione già in fase di produzione.

2.9 Mobile

La diffusione pervasiva dell'utilizzo degli smartphone all'interno della vita quotidiana ha consentito lo sviluppo di una serie di servizi di pagamento e commerciali usufruibili tramite canale mobile. In particolare, studi specifici sul canale distinguono i servizi fruibili in mobile banking, mobile payment, mobile commerce e mobile service. Per quanto concerne il primo strumento relativo all'accesso al proprio account di e-banking tramite apposita applicazione mobile, i rischi sono legati prevalentemente all'aumento del numero di malware ed alla sofisticazione degli attacchi sulle diverse piattaforme mobili (Android è la piattaforma più colpita da software malevoli) ed all'uso di tecniche di social engineering in grado di sfruttare l'utilizzo di social network dagli smartphone e la scarsa diffusione di strumenti di difesa a bordo dei device [44]. Le ultime analisi effettuate sui malware mobile dimostrano inoltre come l'infezione dei dispositivi non avvenga solamente mediante il download e l'installazione di app malevole da fonti non ufficiali, ma anche tramite bluetooth e phishing.

Per quanto concerne le attività di mobile payment, mobile commerce e mobile service, l'analisi del device è effettuata in relazione al contesto di utilizzo del dispositivo distinguendo tra "Remote" e "Proximity" a seconda della distanza tra cliente ed esercente e della tecnologia di scambio sottostante (il "Remote" sfrutta la rete cellulare, mentre il "Proximity" si basa su tecnologie a corto raggio). I differenti scenari di mobile payment sono mostrati nella seguente figura:

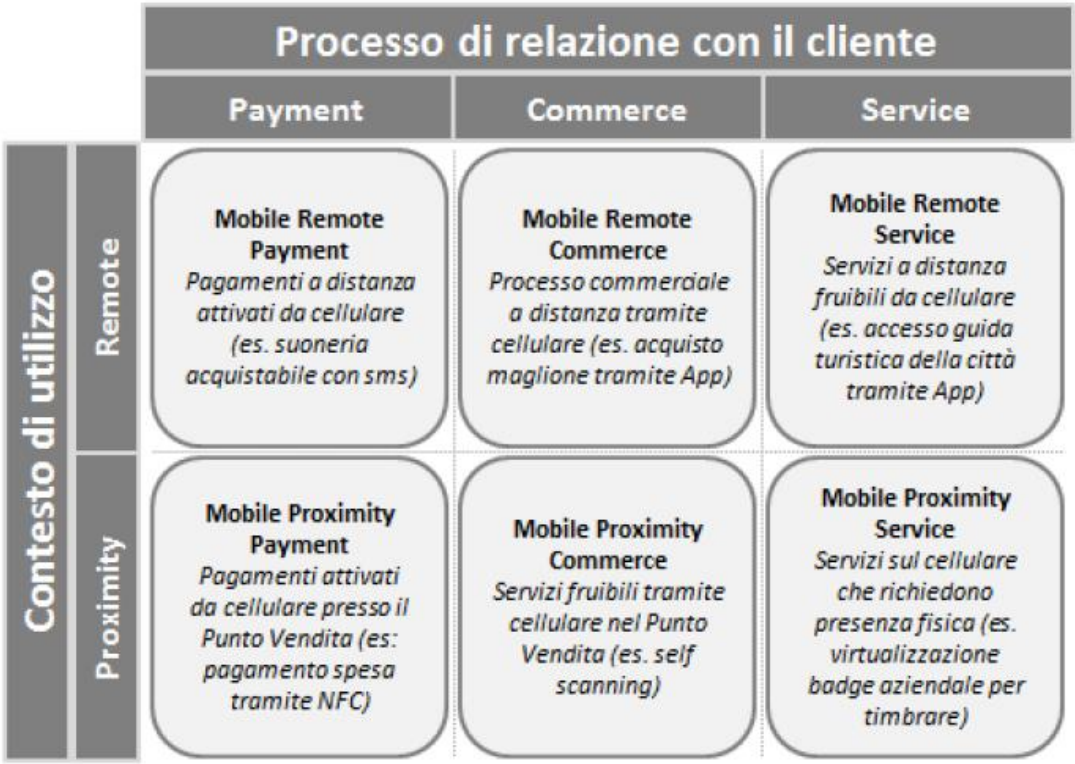


Figura 19: contesto di utilizzo dei pagamenti tramite device

Tra i servizi di mobile proximity, tra cui quelli di marketing, di virtualizzazione di ticket e di supporto all'acquisto, il rischio frode si sviluppa in modo omogeneo per le controparti interessate, cioè esercente e cliente. In particolare però, per quanto concerne l'ambito dei pagamenti, è bene distinguere tra tecnologie che prevedono che le credenziali di pagamento siano fisicamente presenti durante il pagamento (nella SIM dell'operatore telefonico, piuttosto che su Micro SD), dai casi in cui tali credenziali sono memorizzate nel cloud (spesso attivate tramite lettura di QR Code, fotocamera OCR o riconoscimento visivo). L'autenticazione e sicurezza dei dati personali tramite uno strumento integrato nel dispositivo mobile offre maggiori tutele a possibilità di attacco da parte di software malevoli, ma espone l'utente a rischi dovuti a furto, smarrimento e accesso illegittimo al device. Inoltre, il fatto che tali dati vengano veicolati tramite tecnologia NFC (Near

Field Communication) non elimina i rischi potenziali di frodi attuate mediante ad esempio il “man in the middle” [22].

Tra i servizi di proximity è bene citare anche l'utilizzo di Mobile POS da parte degli esercenti per minimizzare i costi di gestione del terminale. Nel caso specifico sono state ben delineate le raccomandazioni per evitare che vi sia accesso illecito (sia fisico che logico) al dispositivo, nonchè per evitare che il device venga infettato da malware (esempio un software in grado di leggere i dati digitati sullo smartphone come il PIN fungendo anche da keylogger) e sia utilizzabile in caso di furto e smarrimento. Infine, lo sfruttamento delle tecnologie di geolocalizzazione dello smartphone consentono di abilitare pagamenti selettivi agli utenti, così da fornire servizi mirati, come pagamenti di biglietti di parcheggi, autobus, musei nel perimetro fisico del potenziale consumatore.

Prevenzione, detection e contrasto delle frodi nel mondo mobile

Un efficace sistema di presidio e contrasto delle frodi, nel mondo mobile così come già visto in generale, si basa su una strategia di prevenzione, monitoraggio e reaction. Cio’ implica che, nelle aziende il cui business sia lo sviluppo di servizi su canale mobile, sia necessaria la presenza [1]:

- Di un modello di governance dei rischi che coinvolga non solo la struttura di Fraud Management ma tutte le funzioni aziendali che partecipino al ciclo di vita dei prodotti e dei servizi;
- Di personale specificatamente formato, esperto e organizzato per un efficace trattamento delle frodi;
- Di adeguate e sempre aggiornate tecnologie a supporto dell’attivita’ di pronta individuazione delle frodi in corso;
- Di sinergie strutturate con comunita’ nazionali ed internazionali di fraud analyst.

Fase di prevention

Come prima azione di prevention, è fondamentale che i servizi in mobilità che vengono offerti alla clientela siano sottoposti ad una approfondita analisi da parte delle aree aziendali che si occupano di sicurezza e di Fraud Management: la stretta collaborazione di queste due strutture con il marketing consente infatti di individuare da subito possibili rischi frodi insiti nel progetto e vulnerabilità, sia di carattere commerciale sia di carattere strettamente tecnico. Questa analisi consente innanzitutto di effettuare una corretta valutazione dei rischi che andrà sottoposta al Management. Allo scopo di prevenire le frodi in ambiente mobile, è fondamentale che i servizi sviluppati tengano conto di alcuni requisiti di base, tra cui, ad esempio [96]:

- Precisa definizione di ruoli e responsabilita', da riportare poi anche in ambito contrattuale, per la gestione delle frodi e dei rischi finanziari, in particolare nel caso di servizi offerti in ecosistemi complessi (come, ad esempio, avviene con le tecnologie NFC), in cui possono essere coinvolti diversi enti (gestore di telefonia mobile, banche, provider di applicazioni, produttore schede SIM etc...);
- Sviluppo sicuro delle applicazioni mobili, con particolare riferimento alle applicazioni di pagamento, secondo le linee guida Owasp per lo sviluppo sicuro, il test e la code review, o gli standard internazionali adottati per i sistemi di pagamento in mobilità;
- In generale, grande attenzione per una corretta implementazione dei meccanismi di autenticazione, l'uso di protocolli criptati per lo scambio di credenziali, dati personali e dati di pagamento, il rapido aggiornamento e diffusione delle patch di sicurezza delle applicazioni, il patching dei sistemi coinvolti e l'esecuzione di Vulnerability Assessment e Penetration Test sulle infrastrutture tecnologiche.

- Precisa definizione di tutti i processi, tecnologici e procedurali, destinati all'identificazione del cliente e alla verifica dei dati forniti dallo stesso, sia nel momento della sottoscrizione e dell'utilizzo del servizio da parte del cliente, sia nella fase di supporto al cliente da parte dell'erogatore del servizio.

Fase di detection

L'obiettivo della fase di detection è di garantire una quotidiana e costante valutazione del rischio sulla base della quale stabilire di volta in volta le priorità, la quantità di risorse da dedicarvi, il modello organizzativo piu' efficiente da adottare per il contrasto delle frodi. A supporto di questa attivita' giocano un ruolo fondamentale i Fraud Management System, che, nel caso del monitoraggio delle transazioni online, utilizzano alcuni criteri tra i quali [150]:

- IP detection: rende possibile la localizzazione dell'utente ed evidenzia un potenziale rischio anche in base ad una lista precostituita di ip particolarmente critici;
- Device fingerprinting: oltre ad identificare l'ip, è in grado di identificare altri parametri identificativi del device (ad esempio la versione del browser, Sistema Operativo, etc..) e di verificare se lo stesso è già stato coinvolto in precedenti fenomeni fraudolenti;
- Order velocity monitoring: segnala gli ordini che sono stati sottomessi in un certo intervallo temporale da un certa carta con un determinato ip address;
- Positive lists: liste di clienti "buoni", sulla base degli ordini precedentemente effettuati;
- Negative lists: liste di clienti "cattivi" sulla base di ip, numeri di carte di credito, device ID, nomi ed indirizzi;

- Shared lists: blacklist/whitelist condivise tra diverse aziende/operatori.

E' pero' necessario che i sistemi antifrode vengano affiancati da tecniche di controllo basate anche sull'analisi economica dei servizi, che sono in grado di evidenziare quelle situazioni in cui vengono generati costi anomali per l'azienda, sfuggiti ai metodi di detection tradizionale [64].

Fase di Reaction

La fase di reaction mette in atto le procedure di gestione delle situazioni critiche, prevedendo la sospensione dei servizi oggetto di frode. La gestione dell'incidente prevede l'individuazione dei meccanismi che hanno originato la frode e la definizione, in breve tempo, di un piano d'azione da condividere con il Management [25].

Le normative e gli standard di sicurezza

Nell'ambito dei servizi di mobile payment particolare rilevanza assumono le soluzioni di mobile POS, ovvero quelle soluzioni che, grazie a un piccolo device (dongle), abilitano ad esempio un semplice smartphone, in uno strumento in grado di accettare qualsiasi carta di pagamento al pari di un POS tradizionale. Gli standard di sicurezza di settore si stanno evolvendo per adeguare le specifiche di sicurezza alle nuove tecnologie che, inevitabilmente, introducono nuovi scenari di frode che ad oggi devono essere mitigate da opportune misure di sicurezza. Attualmente a livello internazionale gli standard di riferimento sono [150]:

- EMV: standard internazionale per le carte di credito e di debito basate su tecnologia a chip nonchè per le apparecchiature ATM e POS;
- PCI: è costituito da un insieme di standard aperti per la protezione dei dati (DSS), di standard di protezione dei dati per le applicazioni di pagamento (PA-DSS) e sicurezza delle transazioni PIN (PTS);

- Standard di Circuito, a livello internazionale principalmente promossi da VISA e MasterCard, si basano sugli standard EMV e PCI e definiscono criteri comuni di sicurezza anche nella forma di best practice. A livello nazionale vi sono invece le Specifiche Tecniche e Funzionali emanate e referenziate dal Consorzio BANCOMAT, che regolano il funzionamento, l'operatività e il processing dei pagamenti sui Circuiti BANCOMAT e PagoBANCOMAT;

A questi standard di sicurezza si aggiunge anche l'iniziativa "SEPA for Mobile" del Consiglio Europeo per i pagamenti (EPC) che, nell'ambito dell'armonizzazione dei sistemi di pagamento nella Single Euro Payments Area (SEPA), promuove lo sviluppo di un ecosistema sicuro per i pagamenti su canale mobile tramite la pubblicazione di white paper sui servizi mobile payment e mobile wallet e linee guida sulla interoperabilità delle tecnologie dei dispositivi mobili.

Recentemente infine, la Banca Centrale Europea ha pubblicato un documento intitolato "Recommendations for the security of mobile payments" riguardante le misure di sicurezza dei provider dei servizi e delle applicazioni di pagamento in mobilità al fine di mitigare le frodi per le tipologie di Mobile Wallet, Mobile Proximity Payment e P2P Payment [147].

2.10 Carte di Credito

Le carte di pagamento si suddividono in carte di debito, comunemente denominate bancomat, carte prepagate e carte di credito. Mentre le carte di debito e le prepagate hanno un addebito sul conto corrente o sul saldo della carta contestuale all'effettuazione del pagamento, le carte di credito possono essere, a seconda dell'emittente, bancarie o non bancarie, e a seconda della modalità di saldo delle spese "charge" (addebito mensile posticipato in un'unica soluzione) o "revolving" (addebito delle spese posticipato in importi rateali) [24].

La letteratura suddivide gli schemi di frode sulle carte di pagamento utilizzando come discriminante la presenza della carta stessa, per cui si configurano le "plastic fraud" o le frodi perpetrate in ambiente "card not present" [150].

Tra le plastic fraud, oltre ai casi di esecuzione della frode a seguito di furto o smarrimento della carta da parte del titolare (tipicamente in modo congiunto al PIN della carta) si configura la fattispecie di carta contraffatta con cui i dati della carta vengono materialmente registrati, trasferiti, clonati o sostituiti al fine di consentire transazioni illecite. Una delle modalità più ricorrenti per il furto dei dati della carta codificati nella banda magnetica è costituita dall'apposizione di uno skimmer sui terminali ATM (Automatic Teller Machine) o POS (Point Of Sale). Tale pratica, utilizzata sinergicamente a tecniche di cattura del PIN come l'apposizione di una microtelecamera o di una pin pad, nonchè associata a tecniche di shoulder surfing, che consente di perpetrare transazioni fraudolente con tecnologia a banda magnetica sugli ATM e sui POS non EMV compliant. Oltre alla modalità di frode sugli ATM appena descritta si possono distinguere tre tipologie di frodi che si differenziano ognuna per il grado di tecnologia adoperata nonché dall'efficacia stessa dell'evento fraudolento [51]:

- Cattura carta (o "tasca libanese"): è una tecnica che prevede la cattura della carta mediante l'inserimento di un elemento metallico all'interno della feritoia dell'ATM. Tale frode è completata con l'associazione di una tecnica di manomissione volta ad identificare il PIN, come ad esempio quelle precedentemente descritte;
- Compromissione dati carta: è la tecnica che prevede l'installazione di strumenti capaci di leggere i dati delle carte (as esempio uno skimmer) e di memorizzare o inviare gli stessi tramite strumenti Wi-Fi a supporti esterni;

- Cattura banconote (Cash Trapping): è una tecnica che prevede l'applicazione di elementi esterni artigianali tesi a compromettere lo sportellino (shutter) dell'ATM in modo da trattenere le banconote erogate;

Le frodi di tipo cash trapping sono spesso caratterizzate dalla relativa semplicità ed elevata efficacia della tecnica di manomissione e dalla rudimentalità degli strumenti utilizzati, ma che consentono un'immediata "riscossione" delle banconote da parte del frodatore. Di seguito vengono mostrate le tipologie di frodi cash trapping:

Tipologie di cash trapping	Modalità
Frode a "tappo"	Apposizione di un frontalino con pellicola biadesiva per la cattura delle banconote in fase di erogazione.
Frode a "forchetta"	Inserimento di un artefatto (es. forchetta metallica) che impedisce l'erogazione delle banconote apposta durante un prelievo effettuato con una carta "civetta" (carte prepagate o al portatore spesso emesse in un paese diverso rispetto a quella dove viene utilizzata e dove sono applicati minori misure di controllo sul titolare carte).
Frode "reversal"	Esecuzione di una prima operazione di prelievo per l'inserimento di una "forchetta" metallica seguita da una seconda operazione di prelievo senza addebito sulla carta sfruttando le vulnerabilità software dell'ATM.

Figura 20: Tipologia di cash trapping

Infine, tra le plastic fraud rientrano anche la fattispecie di "boxing", cioè l'intercettazione della carta tra l'invio della stessa da parte dell'emittente e la consegna al titolare, e di "carding", che consistono rispettivamente nella falsificazione materiale di una carta ex novo, e sostituzione o cancellazione dei dati presenti nella carta.

Con l'introduzione degli standard EMV e della Payments Service Directive (PSD) gli schemi tipici delle frodi si sono evoluti tendendo sempre più alle tipologie di frodi riconducibili alla classificazione di "card not present".
Le frodi perpetrate in ambiente “card not present” fanno tipicamente riferimento alle transazioni effettuate su canale internet e MO/TO (Mail Order e Telephone Order) [71]. Tra le diverse condotte criminose, le più diffuse nel cosiddetto furto d'identità informatico vengono attuate con tecniche di "sniffing", "key logging" e "man in the middle": in tutti i casi vi è un'intercettazione o un dirottamento dei dati della carte che vengono trasmessi su rete telematica, tra host, o digitati e salvati su hardware/software. Sempre di maggior rilevanza e diffusione sono le fattispecie di "social engineering", "phishing", "smishing" con cui vi è un acquisizione fraudolenta delle informazioni sulla carta da parte di falsi operatori bancari o siti istituzionali che richiedono via telefono, e-mail e sms i dati necessari all'effettuazione di successive transazioni illecite [105].

Prevenzione, detection e contrasto delle frodi nel settore carte di credito

Le tecniche di contrasto alle frodi perpetrate tramite ATM sono sia di tipo hardware/software sia di standard di sicurezza di Circuito [145]:

- Soluzioni hardware: consistono nell’irrobustimento dei dispositivi di interazione con il titolare carta (ad esempio la protezione esterna della bocchetta di uscita delle banconote, l’installazione di anti-skimmer nel lettore carta) e nel posizionamento di sensori in grado di rilevare eventuali anomalie dei dispositivi (ad esempio il timeout dell’apertura dell’erogatore banconote);
- Soluzioni software: patch sugli applicativi di gestione dello sportello per massimizzare i controlli logici sui dispositivi hardware (ad esempio il timeout ritiro banconote/carta, sequenza operazioni);

- Soluzioni di Circuito: mediante l'irrobustimento e aggiornamento degli standard di sicurezza (esempio EMV, PCI DSS) da parte dei principali Circuiti internazionali e nazionali.

Per quanto concerne le frodi perpetrate attraverso l'uso fraudolento delle carte di pagamento si possono distinguere quattro tipologie di misure di prevenzione:

- Tecnologie EMV (Europay Mastercard Visa), 3DS (3D Secure): sono standard tecnologici legati a flussi di operazioni di autenticazione che aiutano nella prevenzione delle frodi basate su furti di identità (sia Card present che Card not present);
- Metodi di Autenticazione: questi sono il maggior oggetto degli investimenti di tutti gli attori di mercato per il rafforzamento della prevenzione degli usi illeciti. Possiamo distinguere:
    - PIN: utilizzo di un codice identificativo durante i pagamenti, direttamente legato allo standard EMV;
    - OTP (One Time Password): codice random assegnato per ogni singola operazione e legato al device che identifica l'utente (nasce dallo standard 3DS);
    - Risk Authentication (Smart Authentication): legato anch'esso agli standard 3DS, è sicuramente il metodo più innovativo. L'autenticazione si basa su parametri legati a vari fattori di rischio inseriti nel profilo dell'utente. L'autenticazione richiesta sarà più rigida in base al discostarsi da tali parametri di rischio. Si tratta, ad esempio di mappare Indirizzo ip, Browser utilizzato, Mac Address, Versione di Java utilizzati dall'utente, creando così un Id univoco che rende più facile l'autenticazione (si potrebbe arrivare, attraverso questa identificazione di "Green Devices", a non richiedere nemmeno l'inserimento di una password). Nel momento in cui la

richiesta arriva da una fonte che si discosta dai parametri tracciati, il metodo di autenticazione diventa più rigido, richiedendo ulteriori informazioni all'utente. Un problema da affrontare potrebbe essere quello del trattamento dei dati personali, probabilmente ovviabile attraverso una corretta e trasparente definizione dei termini contrattuali tra chi emette la carta e il cliente finale;

  - Geo localizzazione: altro settore in sviluppo è quello di basare il livello di autenticazione sulla posizione geografica del device che opera, in base alla distanza dalla posizione consueta dell'utente registrato;

- Autorizzazione: la tendenza è quella di rendere sempre più in " Real Time" il processo di autorizzazione, allontanandosi dal tradizionale metodo di elaborazione di chiusura "batch" delle transazioni, operata a fine giornata. Questa avviene già per le carte di debito, ma non ancora per tutte le carte di credito;
- Metodi "tradizionali": sono ormai considerati obsoleti i metodi basati su raccolta diretta dei dati delle transazioni sospette da parte delle autorità competenti, rese sempre più difficili dalla globalizzazione dei mercati sui quali si opera con strumenti di pagamento sempre più "virtuali".

Per quanto concerne le fattispecie di "social engineering" sicuramente è fondamentale, al di là delle tecniche di sicurezza implementate dagli istituti che emettono le carte, che si diffonda la cultura della prevenzione. Bisogna educare gli utenti, anche lontani dalla tecnologia, ad adottare un comportamento più attento. A titolo di esempio sono citati: fare caso al livello di crittografia dei siti usati per fare acquisti (HTTPS), diffidare delle richieste di dati personali pervenute attraverso gli strumenti informatici o telefonici, anche se provenienti da

fantomatici “amici” del social network utilizzato o mascherate sotto forma di proproste commerciali imperdibili.

3. PROGETTAZIONE DEL MODELLO DI FRAUD DETECTION

Lo scopo di questa tesi è quello di progettare ed implementare un modello che rilevi le transazioni fraudolente eseguite con carte di credito, sfruttando le tecnologie disponibili al giorno d'oggi, come il machine learning.

Il modello è stato concepito tenendo conto che l'utente finale necessita di un ambiente di simulazione personalizzato, nel quale poter modificare i parametri con lo scopo di trarre delle conclusioni.

Le specifiche che deve soddisfare il modello sono quindi le seguenti:

- Permettere all'utente di ricevere in input dati provenienti da fonti variegate;
- Fornire un ambiente di sviluppo comprensivo degli strumenti per la creazione e la modifica del modello;
- Permettere all'utente di alterare i parametri in gioco per testare il comportamento del modello;
- Permettere di analizzare i risultati con l'ausilio di grafici;
- Permettere la connessione con applicazioni esterne.

Dopo un'accurata ricerca si è scelto di utilizzare come ambiente di programmazione Microsoft® Azure Machine Learning.

3.1 Il Machine Learning

I dati possono contenere informazioni nascoste, soprattutto se se ne possiedono molti. Procedendo ad un esame strutturato ed intelligente, è possibile rilevare schemi che possono aiutare a risolvere un problema [17]. Questo è esattamente ciò che fa il machine learning: esamina grandi quantità di dati alla ricerca di schemi, che consentono successivamente di riconoscere gli stessi in nuovi dati per creare così previsioni migliori, risultando quindi di aiuto nel processo di creazione di applicazioni intelligenti [19].

Nel caso trattato in questa tesi, si vuole creare un modello in grado di determinare, con un alto grado di precisione ed accuratezza, se una transazione effettuata con con carta di credito è fraudolenta o meno. Utilizzando un approccio classico per la creazione di una soluzione software, si potrebbe assolvere lo scopo scrivendo il codice con l'uso di un linguaggio di programmazione [54]. Avendo però a disposizione dei dati sul problema che si sta cercando di risolvere, è possibile utilizzarli per cercare una soluzione più efficace. Contestualizzando tutto ciò nel caso di interesse, supponiamo di cercare l'approccio migliore per rilevare le frodi nelle transazioni con carte di credito, avendo a disposizione i dati mostrati in figura 21 [37]:

Name	*Amount*	*Fraudulent*
Smith	$2,600.45	No
Potter	$2,294.58	Yes
Peters	$1,003.30	Yes
Adams	$8,488.32	No

Figura 21: esempio di dati transazionali

La cosa positiva di avere pochi dati è di poter riconoscere uno schema logico semplicemente osservandoli. D'altro canto, questa metodologia potrebbe indurre

ad un errore, giungendo così a conclusioni sbagliate [79]. Osservando quindi la figura 21 si potrebbe modellare lo schema logico identificando come frodatore chiunque abbia il nome che inizia con la "P", che probabilmente non è corretto. Avendo a disposizione più dati, le probabilità di trovare uno schema comportamentale più accurato e preciso aumentano, ma ciò comporterebbe una difficoltà maggiore nella rilevazione della logica stessa. Ad esempio, supponiamo di avere l'insieme di dati sulle transazioni con carta di credito mostrato nella figura successiva:

Name	***Amount***	***Where Issued***	***Where Used***	***Age of Cardholder***	***Fraudulent***
Smith	$2,600.45	USA	USA	22	No
Potter	$2,294.58	USA	RUS	29	Yes
Peters	$1,003.30	USA	RUS	25	Yes
Adams	$8,488.32	FRA	USA	64	No
Pali	$200.12	AUS	JAP	58	No
Jones	$3,250.11	USA	RUS	43	No
Hanford	$8,156.20	USA	RUS	27	Yes
Marx	$7,475.11	UK	GER	32	No
Norse	$540.00	USA	RUS	27	No
Edson	$7,475.11	USA	RUS	20	Yes

Figura 22: esempio di dati transazionali

Con questi dati a disposizione, è immediato riconoscere che l'ipotesi fatta precedentemente, ovvero che tutti i nomi che iniziano con "P" sono autori di transazioni fraudolente, non può essere corretta. Si potrebbero quindi fare delle supposizioni sulle persone che hanno un'età all'incirca di venti anni, le cui carte di credito sono state emesse negli Stati Uniti e poi usate in Russia. Anche questa analisi potrebbe identificare dei potenziali sospetti, ma guardando il cliente di nome "Norse", ci si rende subito conto che non si adatta allo scopo. La verità è

che lo schema supportato dai dati è questo: una transazione è fraudolenta se il titolare della carta ha circa venti anni, la carta è stata emessa negli Stati Uniti ed utilizzata in Russia e l'importo è superiore a $1.000. Avendo a disposizione del tempo, probabilmente sarebbe possibile capirlo, visto che i dati a disposizione non sono molti.

Supponiamo ora di non avere solo dieci record con cui lavorare ma ad esempio dieci milioni, e per ciascun record di avere non solo sei colonne di dati ma sessanta. Probabilmente dietro ad una numerosità di dati così elevata si nascondono degli schemi utili per determinare quali transazioni siano o meno fraudolente, che non è però possibile semplicemente ricorrendo all'osservazione dei dati. Approcciando quindi il problema con l'uso di tecniche statistiche [84] per trovare degli schemi di comportamento in grandi quantità di dati, è possibile arrivare ad una soluzione consistente in un tempo ragionevole [67].

Questo è esattamente ciò che fa il processo di machine learning [77]: applica tecniche statistiche a grandi quantità di dati, trovando schemi comportamentali che vengono usati per predire gli stessi in nuovi set dati, diminuendo o aumentando così il rischio di accadimento delle casistiche di interesse. Una volta validato, il modello viene connesso con applicazioni esterne, che forniscono in input dati strutturati in maniera corretta [57]. Per quanto riguarda il rilevamento delle frodi, ad esempio, l'applicazione deve fornire informazioni sulle transazioni, come l'importo, l'account, il luogo di emissione della carta ed il luogo di utilizzo. Il modello creato restituirà quindi una probabilità indicante se la transazione sia fraudolenta o meno.

Questa tecnologia può essere utilizzata non solo nel campo dell'antifrode [56], ma per esempio per prevedere i ricavi futuri di un'organizzazione, determinare se un cliente di un operatore di telefonia mobile è probabile che passi ad un altro fornitore, decidere quando un motore necessita di manutenzione, consigliare film

ai clienti abbonati ad un servizio o qualsiasi altra cosa in cui siano disponibili dei dati storici. Tutto ciò che serve, quindi, sono dei dati, un software di machine learning che impari da quei dati e, ovviamente, delle persone con competenze specifiche che sappiano usare quel software [65].

Azure Machine Learning [129] è un servizio in cloud offerto da Microsoft® che permette di implementare il processo di machine learning su grandi quantità di dati. Essendo in cloud, il suo utilizzo richiede solo un browser web ed una connessione internet.

3.2 Il Processo di Machine Learning

In questo paragrafo sarà effettuato uno sguardo approfondito sugli step di processo che vengono applicati nella creazione di un modello basato sul machine learning [78]. I macrostep di processo si sviluppano come mostrato in figura 23:

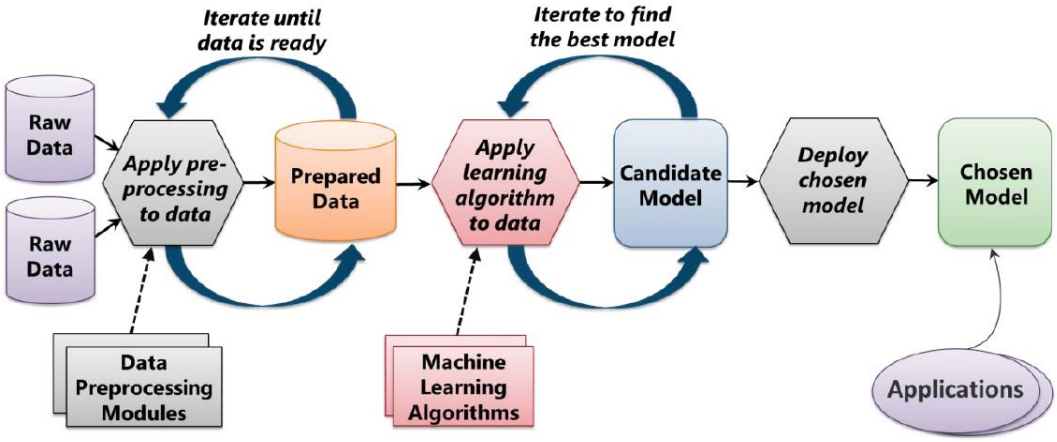


Figura 23: step di processo di un modello di machine learning

Il machine learning inizia con i dati a che si hanno a disposizione, che sono di tipo grezzo: più se ne posseggono, più possibilità si hanno di ottenere migliori risultati. Nell'era attuale, quella dei big data, la disponibilità di dati grezzi non risulta essere affatto un problema [48], quindi la scelta di quelli corretti con cui lavorare è di

fondamentale importanza. Ad esempio, quali dati dovrebbero essere usati per rilevare le frodi con carta di credito? Alcuni risultano essere ovvi, come l'età di un cliente, il paese nel quale la carta è stata emessa ed il luogo in cui la carta viene utilizzata. Ma potrebbero essere rilevanti anche altri dati, come l'ora ed il giorno in cui la carta viene utilizzata, il tipo di struttura in cui viene utilizzata e forse anche il clima al tempo di utilizzo. Determinare i dati più rilevanti per un progetto di machine learning è una parte fondamentale del processo, ed è un'area in cui gli esperti dei vari settori di business hanno un ruolo fondamentale [34].

Qualunque siano i dati scelti, spesso non sono nelle giuste condizioni per essere utilizzati direttamente [36]. Nel rilevamento delle frodi con carta di credito, ad esempio, i dati grezzi potrebbero contenere voci duplicate per alcuni clienti, magari con informazioni contrastanti, oppure delle mancanze di informazioni in alcuni campi, come ad esempio dove sono state emesse o utilizzate le carte di credito. Nei progetti di machine learning i dati vengono elaborati come mostra la Figura sopra 23 [20]:

- Fase di pre-processing: i dati ricevuti in input vengono aggregati e processati per renderli pronti all'addestramento;
- Fase di scelta dell'algoritmo: il modello viene addestrato con l'uso dei dati processati e di un algortimo statistico;
- Fase di deployment: una volta testato e validato il modello, si procede al rilascio dello stesso.

L'obiettivo della pre-elaborazione dei dati è creare quelli che vengono chiamati dati preparati. Come mostrato in figura 23 è un processo di tipo iterativo, con diversi moduli di pre-elaborazione applicati ai dati grezzi [37].

Lo step relativo alla creazione dei dati preparati a partire da quelli grezzi, può richiedere spesso molto del tempo impiegato in un progetto di machine learning.

Una volta che si hanno a disposizione i dati preparati, si può procedere alla ricerca del miglior modo per risolvere il problema su cui si sta lavorando. Per fare questo vengono usati algoritmi di apprendimento automatico da applicare ai dati preparati, che utilizzano analisi statistiche, come una semplice regressione fino a tecniche più complesse, come gli alberi decisionali [36].

L'obiettivo è quindi quello di determinare quale combinazione tra gli algoritmi di machine learning ed i dati preparati genera i risultati più consistenti. Una volta ottenuti i risultati desiderati, è possibile connettere al modello le applicazioni esterne per rispondere alla domanda principale che ha motivato l'analisi, che nell'ambito del caso di interesse è determinare se una transazione è fraudolenta o meno. È inoltre importante comprendere che un modello in genere non restituisce una risposta di tipo binario ma, al contrario, restituisce una probabilità compresa tra zero ed uno. Decidere cosa fare con la probabilità risultante è generalmente una decisione commerciale. Ad esempio, se un modello di rilevamento frodi derivate da transazioni con carta di credito restituisce una probabilità di 0,9, è molto probabile che la transazione venga contrassegnata come fraudolenta, mentre una probabilità del valore di 0,1 consentirà l'elaborazione normale della transazione. Quando però il modello assegna una probabilità di frode di 0,5, la decisione di accettare o meno il rischio di consentire il regolare processo della transanzione verrà, come detto, presa in funzione di logiche commerciali [65].

3.3 Azure machine learning

Molti aspetti del processo di machine learning non sono semplici. Ad esempio, capire come devono essere trattati i dati per creare i dati preparati, quali combinazioni di dati preparati e algoritmi di apprendimento automatico dover

usare per creare il modello migliore risulta essere un'operazione con un grado di di complessità alto.

Per semplificare questo processo, Azure Machine Learning fornisce diversi componenti [151]. La Figura 24 mostra quali sono questi componenti e dove si inseriscono nel processo di apprendimento automatico:

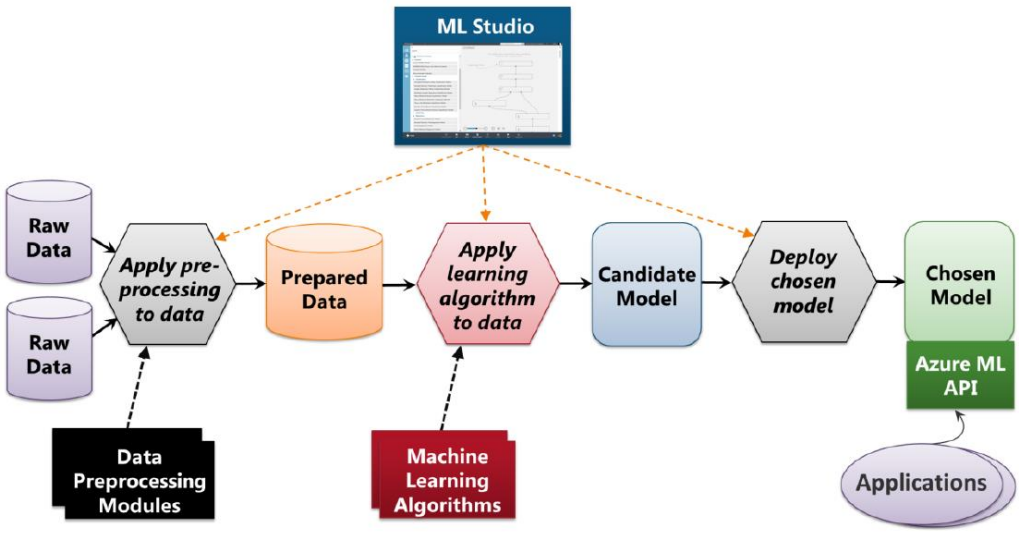


Figura 24: Azure Machine Learning

I componenti forniti da Azure ML sono i seguenti:

- Un ambiente grafico che può essere utilizzato per controllare il processo dall'inizio alla fine;
- Un insieme di moduli di pre-elaborazione dei dati;
- Un insieme di algoritmi di machine learning;
- Un'API ML di Azure che consente alle applicazioni di accedere al modello.

La Figura 25 mostra un esempio dell'interfaccia utente fornita da questo strumento:

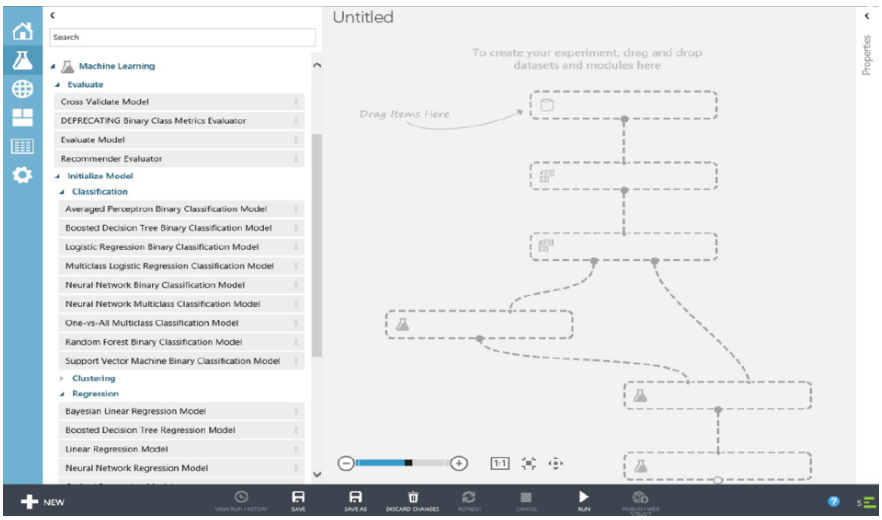


Figura 25: Ambiente di lavoro in Azure Machine Learning

Come suggerisce la figura, Azure Machine Learning consente all'utente di trascinare e rilasciare set di dati, moduli di pre-elaborazione dei dati, algoritmi di apprendimento e altro sulla superficie di progettazione, collegandoli tra loro graficamente e quindi eseguire il risultato. Machine Learning Studio è quindi un unico strumento per il controllo dell'intero processo di apprendimento automatico.

3.4 Fasi progettuali del machine learning

Preparazione dei dati

Come accennato in precedenza, ottenere i dati in una forma pronta da poter essere processata da algoritmi di machine learning può richiedere molto tempo. La Figura 26 aiuta a capire il processo [129]:

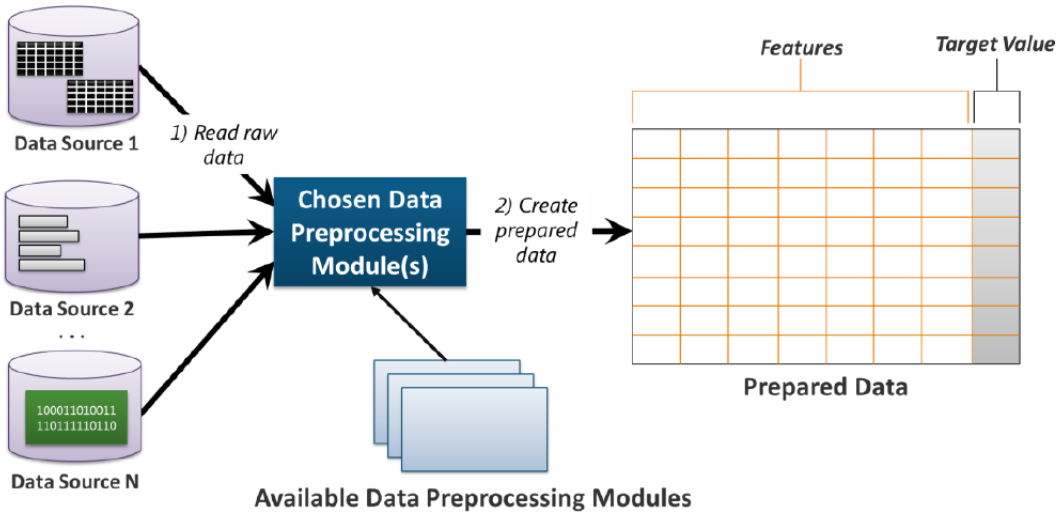


Figura 26: Preparazione dei dati

Come mostra la figura, i dati preparati vengono archiviati come tabella. È possibile che i dati grezzi provengano da fonti disparate, come ad esempio un archivio NoSQL, un DocumentDB di Azure, dati binari archiviati in Hadoop ed altro. Per trasformare questi dati grezzi in dati preparati è necessario quindi poter leggere da più origini di dati (passaggio 1, figura26), per poi processarli attraverso vari moduli di preelaborazione dei dati per creare i dati preparati (passaggio 2, figura 26). Microsoft azure Machine learning gestisce nativamente tutto il processo, e questo rappresenta un vantaggio strutturale di non poco conto.

Azure Machine Learning offre quindi una varietà di moduli di pre-elaborazione dei dati, tra i quali:

- *Clean missing data*, che consente ad un utente di Azure Machine Learning di inserire i valori mancanti in un set di dati. L'utente potrebbe scegliere ad esempio di sostituire tutti i valori mancanti con zero, o sostituire ogni valore mancante con la media, la mediana calcolate rispetto agli altri valori nella relativa colonna della tabella [131];

- *Project Columns*, che rimuove le colonne non utili. Ad esempio, due colonne nella tabella potrebbero contenere dati che sono altamente correlati tra loro. In questa situazione, il processo di apprendimento automatico necessita solo di una delle due colonne. Questo modulo di pre-elaborazione dei dati consente all'utente di eliminare le colonne in un set di dati che non sono utili [132];
- *Metadata Editor*, che consente di modificare i tipi di colonne in un set di dati [130];
- *Apply Math Operations,* che consente di eseguire operazioni matematiche sui dati. Ad esempio, supponiamo che i dati non elaborati abbiano una colonna contenente i prezzi in dollari e centesimi. Se si necessitano solo valori in dollari, è possibile utilizzare questo modulo per effettuare la trasformazione [133].

È anche possibile utilizzare altri moduli di pre-elaborazione dei dati scritti in R o Python, non limitando quindi l'utente a scelte legate ai soli moduli forniti [137]. In una tabella di dati preparata, ogni colonna è chiamata *features*, in quanto viene considerata una caratteristica del modello, e spesso una di queste contiene il valore che stiamo cercando di prevedere. Ad esempio i dati preparati che saranno utilizzati per determinare se una transazione effettuata con carta di credito è fraudolenta o meno, saranno caratterizzati da informazioni sulle transazioni, con l'aggiunta di una colonna contenente valori per riconoscere se la transazione sia o meno fraudolenta. Questo valore è proprio quello che si cerca di prevedere, e viene quindi chiamato *valore target*.

Il ruolo di R

Risulta ormai chiaro come il ruolo della statistica sia di primo piano nel'identificazione del valore target. Il linguaggio open-source chiamato R, creato

in Nuova Zelanda più di venti anni fa, è diventato il linguaggio di riferimento per scrivere codice in questo ambito. Quindi Microsoft® ha incluso un ampio supporto a R in Azure Machine Learning, che può essere usato al suo interno per implementare nuovi algoritmi di machine learning, nuovi moduli di pre-elaborazione dei dati ed altro ancora [151].

Esecuzione degli esperimenti

Una volta che i dati sono pronti, si può procedere con l'esecuzione dell'esperimento. La figura 27 illustra il processo:

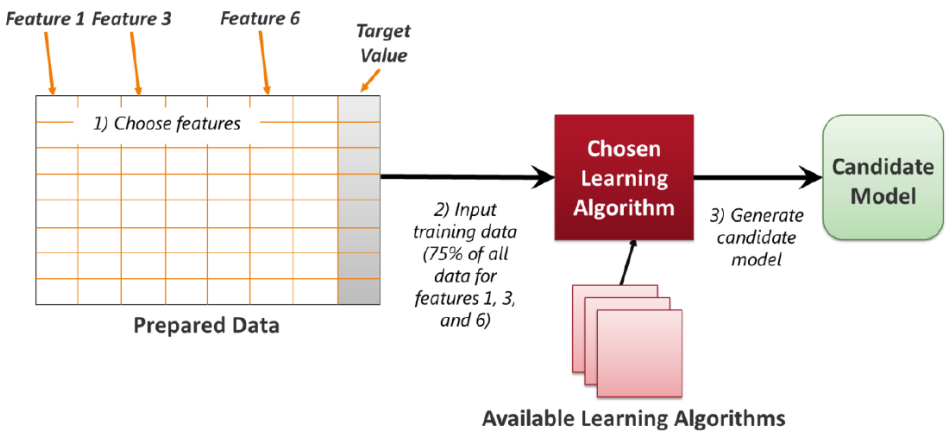


Figura 27: Preparazione dei dati

Come mostra la figura 27, è possibile scegliere quali features (ovvero quali colonne) devono essere usate nella tabella dei dati preparati (in figura 27 colonne 1, 3 e 6). Queste features sono quindi inserite in un algoritmo di machine learning scelto per l'esperimento (fase 2), creando quindi un modello candidato (passaggio 3). I dati usati in input per creare un modello candidato sono chiamati *training data*, rappresentano il 75% dei dati pre-eleaborati, e vengono utilizzati per l'addestramento del modello attraverso l'algoritmo scelto di machine learning. Il

restante 25% dei dati è trattenuto, perché viene utilizzato per testare e valutare il modello in una fase successiva a quella dell'addestramento.

Algoritmi di machine learning

Azure Machine Learning offre sia un ampio set di algoritmi che la possibilità di crearne uno proprio. Alcuni algoritmi di machine learning sono particolarmente utili per i problemi di classificazione, dove l'obiettivo è quello di creare un modello in grado di prendere un set di dati di input e determinare con precisione in quale delle due o più categorie definite i dati di input rientrano. Un buon esempio di questo è proprio lo scenario di frode con carta di credito che si sta trattando in questa tesi, in cui l'obiettivo è quello di acquisire dati su una transazione effettuata con carta di credito, per poi trovare un modello che classifica accuratamente la transazione in una delle due categorie: valida o fraudolenta. Azure Machine Learning offre diversi algoritmi per problemi di classificazione, come Multiclass Decision Jungle , two-class Boosted Decision Tree e One-vs-All Multiclass. È possibile utilizzare uno di questi algoritmi semplicemente selezionandolo dal menù fornito da Azure Machine Learning [137].

Un altro gruppo di algoritmi di machine learning è utile per problemi di previsione, dove è possibile usare la regressione per prevedere ad esempio la domanda futura di un prodotto in base alla domanda precedente e ad altri fattori. Azure Machine Learning supporta diversi algoritmi per fare questo, incluso Bayesian Linear Regression, Boosted Decision tree Regression e Neural Network Regression, che, come per gli algoritmi di classificazione, è possibile selezionare dal menù presente.

Un altro gruppo di algoritmi di machine learning è quello utilizzato per problemi di clustering. In questa casistica l'obiettivo è trovare raggruppamenti significativi a partire da grandi quantità di dati di input, per poi creare un modello in grado di

capire a quale cluster devono essere assegnati gli elementi presenti nei dataset [151].

Apprendimento Supervisionato E Non Supervisionato

Gli algoritmi di apprendimento automatico possono essere raggruppati in due tipi: supervisionato e non supervisionato. Nel primo caso, il valore target che si sta cercando di prevedere è conosciuto, e vengono utilizzati gli algoritmi di classificazione e regressione per l'apprendimento. Il caso trattato in questa tesi, ovvero il rilevamento di frodi con carte di credito, oltre ad essere un caso di apprendimento supervisionato, è anche un caso di apprendimento controllato, perché il valore che si sta cercando (indipendentemente dal fatto che la transazione sia fraudolenta) è contenuto nei dati storici con cui si lavora.

Nell' apprendimento non supervisionato invece, non sono conosciuti i valori target che si sta cercando. Un esempio di apprendimento senza supervisione è uno scenario in cui si cerca ad esempio di raggruppare i clienti in gruppi in base alla loro fidelizzazione, in cui vengono usati algoritmi di clustering per l'apprendimento e spetta a colui che ha creato il modello decidere se i risultati sono o meno consistenti. Questo tipo di problemi sono generalmente più difficili rispetto a quelli di apprendimento supervisionato[137].

Test del modello

Una volta determinato il modello per l'esperimento, risulta necessario poter effettuare una valutazione di esso. Nasce quindi il problema dei dati da utilizzare per il test. Come detto in precedenza, i dati per il test provengono dai dati preparati, dal momento che in fase di creazione del modello viene trattenuto il 25% dei dati, che viene usato in questa fase per verificarne il rendimento. La figura 28 illustra questo processo:

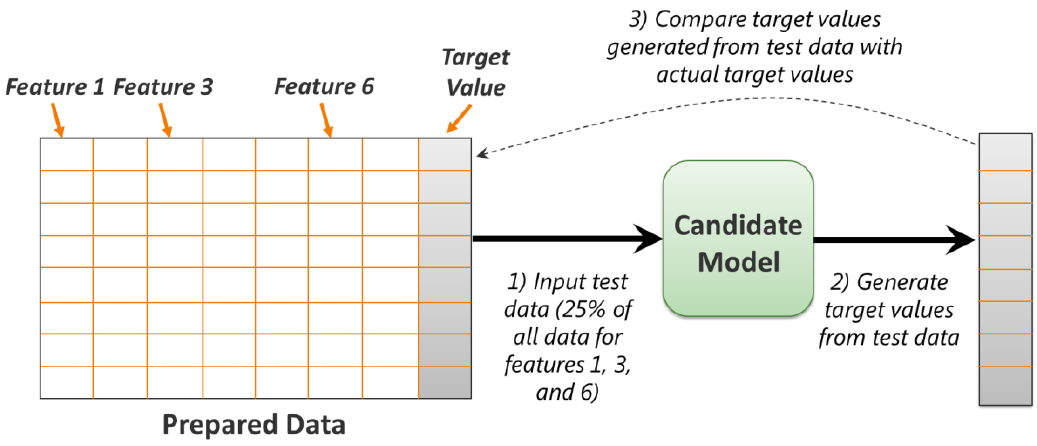


Figura 28: Test del modello

Il processo inizia inserendo i dati di test nel modello addestrato, per generare i valori target (passaggio 2, figura 28). Si possono quindi confrontare i valori target generati con il set di dati dedicato al testing con quelli generati in precedenza. Qualora corrispondano in maniera soddisfacente, si avrà un modello che soddisfa lo scopo mentre, in caso contrario, si dovrà fare un passo indietro e scegliere una nuova combinazione di features ed algoritmi di apprendimento automatico.

Distribuzione e utilizzo di un modello

Una volta che il modello è stato validato, è pronto per essere rilasciato in modo che sia accessibile da applicazioni esterne. Il rilascio può essere un problema di non poco conto, perché i modelli vengono spesso creati in R, senza una API per accedere agli algoritmi utilizzati. Senza contare che un'azienda in un mercato in rapida evoluzione potrebbe aver bisogno di rilasciare aggiornamenti del modello con una frequenza alta, comportando così dei rallentamenti.

Azure Machine Learning supporta la distribuzione dei modelli tramite un servizio API, come mostrato in figura 29:

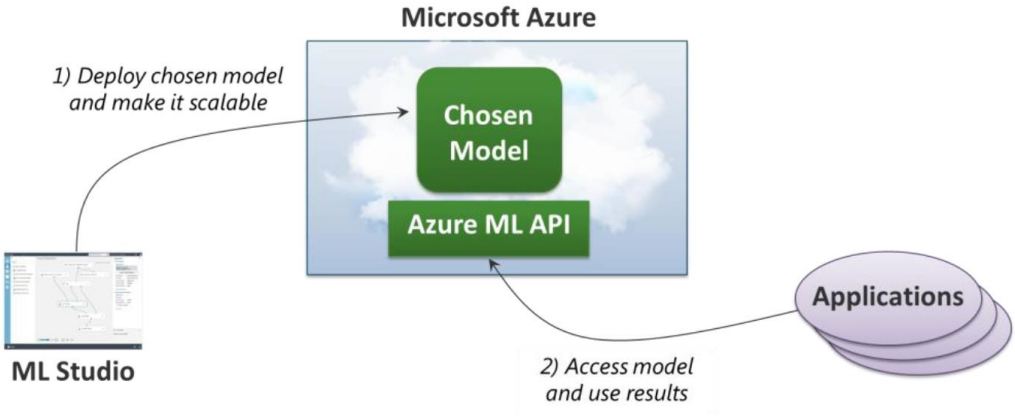


Figura 29: Preparazione dei dati

Quando un modello è pronto, è possibile usare Azure ML per distribuirlo direttamente in Microsoft Azure (passaggio 1). Il modello espone la sua funzionalità tramite l'interfaccia RESTful dell'API di Azure ML, che consente l'accesso alle applicazioni (passaggio 2).

3.5 Implementazione del modello

In questa sezione verranno descritte le fasi della realizzazione del modello di fraud detection proposto per la rilevazione delle frodi. Come visto in precedenza, il rilevamento delle frodi può essere considerato come un problema di classificazione binario, dove la popolazione è sbilanciata, in quanto i casi di frode sono generalmente più rari rispetto al volume complessivo delle transazioni. Tendenzialmente quando una frode viene scoperta, l'azienda adotta misure per bloccare le transazioni ed i relativi account per prevenire ulteriori perdite.

Pertanto, le prestazioni del modello verranno misurate utilizzando metriche a livello di account e di transazione.

Il modello proposto utilizza le transazioni di acquisto eseguite online come input al processo di modellizzazione del rilevamento delle frodi, che è suddiviso in cinque macrostep, come mostrato nella seguente figura:

Figura 30: fasi del modello

- Data aggregation: in questa fase, i dati ricevuti in ingresso da fonti di vario tipo vengono aggregati in un unico set;
- Data processing: i dati aggregati vengono processati per renderli pronti per l'analisi;
- Feature engineering: in questa fase del processo vengono inserite delle colonne nel dataset al fine di arricchirlo con informazioni utili all'analisi;
- Model and training evaluation: in questa fase avviene l'addestramento e la valutazione delle performance del modello;
- Model deployment: il modello viene rilasciato e reso pronto alla connessione con applicazioni.

3.6 Aggregazione dei dati

In questa macrofase le sorgenti di dati in input vengono aggregate attraverso l'implementazione dei seguenti moduli in Azure Machine Learning:

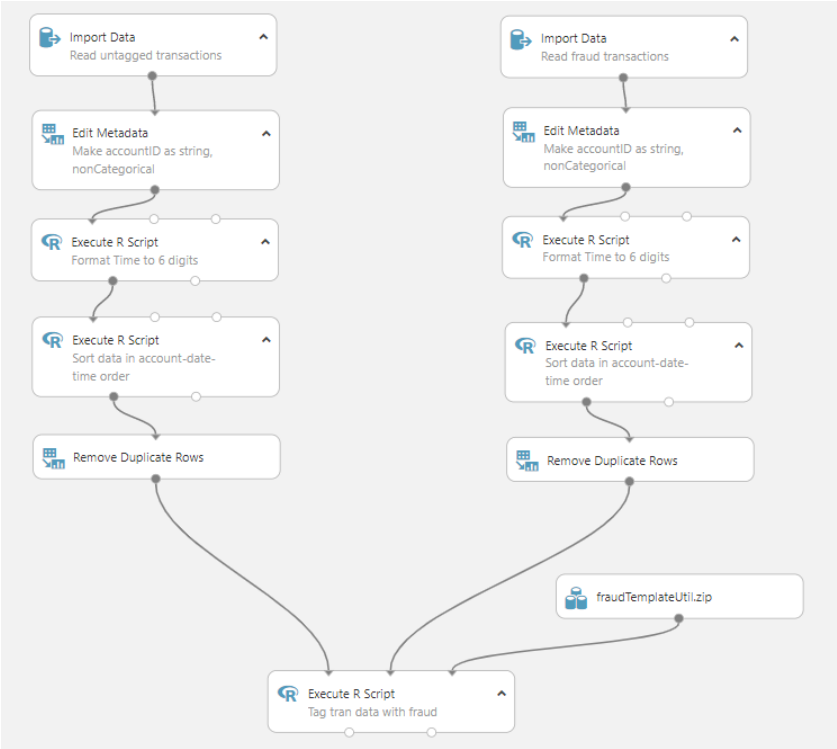


Figura 31:blocchi utilizzati nella fase di data aggregation

Come mostrato in figura, sono presenti due flow paralleli, in quanto il modello riceve in ingresso due database di dati transazionali reali in formato .csv, uno rappresentante un insieme di transazioni di cui non si conosce la natura, che vengono definiti quindi "untagged", ed un altro contenente esclusivamente transazioni di natura fraudolenta, "tagged".

I due database presentano dei campi di dati tipici dei dati transazionali, che possono essere ricondotti a tre macrogruppi di dati:

- Transactional Data: contegono campi di dati relativi alla transazione corrente;
- Account Data: contegono campi di dati relativi all'account dell'utente che effettua la transazione;

- Aggregated Data: contegono dati aggregati in funzione dello storico dell'attività dell'account. Possono essere pre-calcolati o calcolati nella fase di feature engineering.

La tabella seguente mostra un sottoinsieme dello schema di dati presenti nelle colonne del set di dati non taggati. Si noti che il formato data e ora specificato in questo schema deve essere rigorosamente seguito per poter utilizzare il modello nelle fasi successive.

Index	Data fields	Type	Descriptions	Required
	Transaction Data			
1	transactionID	String	Unique transaction Id	x
2	accountID	String	Unique account Id	x
3	transactionAmountUSD	Double	Transaction amount in USD e.g., 12345.00	x
4	transactionAmount	Double	Transaction amount in currency expressed in transactionCurrencyCode e.g., 12345.00	x
5	transactionCurrencyCode	String	Currency code of the transaction. 3 alphabet letters, e.g., USD	x
6	transactionCurrencyConversionRate	Double	Conversion rate to US Dollars e.g. 1.0000 for USD to USD	x
7	transactionDate	String	Date when transaction occured Typically in the time zone of the processor. Format: yyyymmdd, e.g., 20000101	x
8	transactionTime	String	Time when transaction occurred. Typically in the time zone of processing end. Format: hhmmss, eg. 153059	x
9	localHour	Double	The hour in local time. Value of 0-23	x
10	transactionScenario	String	A -- Authorization O -- Others	x

Figura 32: campi dei dati transazionali

Import data

Il blocco import data genera il tipo di dati per ciascuna colonna in base ai valori in essa contenuti, e carica i dati nello spazio di lavoro di Azure Machine Learning. Il modulo Importa dati supporta le seguenti origini dati [129]:

Data source	**note**
Web URL via HTTP	Ottieni dati ospitati su un URL web che utilizza HTTP e che è stato fornito nei formati CSV, TSV, ARFF o SvmLight
Hive Query	Ottieni dati dallo storage distribuito in Hadoop. È possibile specificare i dati desiderati utilizzando il linguaggio HiveQL
Azure SQL Database	Ottieni dati dal database SQL di Azure o dal data warehouse di Azure SQL
Azure Table	Ottieni dati archiviati nel servizio tabelle di Azure
Import from Azure Blob Storage	Ottieni i dati archiviati nel servizio BLOB di Azure
Data Feed Providers	Ottieni dati esposti come feed in formato OData
Import from On-Premises SQL Server Database	Ottieni dati da un database SQL Server locale utilizzando Microsoft Data Management Gateway
Azure Cosmos DB	Ottieni i dati archiviati in formato JSON in Azure Cosmos DB.

Nello spazio di lavoro fornito da Azure Machine Learning, il modulo viene rappresentato graficamente nel seguento modo:

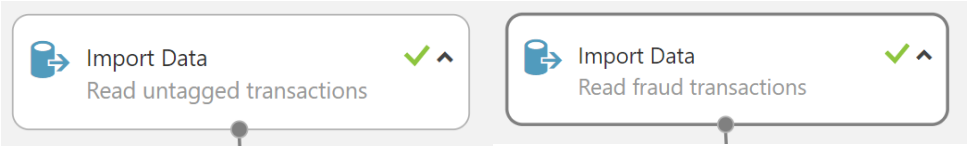


Figura 33: modulo di import data

In questo modello, come mostrato in figura 33, sono stati inseriti due moduli di import data per leggere in ingresso i due file .csv relativi alle transazioni.

Metadata Editor

Il modulo viene utilizzato per assicurarsi che il campo *accountId* non sia numerico. Azure Machine Learning tratta sempre i campi di dati con all'interno numeri come tipi di dati numerici, che non sempre è il comportamento desiderato. In questo modello, è stato modificato il numero di conto in una stringa per consentire il corretto confronto dei numeri di conto nella fase di ordinamento.

Di seguito la rappresentazione grafica nello spazio di lavoro di Azure Machine Learning[130]:

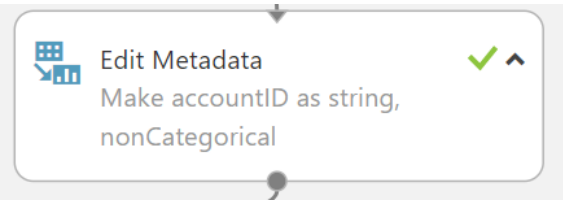


Figura 34: modulo edit metadata

Executive R Script

Il campo *transactionTime* segue il formato "HHMMSS", ma a volte nei dati di input vengono tralasciati gli zeri iniziali. Pertanto, si utilizza uno script R per formattare i dati temporali secondo il formato "HHMMSS", necessario per il successivo ordinamento. Di seguito il codice dello script in R di riferimento per questo blocco [131]:

```
data.set = dataset1
data.set$transactionTime = sprintf("%06d", as.numeric(dataset1$transactionTime))
```

Executive R Script

Attraverso questo step, entrambi i dataset in input al modello vengono ordinati per data ed ora nella quale l'account relativo alla transazione ha effettuato il pagamento. La disponibilità di dati ordinati a livello di account semplifica la codifica delle frodi, l'aggregazione delle features e la misurazione delle prestazioni del modello, che avverranno negli step successivi. Di seguito il codice dello script R di riferimento per questo blocco:

```
data.set = dataset1[with(dataset1, order(accountID,transactionDate,transactionTime)),]
```

Remove duplicates

In questo step viene utilizzato il modulo *remove duplicates* fornito da Azure ML[132], per rimuovere i record duplicati in entrambi i file nei seguenti campi:

```
accountID,transactionID,transactionAmount,transactionDate,transactionTime
```

Executive R Script

In questo passaggio i dati vengono aggregati in un unico dataset, per poi essere taggati in una colonna definita *label*, che definisce se la transazione deriva dal set di dati fraudolento o meno, come mostrato dalla seguente figura:

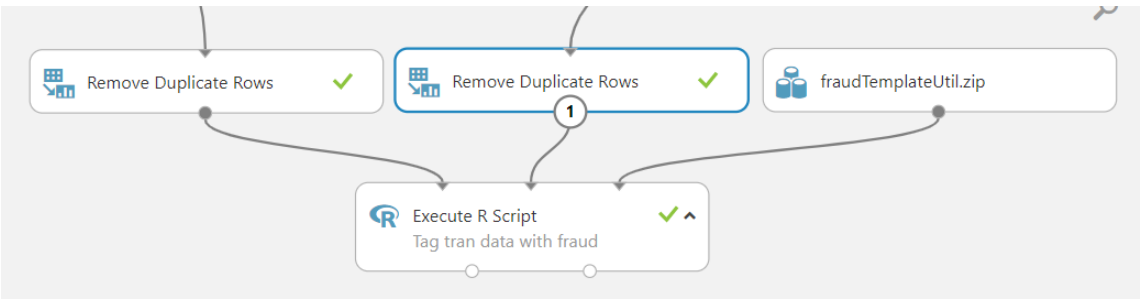


Figura 35: modulo execute R script

Per fare questo, oltre ai due dataset il modulo riceve in ingresso un modulo appositamente progettato, che contiene una libreria di funzioni in codice R. Una di queste, chiamata *tagTranDataWithFraud ()*,viene eseguita per generare la nuova colonna *label*, contenente i valori dei tag assegnati alle transazioni. Nella tabella seguente sono elencati i parametri che è possibile utilizzare quando si chiama questa funzione:

Parameters	Description	Type
df	Name of transaction dataset	data frame
frd_df	Name of fraud transaction data	data frame
mode	"Acct" for account-level tagging, or "Tran" for transaction-level tagging	string

A livello di transazione, vengono utilizzati i seguenti tag:

- 0: Frode (transazioni fraudolente)
- 1: NonFrode (transazioni non fraudolente)

A livello di account, vengono utilizzati i seguenti tag:

- 0: NonFrode (transazioni da un conto non fraudolento)
- 1: Frode (transazioni all'interno della finestra delle frodi)
- 2: Pre-frode e post-frode (transazioni al di fuori della finestra delle frodi)

Le transazioni pre-frode rappresentano quelle derivanti da un conto prima che questo generi una transazione fraudolenta, mentre le transazioni post-frode sono quelle transazioni derivanti da un conto che ha generato una transazione fraudolenta. In uno scenario aziendale, i conti fraudolenti vengono generalmente bloccati quando viene rilevata una transazione fraudolenta. Pertanto, le pre-frodi e le post frodi sono generalmente escluse dalla valutazione.

Per eseguire questo primo step ed in generale tutti quelli che verranno descritti, è necessario cliccare sul tasto "run", mostrato in figura 36. Il set di dati così processato viene salvato in modo da poterlo utilizzare nello step successivo.

Figura 36: tasto run

3.7 Strutturazione dei dati

In questo step i dati ricevuti in input dalla fase di data aggregation vengono processati e trasformati per correggere eventuali mancanze e renderli conformi e pronti per le analisi successive. Nella figura sottostante vengono mostrati gli step implementati in questa fase:

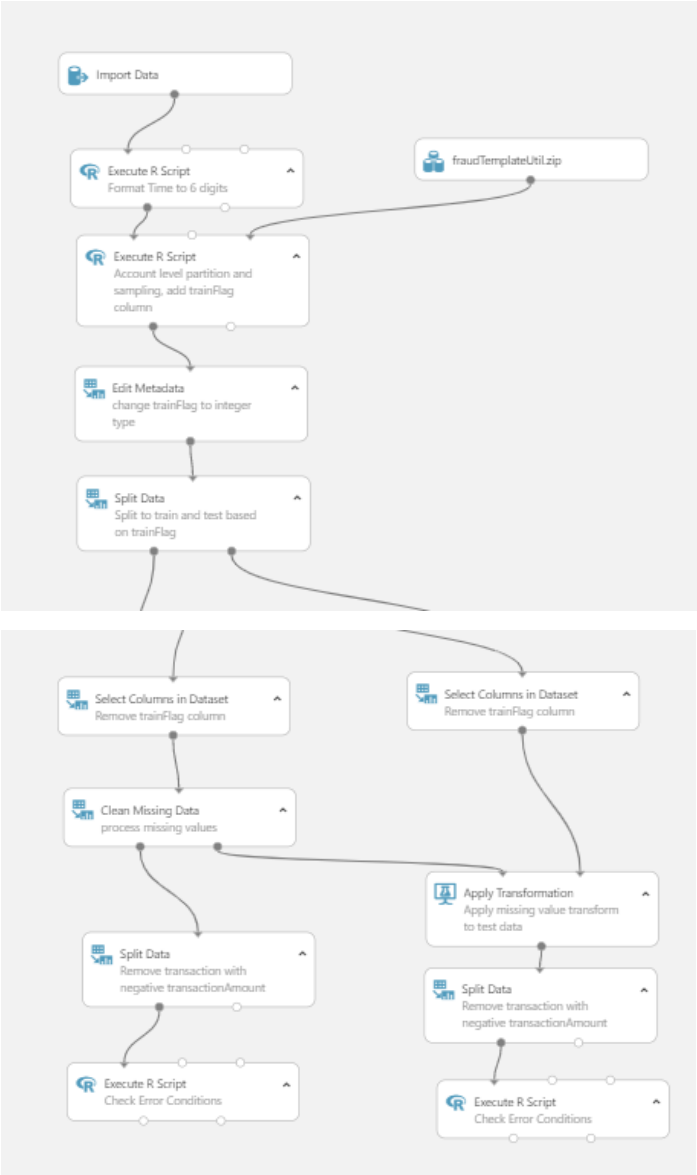


Figura 37: blocchi della fase di processing

Import data

Con questo modulo viene importato l'output della fase precedente.

Executive R Script

In questo passaggio i dati vengono campionati in maniera randomica rispetto al campo *accountID* per poter ottenere due set di dati, uno destinato all'addestramento del modello e l'altro al test, riconoscibili grazie all'aggiunta nel dataset di una colonna, denominata "trainflag", che indica l'appartenenza della singola transazione ad uno dei due set di dati. Tutto questo viene effettuato utilizzando la funzione:

```
data.set = splitDataByKey(dataset1, key, nfRate, frdRate)
```

disponibile nella libreria di funzioni in codice R appositamente creata per il modello, come mostrato dalla seguente figura:

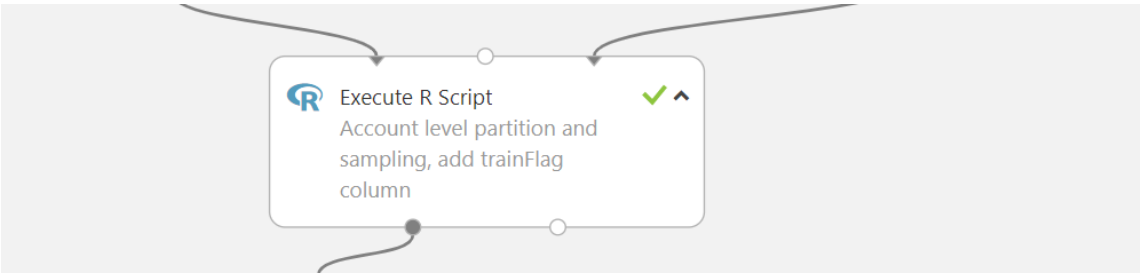


Figura 37: modulo execute R script

I seguenti campi vengono utilizzati dalla funzione splitDataByKey:

- Key: campo rispetto a cui viene effettuato il campionamento (accountID);
- nfRate: tasso di campionamento per gli account non fraudolenti, pari a 0,7;
- frdRate: tasso di campionamento per gli account fraudolenti, pari a 0,7;

La colonna trainflag che viene aggiunta può assumere i seguenti valori:

- trainflag=true per il set di dati destinato all'addestramento del modello;
- trainflag=false per il set di dati destinato al test del modello;

Per il rilevamento delle frodi e la valutazione delle performance del modello rispetto al campo account, è necessario che le transazioni per ogni singolo account vengano inserite nel set di training o nel set di test, ma non in entrambi.

Metadata Editor

Questo blocco(figura 38) cambia il tipo di dato nella colonna "Trainflag" aggiunta nel passaggio precedente in integer. Quindi in uscita avremo la colonna trainflag con i seguenti valori:

- trainflag=1 per il set di dati destinato all'addestramento del modello;
- trainflag=0 per il set di dati destinato al test del modello;

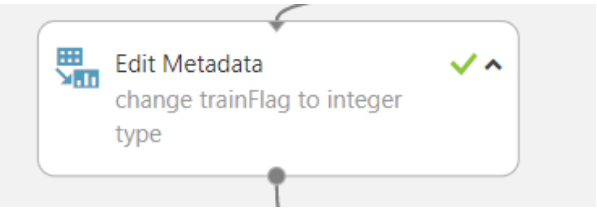


Figura 38: modulo edit metadata

Split Data

L'inserimento di questo modulo [134] (figura 39) ha lo scopo di separare i dati nei due dataset di utilità:

- *traindata*: set di dati che verrà utilizzato per "addestrare" il modello;
- *testdata*: set di dati che verrà utilizzato per "testare" il modello.

Quindi in uscita avremo i due dataset separati, dando vita così ad un flusso di lavoro in parallelo [134].

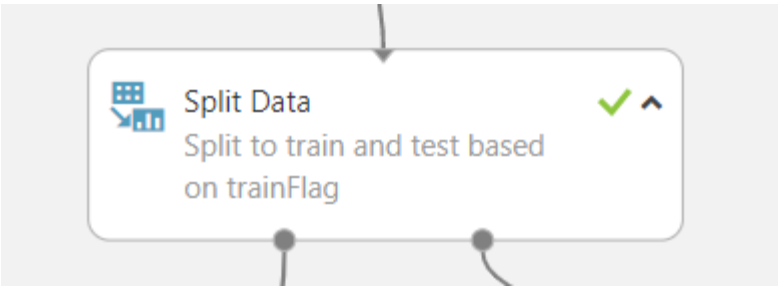


Figura 39: modulo split data

Select columns in dataset

Ora che i due dataset sono separati [133], viene rimossa la colonna trainflag precedentemente aggiunta, ora non più funzionale.

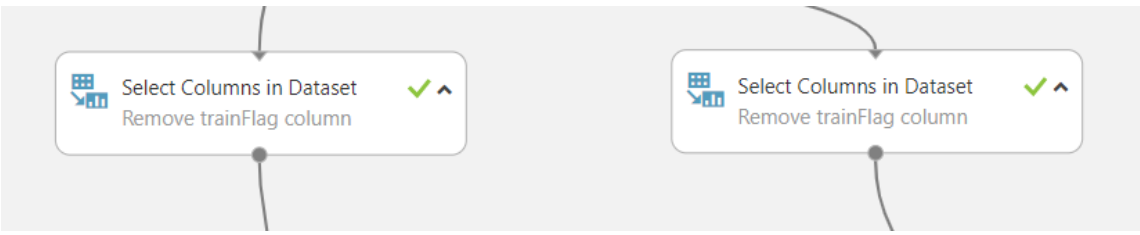


Figura 40: moduli select columns dataset

Clean missing data – Apply Transformation

Con il blocco Clean Missing Data vengono gestiti i valori mancanti in tutti i campi ad esclusione di quello *label*, inserendo il valore "0" dove non sono presenti. Come mostrato dalla figura seguente, la stessa trasformazione viene applicata anche al dataset di test con il blocco Apply transformation:

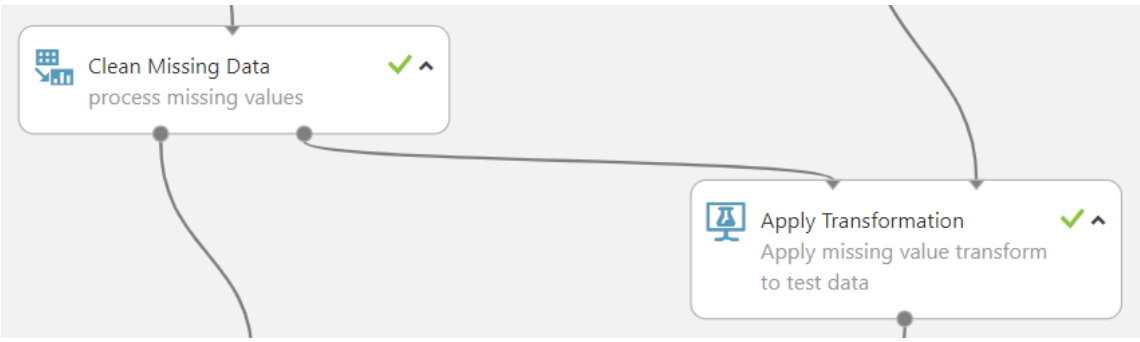


Figura 40: moduli clean missing data e apply transformation

Split Data

Con questo blocco, applicato ad entrambi i dataset [136], vengono eliminate le transazioni con valori negativi.

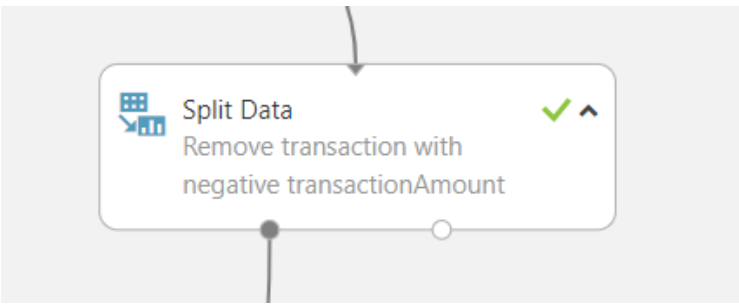


Figura 41: modulo split data

Execute R script

Come ultimo step della macrofase di Data Processing viene effettuato un controllo sulla qualità dei dati per verificare che tutto sia corretto attraverso l'uso di uno script R. In particolare, vengono generate delle *error flag* nel caso in cui vengano trovate delle transazioni con data non valida.

3.8 Implementazione logiche di arricchimento

In questa macrofase vengono aggiunte delle colonne ai due dataset processati precedentemente, che contengono informazioni utili all'analisi per il riconoscimento delle transazioni fraudolente, chiamate *features*.

Le features che vengono create sono elaborate in maniera distinta, generando quattro processi separati che hanno lo stesso input, ovvero i due dataset:

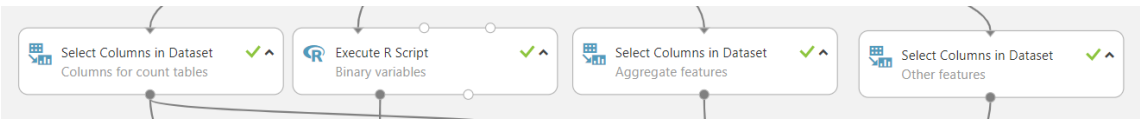


Figura 42: modulo per l'implementazione delle features engineering

Le quattro categorie di features sono:

- Count Based features;
- Binary features;

- Aggregated account-level features;
- Selected raw features.

Count Based Features

L'idea di base di questo passaggio è quella di selezionare i campi dati, contenuti nel set di dati destinato all'addestramento, che hanno una numerosità alta di valori unici, per ottenere così rapidamente un riepilogo di quali colonne contengono le informazioni più importanti. Questo rappresenta un modo efficace per creare un set compatto di features derivanti dal set di dati. Nel caso del modello proposto, ad esempio, un'informazione cruciale può essere la provienza della transazione, la cui codifica più comune è il codice postale. Nel dataset potrebbe essere presente un numero di codici postali molto alto da tenere in considerazione e, a quel punto, ci si dovrebbe chiedere se il modello elaborato ha la capacità di apprendere da una numerosità alta e se si dispone di un dataset di addestramento abbastanza numeroso da impedire un overfitting. Se si disponesse di dati validi, con molti campioni, tale granularità locale potrebbe essere utile, ma, se per assurdo si avesse a disposizione un solo un campione di una transazione fraudolenta, proveniente da una piccola località identificata tramite il codice postale, significherebbe che tutte le transazioni provenienti da quel luogo sono fraudolente. Quindi risulta plausibile introdurre features osservando i conteggi e le proporzioni delle frodi per ciascun codice postale, ottenendo informazioni in base alle evidenze derivanti per ciascun valore. L'apprendimento basato sul conteggio permette di avere nel modello meno funzioni, che richiedono quindi meno parametri, consentendo un apprendimento ed una previsione più rapida, nonché una minore probabilità di overfitting. Gli step eseguiti per la count based featurization nel modello sono i seguenti:

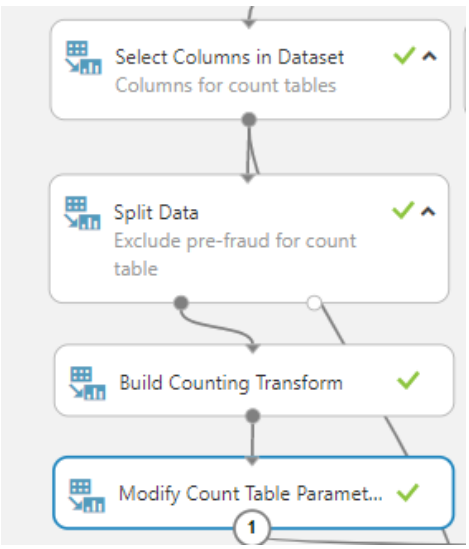


Figura 43: moduli per l'implementazione della count based featurization

Select columns in dataset

A partire dal dataset di addestramento, con questo modulo vengono selezionati i seguenti campi [133]:

transactionCurrencyCode,localHour,ipState,ipPostalCode,ipCountry,browserLanguage,shippingPostalCode,shippingState,shippingCountry,accountPostalCode,accountState,accountCountry,paymentBillingPostalCode,paymentBillingState,paymentBillingCountryCode,Label

Split Data

Con questo modulo vengono escluse le prefrodi e le postfrodi, eliminando il valore "2" nella colonna Label.

Build Counting Transformation

Questo modulo genera, a partire dalle colonne selezionate nel modulo precedente, una count table contenente la distribuzione congiunta di tutte le colonne relative alle features. Come detto in precedenza, queste statistiche sono

utili nel determinare quali colonne hanno il maggior valore di informazioni, per poi creare le features stesse. Essenzialmente svolge le seguenti azioni:

- Crea una count table che riepiloga il numero di campioni non fraudolenti e fraudolenti per ciascun valore univoco;
- Genera features basate sulla numerosità dei valori;
- Emette una trasformazione che può essere applicata a un nuovo set di dati.

Modify Count Table Parameter

Questo modulo permette di creare un nuovo set di statistiche basate sul count table senza dover analizzare nuovamente il set di dati.

Apply Transformation

Il modulo viene utilizzato per sostituire i valori originali nei dataset di addestramento e test, con i dati derivati dal count based features.

Binary features

Come precedentemente visto, Azure Machine Learning può creare un numero di flag binari che rappresentano possibili stati in nuove colonne. Inoltre, è possibile creare anche variabili binarie confrontando le coppie di valori: ad esempio, potremmo confrontare l'indirizzo di spedizione con l'indirizzo dell'utente e generare un flag che indica se gli indirizzi corrispondono. Con questo modulo vengono identificati:

- gli amount superiori a 150 dollari;
- mancata corrispondenza tra le varie combinazioni di indirizzi.

Di seguito il codice R usato per generare queste features:

```
#generate binary variables
```

```
is_highAmount = df$transactionAmountUSD > 150
bVars.df = as.data.frame(is_highAmount)

#addresss mismatch flags
bVars.df$acct_billing_address_mismatchFlag = as.character(df$paymentBillingAddress) ==
as.character(df$accountAddress)
bVars.df$acct_billing_postalCode_mismatchFlag = as.character(df$paymentBillingPostalCode) ==
as.character(df$accountPostalCode)
bVars.df$acct_billing_country_mismatchFlag = as.character(df$paymentBillingCountryCode) ==
as.character(df$accountCountry)
bVars.df$acct_billing_name_mismatchFlag = as.character(df$paymentBillingName) ==
as.character(df$accountOwnerName)

bVars.df$acct_shipping_address_mismatchFlag = as.character(df$shippingAddress) ==
as.character(df$accountAddress)
bVars.df$acct_shipping_postalCode_mismatchFlag = as.character(df$shippingPostalCode) ==
as.character(df$accountPostalCode)
bVars.df$acct_shipping_country_mismatchFlag = as.character(df$shippingCountry) ==
as.character(df$accountCountry)

bVars.df$shipping_billing_address_mismatchFlag = as.character(df$shippingAddress) ==
as.character(df$paymentBillingAddress)
bVars.df$shipping_billing_postalCode_mismatchFlag = as.character(df$shippingPostalCode) ==
as.character(df$paymentBillingPostalCode)
bVars.df$shipping_billing_country_mismatchFlag = as.character(df$shippingCountry) ==
as.character(df$paymentBillingCountryCode)
```

Aggregated Account level features – Select Columns in Dataset

Queste funzionalità riepilogano l'attività storica degli account, come la quantità totale di acquisti eseguiti durante la settimana ed il mese. I campi inseriti sono:

sumPurchaseAmount1Day,sumPurchaseAmount30Day,sumPurchaseCount1Day,sumPurchaseCount30Day,numPaymentRejects1Day

Selected raw features – Select Columns in Dataset

Vengono escluse le colonne di dati non elaborati che saranno più utilizzate direttamente come input del modello, come:

transactionAmountUSD,transactionAmount,transactionType,transactionMethod,transactionDeviceType,isProxyIP,browserType,paymentInstrumentType,cardType,cardNumberInputMethod,cvvVerifyResult,responseCode,digitalItemCount,physicalItemCount,purchaseProductType,accountAge,isUserRegistered,paymentInstrumentAgeInAccount

Add Columns

Utilizzando il modulo Add Columns tutte le colonne di tutte e quattro le features implementate vengono aggregate:

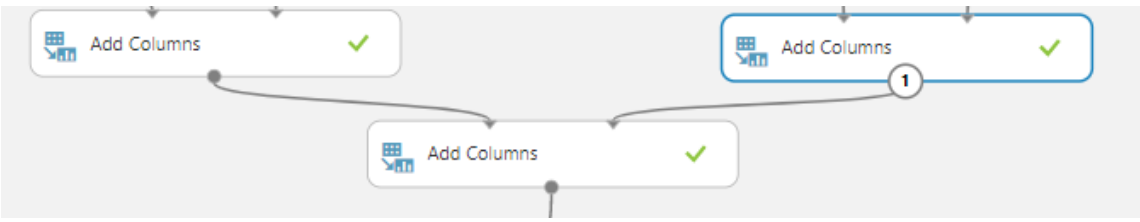


Figura 44:moduli add columns

Split Data

Utilizzando il modulo Split le transazioni pre-frode e post-frode sono escluse da entrambi i dataset.

Come per gli step precedenti, si esegue questa macrofase cliccando su run. L'output consiste in due dataset, il trainset ed il testset arricchiti con le feature descritte, che verranno utilizzati nella fase successiva per addestrare e testare il modello.

3.9 Addestramento del modello

Partendo dai due dataset costruiti nello step precedente, in questa macrofase il modello verrà prima addestrato con il trainset e poi valutato con il testset. Gli step per far ciò sono mostrati nella seguente figura:

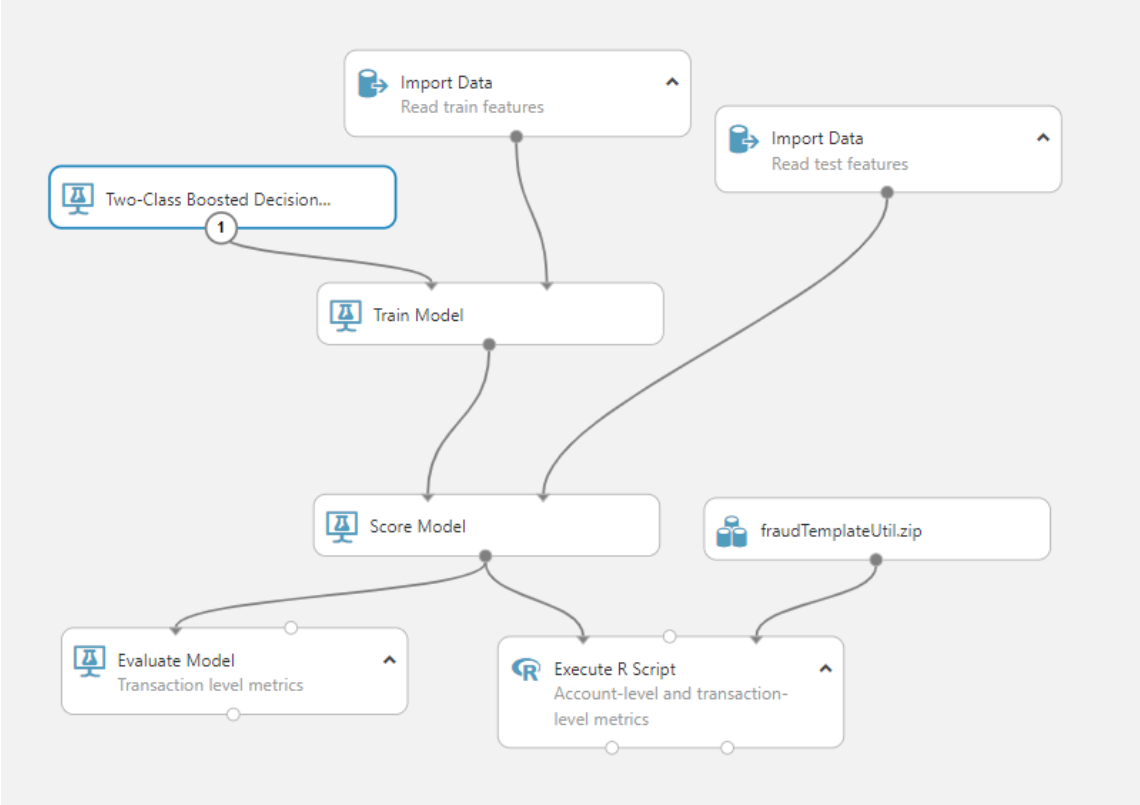


Figura 45: moduli per l'implementazione della fase di test e valutazione

Import Data

Il modulo di import data legge in ingresso il trainset.

Train Model

Questo modulo ha lo scopo di addestrare il modello. Per far ciò, in ingresso riceve il dataset di addestramento e il modulo *two class boosted decision*, che rappresenta l'algoritmo di machine learning scelto per il training.

Scelta dell'algoritmo di Machine Learning

La risposta alla domanda "Quale algoritmo di Machine Learning deve essere usato" è sempre "Dipende". Dipende dalla dimensione, dalla qualità e dalla natura dei dati, da cosa si vuole ottenere con la risposta ed infine dal tempo a disposizione. Machine Learning Studio fornisce algoritmi avanzati, ad esempio gli alberi delle decisioni con boosting scalabile, i sistemi bayesiani e le reti neurali. Sono inclusi anche pacchetti open source scalabili di apprendimento automatico. Il rilevamento delle frodi è un problema supervisionato di classificazione a due output, ovvero è necessario capire se una transazione sia o meno fraudolenta.

La scelta dell'algoritmo Two class Boosted Decision

A valle delle considerazioni di cui sopra, è stato quindi selezionato l'algoritmo Two class boosted decision. Questo perchè il modello di rilevazione delle frodi deve:

- predire tra due categorie, rispondendo ad una domanda con risposta di tipo binario, true o false;
- essere in grado di apprendere velocemente;
- essere accurato e preciso.

Un albero decisionale potenziato è un metodo di apprendimento d'insieme in cui il secondo albero corregge gli errori del primo albero, il terzo albero corregge gli errori del primo e del secondo albero e così via. Le previsioni si basano sull'insieme di tutti gli alberi previsionali [138].

Di seguito viene descritto il setting dei parametri scelto per il modulo two class boosted decision:

- Maximum number of leaves per tree: viene chiesto di indicare il numero massimo di nodi terminali (foglie) che possono essere creati in qualsiasi albero. Aumentando questo valore, si aumenta potenzialmente la dimensione dell'albero e si ottiene una migliore precisione, con il rischio di overfitting e tempi di addestramento più lunghi. È stato scelto il valore 20.
- Minimum number of samples per leaf node: viene indicato il numero di casi richiesti per creare un nodo terminale (foglia) in un albero. Aumentando questo valore, si aumenta la soglia per la creazione di nuove regole. Ad esempio, con il valore predefinito 1, anche un singolo caso può causare la creazione di una nuova regola. Se si aumenta il valore a 5, i dati di allenamento dovrebbero contenere almeno 5 casi che soddisfano le stesse condizioni. Viene scelto il valore 10.
- Learning rate: è un numero compreso tra 0 e 1 che definisce la dimensione del passo durante l'apprendimento. Il tasso di apprendimento determina la velocità o la lentezza con cui si converge alla soluzione ottimale. Se la dimensione del passo è troppo grande, si potrebbe andare oltre la soluzione ottimale, se troppo piccola, la sessione di addestramento impiega più tempo a convergere sulla soluzione migliore. Si è scelto il valore 0.2.
- Number of trees constructed: indica il numero totale di alberi decisionali da creare. Creando più alberi decisionali, si può potenzialmente ottenere una migliore copertura, ma i tempi di addestramento aumenteranno. Viene scelto il valore 100.

Score model

Una volta addestrato il modello con il dataset di training e l'ausilio dell'algoritmo two class decision boosted tree, viene effettuato lo scoring, utilizzando come input del modulo il dataset di test e l'output del modulo train model.

Evaluate model

In questo step viene effettuata la valutazione del modello, sia a livello di transazione che di account, attraverso l'inserimento di due moduli:

- Evaluate model;
- Execute R script.

3.10 Definizione metriche di valutazione

Da un punto di vista macroscopico la funzione di un Fraud Management System è quella di classificare gli eventi osservabili in modo da poterli associare, o meno, a casi di frode. Lo "score" che viene assegnato dall'FMS a ciascun caso è un punteggio che permette di stabilire un ordine basato sulla probabilità che si tratti di vere frodi (True Positive, TP) oppure di falsi allarmi (False Positive, FP). Ciò permette di alleggerire il lavoro degli analisti e di farli concentrare sui casi a maggior rischio. Nel seguito verranno stabiliti I KPI (Key Performance Indicator) utili a misurare le capacità di previsione del modello implementato, ovvero, la qualità della sua funzione di Scoring.

Alcuni KPI, come l'Accuracy, il Misclassification-Rate o l'Hit-Rate sono molto diffusi, ma non risultano essere indicati nel caso dei FMS a causa dello sbilanciamento tra le due classi, Frode e Non-Frode. Ad esempio un'accuratezza del 99,99% può in generale essere considerata accettabile, tuttavia se il rapporto tra le classi è di 1 a 10.000, con questa Accuracy si potrebbero classificare

erroneamente tutti i casi di vera frode. Analogamente, anche il Misclassification-Rate, che corrisponde al valore complementare dell'Accuracy (Misclassification Rate = 1- Accuracy), non è un KPI adatto al fraud management per la presenza del forte sbilanciamento tra le due classi. Ben più efficace è ad esempio la coppia Precision/Recall. Si può poi notare che la coppia Sensitivity (la percentuale di casi di frode identificati come tali) e Specificity (la percentuale di casi di non frode identificati come tali) mantiene la sua validità anche quando la proporzione tra i casi di frode e non-frode è fortemente sbilanciata. Grazie a tale proprietà, una curva ROC (Receiver Operating Characteristic) [152], ovvero la linea che traccia i valori della Sensitivity nei confronti del complemento ad uno della Specificity, in corrispondenza a diversi livelli di soglia, è insensibile allo sbilanciamento delle classi (skewness), e l'area sottesa a tale linea, nota come AUC (Area Under Curve), misura l'abilità che ha l'FMS di separare correttamente I casi di frode da quelli di non-frode e quindi la sua capacità predittiva. L'AUC è pertanto il miglior parametro che si possa calcolare per valutare le capacità predittive perché rappresenta allo stesso tempo sia l'efficacia di un FMS, tramite la percentuale di casi di vera frode (True Positive), sia la sua efficienza, indicando quanti falsi allarmi (False Positive) stiano influenzando negativamente il processo di contrasto alle frodi.

La totalità delle frodi, ovvero il 100% dei casi di frode osservati, corrisponde al numero Total Positive "p" dato dalla somma delle frodi individuate (True Positive) e delle frodi non trovate (False Negative) dal modello. La percentuale che rappresenta il True Positive Rate di un FMS, TF, si ottiene dividendo il numero di True Positive per il totale delle frodi p. ll False Negative Rate di un FMS, FN, si ottiene dividendo il numero dei False Negative per lo stesso p; si tratta di valori complementari perchè TP + FN = 100% = 1.

Similarmente, la totalità dei casi dovuti a falsi allarmi corrisponde al numero Total Negative "n" di casi dato dalla somma di falsi allarmi (False Positives) e dalla restante parte (True Negatives). Le percentuali associate FP e TN sono complementari: FP + TN = 100% =1.

I KPI rappresentati dalle quattro percentuali TP, FN, FP e TN sono normalmente raggruppati nella matrice di classificazione, riportata in figura 46, dove le righe riportano la classificazione dei casi eseguiti dal FMS e le colonne indicano invece i valori reali in termini di Frode e Non-Frode. Tale matrice di classificazione viene spesso chiamata "Confusion Matrix", in quanto visualizza il grado di confusione residua all'interno della classificazione, e fornisce una misura della qualità delle prestazioni di un FMS.

Confusion Matrix		
	Frode	**Non-Frode**
Casi previsti come Frode	True Positive ***TP = True Positive/p***	False Positive ***FP = False Positive/n***
Casi previsti come Non-Frode	False Negative ***FN = False Negative /p***	True Negative ***TN = True Negative/n***
Casi Totali	Total Positive = p ***TP + FN = 1***	Total Negative = n ***FP + TN = 1***

Figura 46: confusion matrix

Precision e Recall

Precision e Recall sono dei KPI molto utilizzati nella misura e valutazione dei sistemi di ricerca delle informazioni. Il valore di Precision si ottiene come rapporto del numero di elementi "rilevanti" che sono stati effettivamente trovati e quello del totale di elementi predetto come rilevante:

Precision = "classificati correttamente" / "totale predetti come di interesse"

Il valore di Recall è invece il rapporto tra numero di elementi "rilevanti" che sono stati trovati rispetto il loro numero totale:

Recall = "classificati correttamente" / "totale di interesse esistente"

Nella realtà esiste un limite ai massimi valori di Precision e Recall dovuto alla quantità di informazione effetivamente fornita nella chiave di ricerca. In altre parole, non è possibile aumentare contemporaneamente sia la Precision sia la Recall senza aumentare il contenuto informativo per la ricerca. Il grafico riportato in Figura 47 visualizza tale limitazione indicando che per avvicinarsi verso il punto ideale, rappresentato in alto a destra, è necessario saltare su una curva Precision-Recall successiva caratterizzata da un maggior contenuto informativo [152]. Diversamente ogni tentativo di aumentare la Precision produce contemporaneamente una diminuzione di Recall, e viceversa, essendo vincolati a rimanere sulla stessa curva.

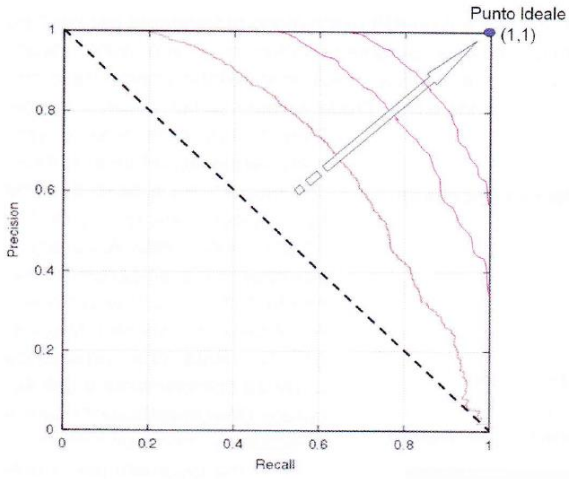


Figura 47: esempio di curva ROC

Nel contesto del fraud management, le definizioni di Precision e Recall diventano:

Precision = True Positive / (True Positive + False positive);

Recall = True Positive / p = True Positive rate;

Sensitivity, Specificity e la curva ROC

Lo stesso limite che si riscontra per la coppia di KPI Precision/Recall è riscontrabile anche con Sentitivity e Specifity. La Sensitività di un FMS è data dalla percentuale di Frodi correttamente classificate come tali, mentre la Specificità corrisponde alla percentuale di Non-Frodi a loro volta classificate correttamente. In pratica però è più utile usare il complemento ad uno della Specificità che si può indicare come "1-Specificity", che corrisponde alla percentuale di Non-Frodi classificate come Frodi. Il modo migliore per analizzare Sensitività e Specificità è osservare le curve ROC (Receiver Operating Characteristic) che si ottengono tracciando i punti, in corrispondenza di una serie di soglie (cut-point), le cui coordinate sono la percentuale dei True Positive e quella dei False positive. La linea diagonale indica valori di Sensitivà e 1-Specificità uguali tra loro, ovvero un andamento puramente casuale, che corrisponde ad una probabilita del 50% e 50% nella classificazione tra Frode e Non-Frode. In senso figurato, seguire la diagonale è come avere un classificatore il cui metodo di decisione consiste nel lanciare in aria una moneta.

In figura 48 sono rappresentate due curve ROC tracciate con diverse soglie per un test di scoring che ha l'obiettivo di valutare due modelli predittivi differenti, uno basato su una rete neurale e l'altro su un albero decisionale [152].

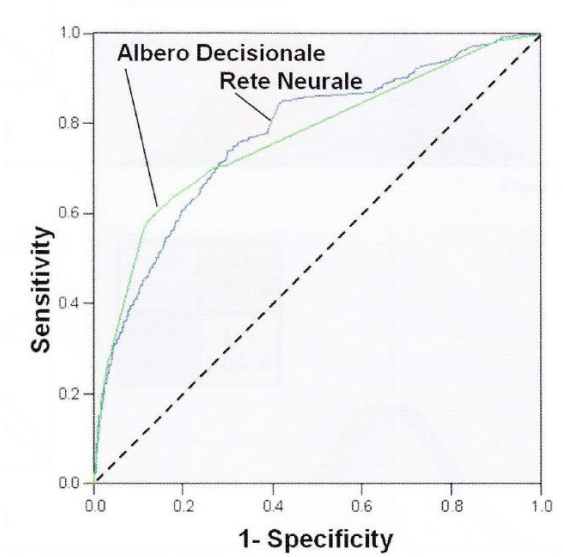


Figura 48: curva ROC basata su Sensitivity e Specificity

Entrambi i modelli dovevano riconoscere 1.387 casi di Frode memorizzati nello stesso archivio contente anche i 25.884 casi di Non-Frode di un operatore di telecomunicazioni italiano. Le coordinate delle curve ROC sono le percentuali di veri e falsi positivi:

Sensitivity = True Positive rate = TP

1 - Specificity = False Positive rate = FP

Le curve ROC hanno la proprietà di essere insensibili alla variazione sia del numero assoluto di casi sia dello sbilanciamento tra le due classi. Esse sono infatti una funzione dei valori percentuali TP e FP rispetto alla classe che è per essi omogenea, Frode per TP e Non-Frode per FP. Questa proprietà si può anche esprimere dicendo di coinvolgere, per ogni KPI, solo i parametri che si trovano all'interno di una stessa colonna della Confusion Matrix. Ogni altro KPI, che utilizza contemporaneamente valori presi da entrambe le colonne, sarà al contrario dipendente dai rapporti esistenti tra Frodi e Non-Frodi e di conseguenza dipendente dal loro sbilanciamento.

3.11 Valutazione delle capacità predittive del modello

Valutazione a livello di transazione

Per la valutazione a livello di transazione, si è utilizzato l'output del modulo evaluate model, che fornisce una curva ROC basata, come visto nel paragrafo precedente, sul rapporto tra il tasso di veri positivi e quello di falsi positivi. Con un valore soglia settato a 0,5 il modello implementato rileva i seguenti valori per i KPI definiti in precedenza:

True Positive	False Negative
26	346
False Positive	**True Negative**
81	58474

Con la corrispondente curva ROC:

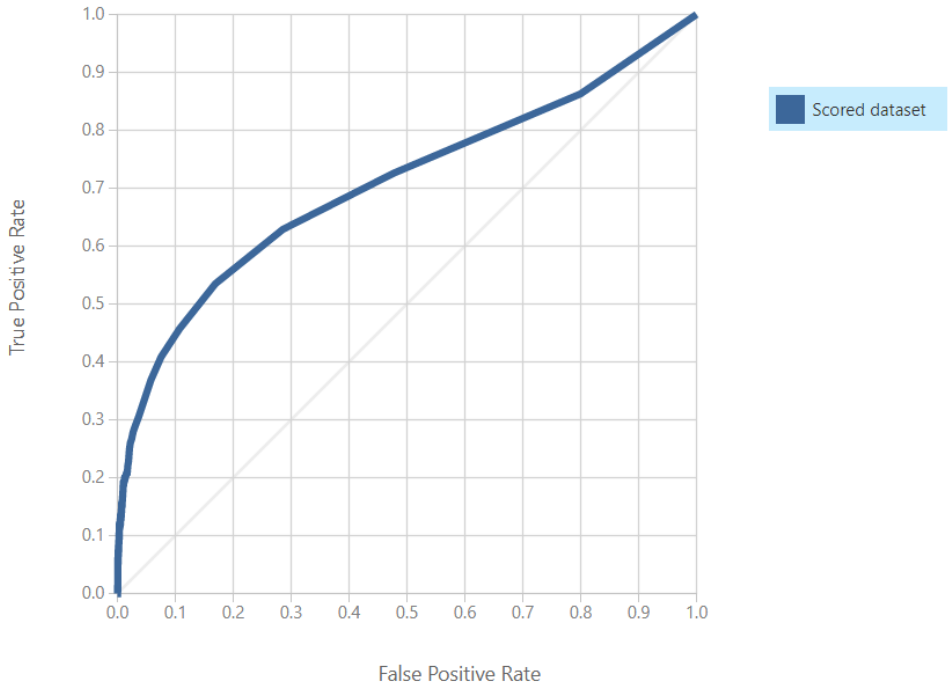


Figura 48: curva ROC basata su TPR e FPR

Il valore dell'AUC corrispondente è il seguente:

La curva Precision/Recall generata è la seguente:

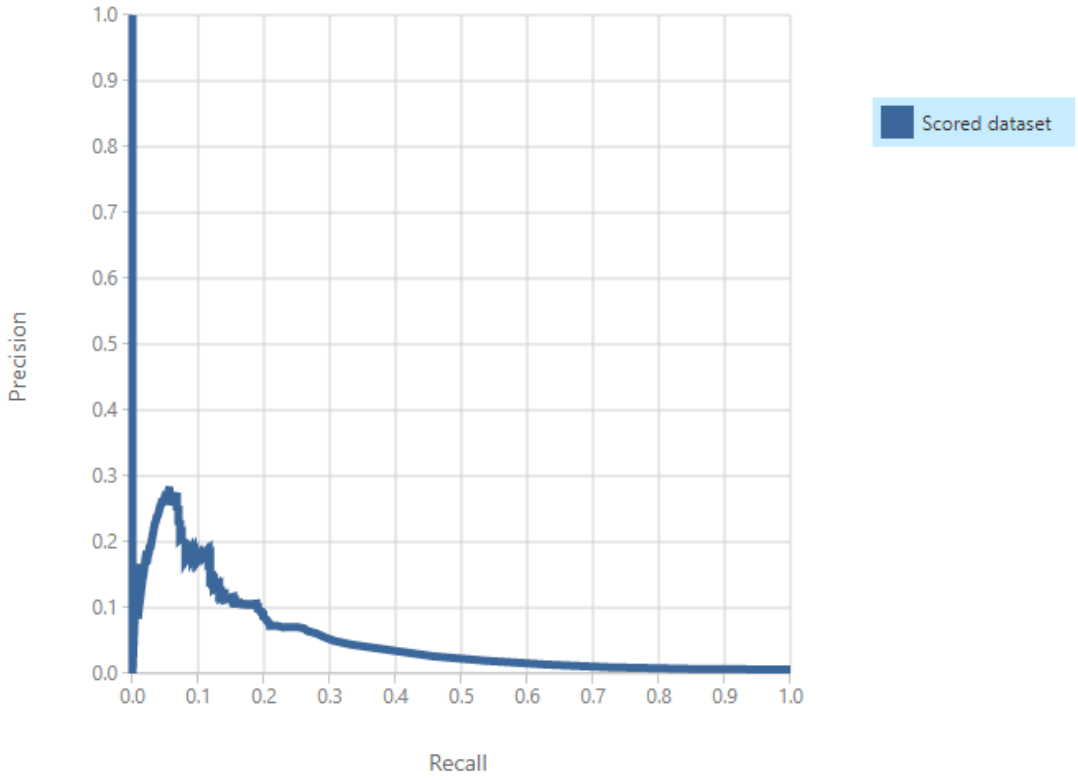


Figura 49: curva Precision Recall

A livello di transazione quindi, il modello implementato fornisce delle ottime performance.

Valutazione a livello di account

Come detto in precedenza, in base al presupposto che una volta che una transazione viene rilevata come fraudolenta verrà intrapresa un'azione per

bloccare tutte le transazioni successive, per il rilevamento delle frodi è utile analizzare le performance anche a livello di account.

Una grande differenza tra le metriche a livello di account e le metriche a livello di transazione è che, in genere un account confermato come falso positivo (ovvero, un'attività fraudolenta è stata prevista dove non esisteva) non verrà contattato di nuovo per un breve periodo di tempo, per evitare disagi al cliente.

Per valutare le prestazioni a livello di account saranno utilizzati i seguenti KPI:

- ADR – Fraud account Detection Rate. La percentuale di account fraudolenti rilevati in tutti gli account fraudolenti.
- VDR – Value Detection Rate. La percentuale di risparmio, presupponendo che la transazione fraudolenta abbia innescato un'azione di blocco sulle transazioni successive, rispetto a tutte le perdite dovute alle frodi.
- AFPR – Account False Positive Ratio. Il rapporto tra account falsi positivi rilevati e account fraudolenti rilevati.

La seguente funzione R genera le suddette statistiche a livello di account e ne aggiunge altre a livello di transazione:

```
scr2stat <-function(dataset, contactPeriod, sampleRateNF,sampleRateFrd)
```

Nella tabella seguente sono elencati i parametri per la funzione splitDataByKey ():

Parameters	Description	Type
input dataset	Scored dataset	data frame
contactPeriod	The wait time period (days) before re-contacting the customer	numeric
sampleRateNF	Sampling rate of nonfraud transactions	float (0,1]
sampleRateFrd	Sampling rate of fraud transactions	float (0,1]

Di seguito vengono mostrate le curve di performance raggiunte dal modello a livello di account, generate a partire dal set di dati utilizzato:

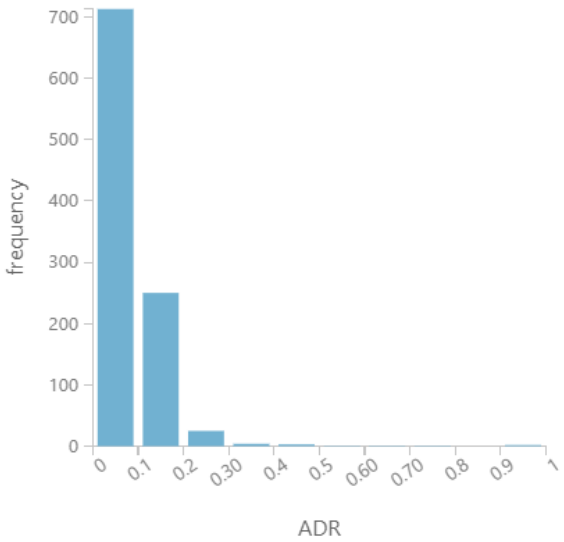


Figura 50: Andamento KPI ADR

Quando il valore del KPI ADR è basso, la frequenza di riconoscimento degli account fraudolenti è molto alta, che risulta essere proprio il valore cercato.

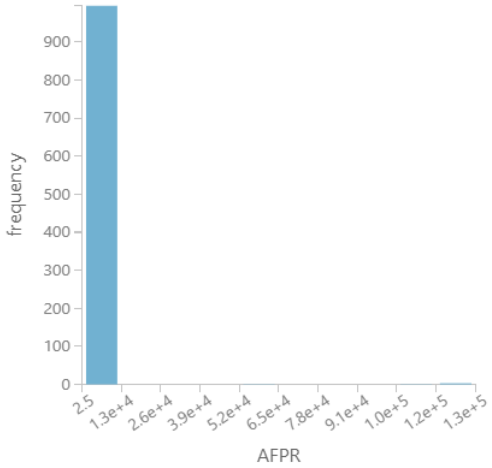


Figura 51: Andamento KPI AFPR

Anche in questo caso si può notare come la frequenza è alta in funzione di un valore basso del KPI AFPR, che sta a significare che vengono rilevati pochi account falsi positivi.

Di seguito vengono mostrate delle curve di prestazione a livello di account, che confrontano I KPI sopra descritti, generate dal un set di dati utilizzato nel modello, che ha una numerosità di circa 200.000 transazioni.

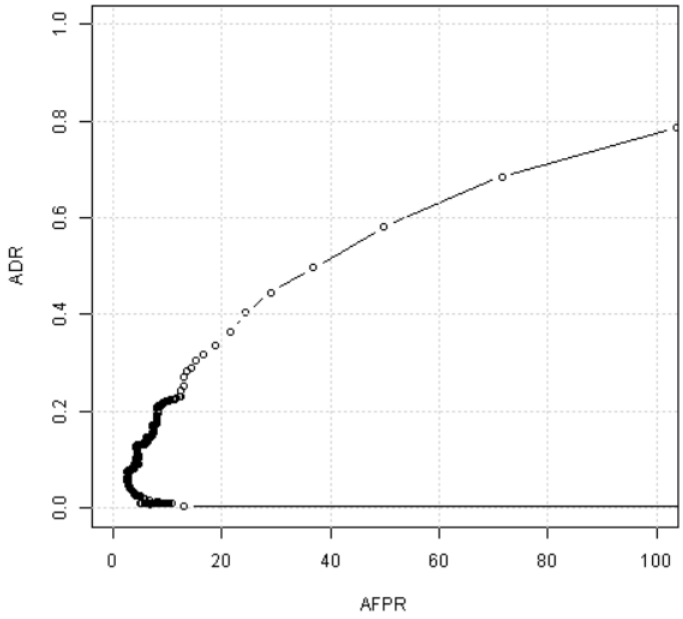


Figura 51: curva ROC ADR - AFPR

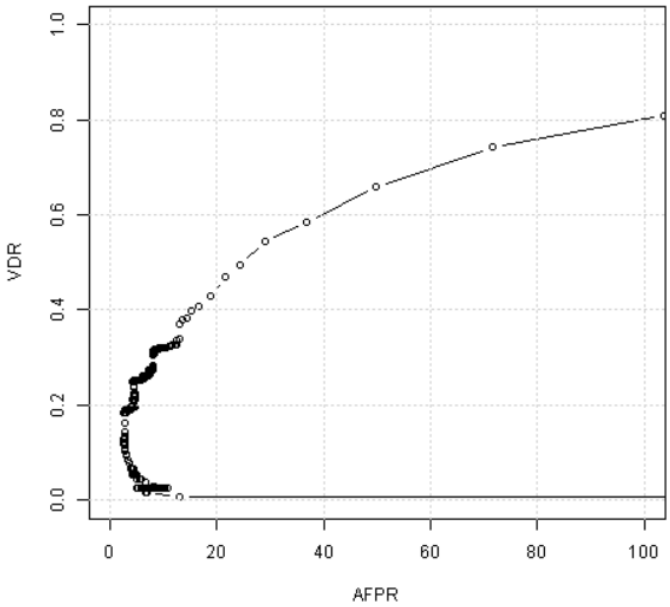


Figura 52: curva ROC VDR - AFPR

Nel caso in cui le dimensioni dei dati sono ridotte e il tasso di frode è molto basso, le curve a livello di account non sembrano uniformi, come si può vedere dalle curve generate da un numero di dati molto minore rispetto a quello usato:

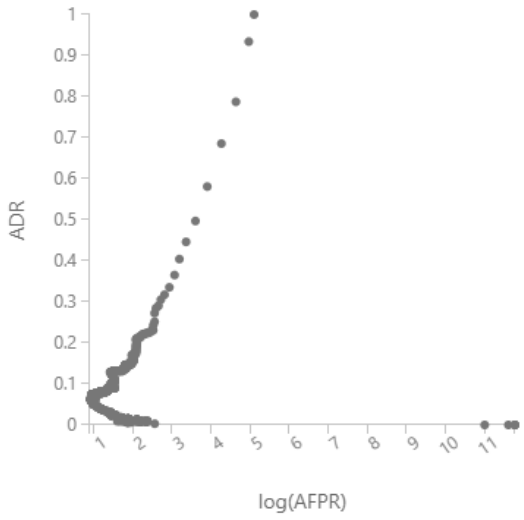


Figura 53: curva ADR – AFPR con dataset di dimensione ridotta

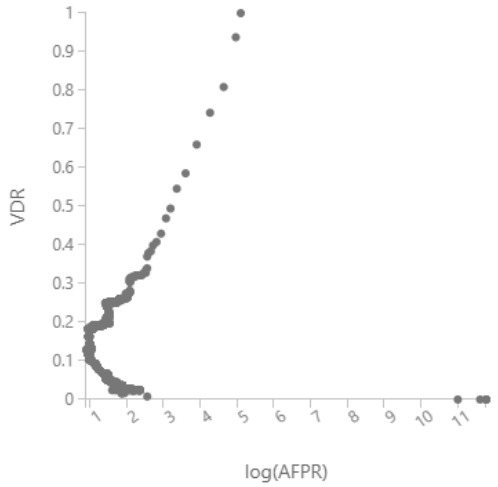
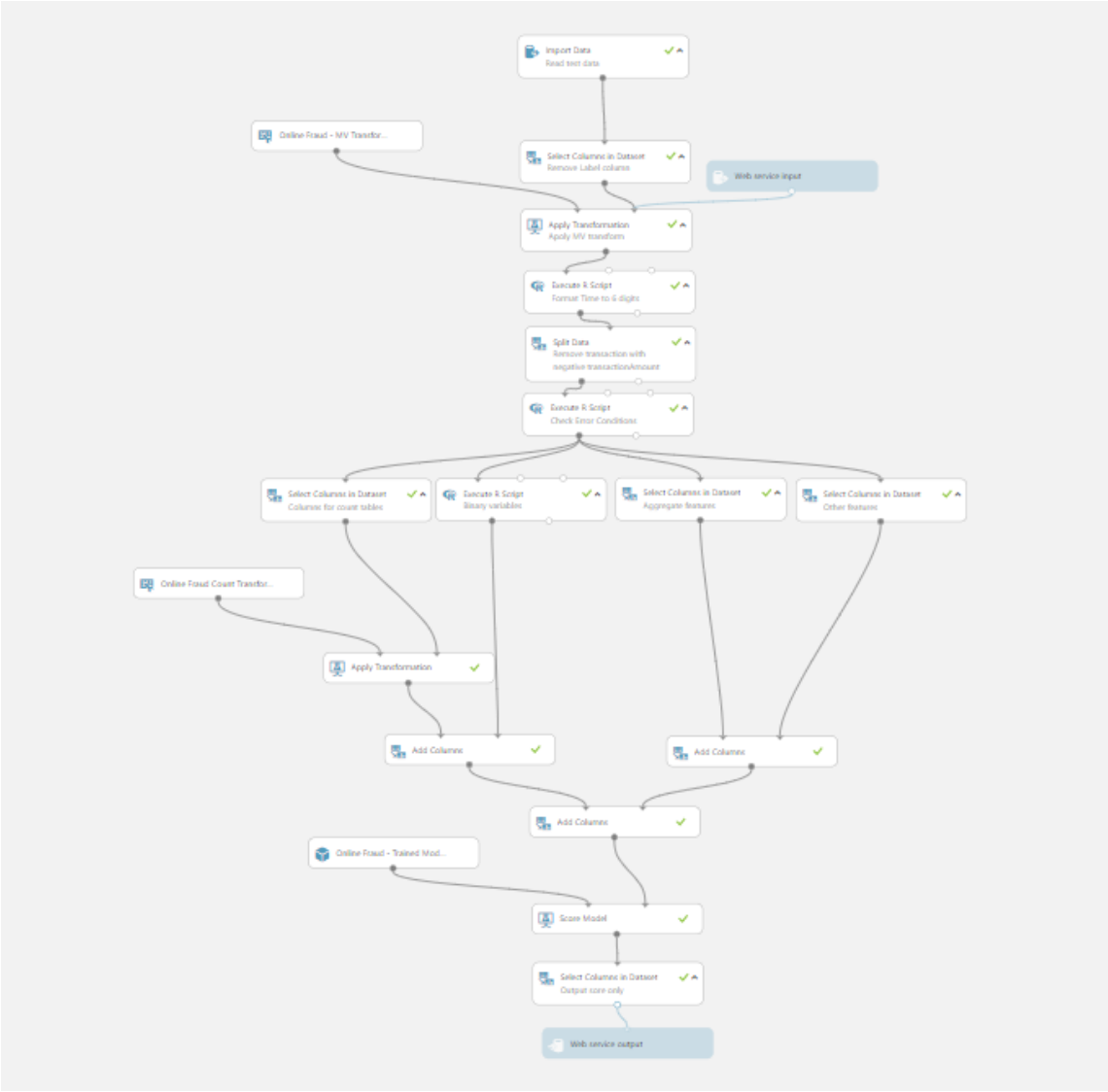


Figura 54: curva VDR – AFPR con dataset di dimensione ridotta

In conclusione, anche rispetto ad un'analisi a livello di account il modello proposto garantisce, quindi, delle performance ottimali.

3.12 Publish web service

Il modello addestrato è ora pronto per l'implementazione come servizio Web. Per distribuire un modello, dobbiamo collegare tutte le macrofasi come mostrato nella figura seguente.



Dopo aver fatto questo, basta cliccare sul pulsante destinato alla pubblicazione per poter collegare il modello creato ad una applicazione esterna.

4. CONCLUSIONI

Il rilevamento delle frodi derivanti da carte di credito è un compito particolarmente impegnativo e complesso. In genere, le attività fraudolente sono eventi rari, difficili da modellare ed in costante evoluzione. Questa tesi ha esaminato come gli algoritmi di apprendimento automatico possano essere utilizzati per affrontare il problema. In particolare, ci si è concentrati sulla progettazione di un framework in grado di valutare le transazioni più rischiose, mediante algoritmi diretti a gestire flussi di dati sbilanciati ed in continua evoluzione, usando logiche basate sull'apprendimento automatico e tecniche di data mining che consentono di rilevare automaticamente frodi in presenza di grandi quantità di transazioni. Attualmente le infrastrutture IT utilizzate di basano su architetture classiche, risultando ben progettate per la produzione di report aziendali, ma non per l'applicazione dell'analisi a grandi volumi di dati. Tramite l'uso del tool Azure Machine Learning messo a disposizione da Microsoft®, è stato implementato un modello di analisi per grandi quantità di dati basato su logiche di machine learning. A partire da un dataset di dati transazionali reali, ottenuto attraverso l'esperienza lavorativa, è stato progettato un modello che permette l'identificazione di schemi fraudolenti nelle transazioni effettuate con carte di credito.

Per fare ciò, sono stati seguiti degli step di processo che sono riassunti nelle seguenti fasi:

- Aggregazione dei dati
- Strutturazione dei dati
- Implementazione logiche di arricchimento
- Addestramento del modello

- Valutazione delle capacità previsionali del modello

Ricevendo in input dei dati grezzi, il modello effettua delle operazioni finalizzate alla standardizzazione dei dati, rispetto ai valori presenti nei campi del dataset di ingresso. Nello step di arricchimento, a partire dalle informazioni presenti nei campi del dataset iniziale, sono state aggiunte caratteristiche al fine di permettere alle logiche di apprendimento di basare le loro stime su informazioni mirate, riuscendo così a diminuire il tempo di computazione ed aumentando l'efficacia del risultato. Il modello è stato addestrato utilizzando una metodologia basata sulla classificazione dei dati, ovvero con lo scopo di definire se la singola transazione sia o meno fraudolenta. A valle di opportuni test, si è scelto l'algoritmo two class boosted decision tree, basato su alberi decisionali che in input ricevono sia i classici campi forniti dal set di dati, che le features aggiunte nello step precedente. Questo algoritmo, attraverso la creazione di un numero di alberi decisionali che può essere regolato dall'utente per aumentare o diminuire l'accuratezza in funzione della numerosità delle transazioni in ingresso, utilizza un metodo che combina il risultato di tutti gli alberi creati per fornire una stima che risulta essere precisa ed accurata. Inoltre questa scelta garantisce un apprendimento rapido, facilità di tuning e la gestione di un numero di variabili molto alto. Nel caso di interesse, questo si riflette in una elasticità del modello che, nell'ambito delle transazioni relative alle carte di credito, in cui i metodi e gli schemi di frode messi in atto risultano essere in continua evoluzione, risulta essere un vantaggio competitivo. Per la valutazione dei risultati si è proceduto all'analisi rispetto alle due leve principali, transazione ed account. Ciò è stato fatto perchè in una logica aziendale, quando una transazione sospetta viene identificata, si procede al blocco del relativo conto. Quindi, attraverso l'uso di curve ROC, si è valutato il modello rispetto al fattore transazione, cha hanno mostrato risultati con ottimi livelli di accuratezza e precisione nella rilevazione delle transazioni

fraudolente. A livello di account invece, sono state utilizzate metriche differenti, come la misurazione della capacità di rilevazione degli account fraudolenti rilevati sulla totalità degli account, e gli account falsi positivi rilevati sul totale degli account fraudolenti rilevati, mettendoli a confronto con la percentuale di risparmio ottenuta. Anche con questo tipo di metriche, il modello ha mostrato alti livelli di accuratezza e precisione.

Altra caratteristica rilevante a livello aziendale, è quella di poter connettere il modello ad applicazioni esterne in maniera molto semplice. Attraverso una API dedicata infatti, è possibile collegare un framework esterno in ingresso al modello, permettendo così l'analisi dei dati in maniera near real time. Questo si traduce inoltre in una elevatà flessibilità, poichè permette al modello implementato di ricevere in ingresso differenti fonti di dati.

In conclusione, il progetto di dottorato è stata un'opportunità unica per lavorare sulla rilevazione di frodi basata su dati reali raccolti nell'esperienza lavorativa che, a causa della loro elevata sensibilità, sono scarsamente disponibili. In genere, le aziende sono interessate a risultati più pratici che teorici, ad esempio "fintanto che l'algoritmo funziona correttamente non è necessario mettere in discussione la sua progettazione o implementazione". Al contrario, il mondo accademico a volte affronta problemi complessi che hanno poche applicazioni pratiche nell'immediato. Con questo lavoro ho avuto modo di mettere in connessione i due mondi che, a mio modesto parere, dovrebbero guardarsi e scambiarsi idee in maniera più frequente ed avere così un impatto concreto per la società.

5. BIBLIOGRAFIA

[1], Doğan, B., Öztayşi, B.Intelligent visual analysis in employee fraud detection2020Advances in Intelligent Systems and Computing

[2], Handoko, B.L., NatasyaFraud diamond model for fraudulent financial statement detection2019International Journal of Recent Technology and Engineering

[3], Koilada, D.V.S.R.K.Strategic Spam Call Control and Fraud Management: Transforming Global Communications2019IEEE Engineering Management Review

[4], Soomro, Z.A., Ahmed, J., Shah, M.H., Khoumbati, K.Investigating identity fraud management practices in e-tail sector: a systematic review2019Journal of Enterprise Information Management

[5], Amasiatu, C.V., Shah, M.H.The management of first party fraud in e-tailing: a qualitative study2019International Journal of Retail and Distribution Management

[6], Repousis, S., Lois, P., Veli, V.An investigation of the fraud risk and fraud scheme methods in Greek commercial banks2019Journal of Money Laundering Control

[7], Ohalehi, P.Fraud in small charities: evidence from England and Wales2019Journal of Financial Crime

[8], Venter, A.C.A procurement fraud risk management model2019Meditari Accountancy Research

[9], Pehlivanli, D., Eken, S., Ayan, E.Detection of fraud risks in retailing sector using MLP and SVM techniques2019Turkish Journal of Electrical Engineering and Computer Sciences

[10], Vitters, C., Oven, C.L., Gelles, M.Cultivating and measuring risk culture to achieve forward momentum on ERM2019Public Sector Enterprise Risk Management: Advancing Beyond the Basics

[11], Trikha, A., Khant, S.M.Queue Classification for Fraud Types: Banking Domain2019Advances in Intelligent Systems and Computing

[12], Soviany, C.The benefits of using artificial intelligence in payment fraud detection: A case study2018Journal of Payments Strategy and Systems

[13], Drábková, Z.CFEBT method as a tool of fraud risk management and decreasing information asymmetry in accounting2018ACRN Journal of Finance and Risk Perspectives

[14], Tarmazakov, E.I., Silnov, D.S.Modern approaches to prevent fraud in mobile communications networks2018Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2018

[15], Amasiatu, C.V., Shah, M.H.First party fraud management: framework for the retail industry2018International Journal of Retail and Distribution Management

[16], Drábková, Z.Fraud risk management from the perspective of cfebt risk triangle of accounting errors and frauds2018Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis

[17], Dawei, L., Anzi, H., Gen, L.Big Data Technology: Application and Cases2018Handbook of Blockchain, Digital Finance, and Inclusion

[18], Yildirim, M.Y., Ozer, M., Davulcu, H.Cost-sensitive decision making for online fraud management2018IFIP Advances in Information and Communication Technology

[19], Magomedov, S., Pavelyev, S., Ivanova, I., Dobrotvorsky, A., Khrestina, M., Yusubaliev, T.Anomaly detection with machine learning and graph databases in fraud management2018International Journal of Advanced Computer Science and Applications

[20], Pandey, P., Saroliya, A., Kumar, R.Analyses and detection of health insurance fraud using data mining and predictive modeling techniques2018Advances in Intelligent Systems and Computing

[21], Liu, X., Wang, X.A network embedding based approach for telecommunications fraud detection2018Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)

[22], [No author name available]1st International Conference on Ubiquitous Communications and Network Computing, UBICNET 20172018Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST

[23], Kühn, S., Nieman, A.Can security vetting be extended to include the detection of financial misconduct?2017African Security Review

[24], Artikis, A., Katzouris, N., Correia, I., Baber, C., Morar, N., Skarbovsky, I., Fournier, F., Paliouras, G.Industry paper: A prototype for credit card fraud management2017DEBS 2017 - Proceedings of the 11th ACM International Conference on Distributed Event-Based Systems

[25], Correia, I., Artikis, A., Katzouris, N., Baber, C., Morar, N., Skarbovsky, I., Fournier, F., Paliouras, G.Demo: Demonstration of a prototype for credit card fraud management2017DEBS 2017 - Proceedings of the 11th ACM International Conference on Distributed Event-Based Systems

[26], Kabuye, F., Nkundabanyanga, S.K., Opiso, J., Nakabuye, Z.Internal audit organisational status, competencies, activities and fraud management in the financial services sector2017Managerial Auditing Journal

[27], Lutui, R., Ahokovi, T.Financial fraud risk management and corporate governance2017Proceedings of the 15th Australian Information Security Management Conference, AISM 2017

[28], [No author name available]Proceedings of the 15th Australian Information Security Management Conference, AISM 20172017Proceedings of the 15th Australian Information Security Management Conference, AISM 2017
[29], Westhausen, H.-U.The escalating relevance of internal auditing as anti-fraud control2017Journal of Financial Crime
[30], Mu, E., Carroll, J.Development of a fraud risk decision model for prioritizing fraud risk cases in manufacturing firms2016International Journal of Production Economics
[31], Alavi, H.Mitigating the Risk of Fraud in Documentary Letters of Credit2016Baltic Journal of European Studies
[32], Hess, M.F., Cottrell, J.H.Fraud risk management: A small business perspective2016Business Horizons
[33], Dzomira, S.Cyber-banking fraud risk mitigation - Conceptual model2015Banks and Bank Systems
[34], Srivastava, U., Gopalkrishnan, S.Impact of big data analytics on banking sector: Learning for Indian Banks2015Procedia Computer Science
[35], Ananthakrishnan, U.M., Li, B., Smith, M.D.A tangled web: Evaluating the impact of displaying fraudulent reviews20152015 International Conference on Information Systems: Exploring the Information Frontier, ICIS 2015
[36], Arora, R., Gupta, D., Pahwa, P.Fraud detection life cycle model: A systematic fuzzy approach to fraud management2015International Journal of Computational Intelligence and Applications
[37], Manisera, M., Zuccolotto, P.Visualizing multiple results from nonlinear CUB models with R grid view ports2015Electronic Journal of Applied Statistical Analysis
[38], Mui, G., Mailley, J.A tale of two triangles: Comparing the fraud triangle with criminology's crime triangle2015Accounting Research Journal

[39], Frimpong, K.Back to basics: Fighting fraud and austerity2015Journal of Financial Crime
[40], Agarwal, N., Sharma, M.Fraud Risk Prediction in Merchant-Bank Relationship using Regression Modeling2014Vikalpa
[41], Stamler, R.T., Marschdorf, H.J., Possamai, M.Fraud prevention and detection: Warning signs and the red flag system2014Fraud Prevention and Detection: Warning Signs and the Red Flag System
[42], Dorfleitner, G., Jahnes, H.What factors drive personal loan fraud? Evidence from Germany2014Review of Managerial Science
[43], Argyriou, E.N., Symvonis, A., Vassiliou, V.A fraud detection visualization system utilizing radial drawings and heat-maps2014IVAPP 2014 - Proceedings of the 5th International Conference on Information Visualization Theory and Applications
[44], Alraouji, Y., Bramantoro, A.International call fraud detection systems and techniques2014MEDES 2014 - 6th International Conference on Management of Emergent Digital EcoSystems, Proceedings
[45], Dilla, W.N., Harrison, A.J., Mennecke, B.E., Janvrin, D.J.The assets are virtual but the behavior is real: An analysis of fraud in virtual worlds and its implications for the real world2013Journal of Information Systems
[46], Le Maux, J., Smaili, N., Amar, W.B.From fraud in management to fraud management [De la fraude en gestion à la gestion de la fraude: Une revue de la literature]2013Revue Francaise de Gestion
[47], Zawadzki, C.Risk of fraud management through informal internal control mechanisms. The SMEs case [La maîtrise du risque de fraude par des mécanismes informels: Le cas d'une pme familial]2013Revue Francaise de Gestion
[48], Ai, J., Brockett, P.L., Golden, L.L., Guillén, M.A Robust Unsupervised Method for Fraud Rate Estimation2013Journal of Risk and Insurance

[49], Jackson, P.M.Debate: Fraud risk management in the public sector2013Public Money and Management
[50], Power, M.The apparatus of fraud risk2013Accounting, Organizations and Society
[51], Gaviglio, A., Pirani, A., Demartini, E.The regulatory framework for trade names of fish products in fraud management: A useful tool or an unsolved problem? [Il quadro normativo sulle denominazioni commerciali dei prodotti ittici nella gestione delle frodi: Strumento utile o problema irrisolto?]2013Economia Agro-Alimentare
[52], Pabst, R.BusinessForensics HQ2012IEEE Conference on Visual Analytics Science and Technology 2012, VAST 2012 - Proceedings
[53], Chou, C.-Y., Liu, C.-W., Tseng, K.-Y., Cheng, C.-W., Lu, F.-S.Challenges of system virtualization: Taking FMS2.0 virtualization as an example201214th Asia-Pacific Network Operations and Management Symposium: "Management in the Big Data and IoT Era", APNOMS 2012 - Final Program
[54], Othman, I.W., Hasan, H., Tapsir, R., Rahman, N.A., Tarmuji, I., Majdi, S., Masuri, S.A., Omar, N.Text readability and fraud detection2012ISBEIA 2012 - IEEE Symposium on Business, Engineering and Industrial Applications
[55], Zhang, Y.Documentary letter of credit fraud risk management2012Journal of Financial Crime
[56], Edge, M.E., Falcone Sampaio, P.R.The design of FFML: A rule-based policy modelling language for proactive fraud management in financial data streams2012Expert Systems with Applications
[57], Jinka, P., Rao, G.S.V.R.K., Sundararaman, K.ClaimPerfect - An application case study of Machine Learning techniques towards a fraud management system for warranty claims processing2012Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication, ICUIMC'12

[58], Pagano, M., Immordino, G.Corporate fraud, governance, and auditing2012Review of Corporate Finance Studies
[59], Chen, Y., Hu, J., Gai, X., Sun, Y.A privilege separation method for security commercial transactions2011Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering
[60], Lopes, J., Belo, O., Vieira, C.Applying user signatures on fraud detection in telecommunications networks2011Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)
[61], Simborg, D.W.There is no neutral position on fraud!2011Journal of the American Medical Informatics Association
[62], Zanzig, J.S., Flesher, D.L.Internal auditors speak out on controlling employee fraud2011Research on Professional Responsibility and Ethics in Accounting
[63], Furlan, S., Vasilecas, O., Bajec, M.Method for selection of motor insurance fraud management system components based on business performance2011Technological and Economic Development of Economy
[64], Ruiz-Agundez, I., Penya, Y.K., Bringas, P.G.Fraud detection for voice over IP services on next-generation networks2010Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)
[65], Unal, E., Yates, D.J.Enterprise fraud management using cloud computing: A cost-benefit analysis framework201018th European Conference on Information Systems, ECIS 2010
[66], Chen, Y., Hu, J., Sun, Y., Gai, X.A privilege separation method for security commercial transactions2010China Communications

[67], Ryman-Tubb, N.F.Neural-Symbolic processing in business applications: Credit card fraud detection2010Computational Neuroscience for Advancing Artificial Intelligence: Models, Methods and Applications
[68], Ghosh, M.Mobile ID fraud: The downside of mobile growth2010Computer Fraud and Security
[69], Hassink, H., Meuwissen, R., Bollen, L.Fraud detection, redress and reporting by auditors2010Managerial Auditing Journal
[70], Thompson, T.Adding up the real cost of fraud2010Computer Fraud and Security
[71], Jamieson, R., Smith, S., Stephens, G., Winchester, D.An approach to managing identity fraud2009Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions
[72], De Bie, B.Fraud in hospitals: Lessons from forensic auditing [Fraude in ziekenhuizen: Lessen uit de forensische auditpraktijk]2009Acta Hospitalia
[73], Edge, M.E., Sampaio, P.R.F., Philpott, O., Choudhary, M.Specifying and compiling high level financial fraud policies into StreamSQL2009ICEIS 2009 - 11th International Conference on Enterprise Information Systems, Proceedings
[74], Edge, M.E., Falcone Sampaio, P.R.A survey of signature based methods for financial fraud detection2009Computers and Security
[75], Bihina Bella, M.A., Eloff, J.H.P., Olivier, M.S.A fraud management system architecture for next-generation networks2009Forensic Science International
[76], Almeida, P., Jorge, M., Cortesão, L., Martins, F., Vieira, M., Gomes, P.Supporting fraud analysis in mobile telecommunications using case-based reasoning2008Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)

[77], Edge, M., Sampaio, P., Philpott, O., Choudhary, M.A policy distribution service for proactive fraud management over financial data streams2008Proceedings - 2008 IEEE International Conference on Services Computing, SCC 2008

[78], Baharim, K.N., Kamaruddin, M.S., Jusof, F.Leveraging missing values in call detail record using naïve bayes for fraud analysis20082008 International Conference on Information Networking, ICOIN

[79], Suntinger, M., Schiefer, J., Obweger, H., Gröller, M.E.The event tunnel: Interactive visualization of complex event streams for business process pattern analysis2008IEEE Pacific Visualisation Symposium 2008, PacificVis - Proceedings

[80], Marks, N.Fraud management in the 21st century2008EDPACS

[81], Jamieson, R., Winchester, D., Smith, S.Development of a conceptual framework for managing identity fraud2007Proceedings of the Annual Hawaii International Conference on System Sciences

[82], Edge, M.E., Falcone Sampaio, P.R., Choudhary, M.Towards a proactive fraud management framework for financial data streams2007Proceedings - DASC 2007: Third IEEE International Symposium on Dependable, Autonomic and Secure Computing

[83], Nambiar, S., Chang-Tien, L.M-payment solutions and m-commerce fraud management2007Advances in Banking Technology and Management: Impacts of ICT and CRM

[84], Rozsnyai, S., Schiefer, J., Schatten, A.Solution architecture for detecting and preventing fraud in real time20072007 2nd International Conference on Digital Information Management, ICDIM

[85], Wong, A.K.A.Y., Paramesh, N., Pradeep, R.A.Y.Towards an ontology mapping approach for security management2006International Journal on Artificial Intelligence Tools

[86], Hanson, S.P., Cassidy, B.S.RHIOs--build in healthcare fraud management from the beginning.2006Journal of healthcare information management : JHIM

[87], Burger, R., Hatt, S.“Are you the weakest link?": The FSA’s financial crime review2006Journal of Financial Regulation and Compliance

[88], Hall, J., Barbeau, M., Kranakis, E.Anomaly-based intrusion detection using mobility profiles of public transportation users20052005 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob'2005

[89], Nadji, B.Future directions in Telecommunications Research2005Proceedings - IEEE Symposium on Computers and Communications

[90], Sevast'yanov, A.Systems for fighting with fraud HP FMS for telecommunication networks operators2004Elektrosvyaz

[91], Sandhu, R.Good-enough security: Toward a pragmatic business-driven discipline2003IEEE Distributed Systems Online

[92], Barraclough, PercyTelecom fraud: Risk management1999Telecommunications (Americas Edition)

[93], Lundin, Catharina, Nguyen, Binh, Ewart, BenFraud management and prevention in Ericsson's AMPS/D-AMPS system1996Ericsson Review (English Edition)

[94], Messham, James, Kelly, Phil, Smith, DeanTelecommunications fraud management reducing costs and winning business1995British Telecommunications Engineering

[95], Shafik, E., Basu, K.Real-time automatic message accounting data transport1994Annales Des Télécommunications

[96], “Analyze Every Transaction in the Fight Against Fraud:Using Technology for Effective Fraud Detection,” ACLServices Ltd., 2008.

[97], “The ‘Big Picture’ of Insider IT Sabotage Across U.S.Critical Infrastructures.” Carnegie Mellon, May 2008.

[98], Cappelli, Dawn; Trzeciak, Randal; Moore, Andrew, “InsiderThreats in the SDLC,” CERT, 2006.

[99], Coderre, David G., Computer Aided Fraud Prevention andDetection: A Step-by-Step Guide, John Wiley & Sons,2009.

[100], Coderre, David G., Fraud Analysis Techniques Using ACL,John Wiley & Sons, 2009.

[101], “Data Breaches Surpass 2007 Level, But Businesses AreRarely Penalized,” The Wall Street Journal, Sept. 9, 2008.

[102], “Fraud Risk Management: Developing a Strategy forPrevention, Detection, and Response,” KPMGInternational, 2006.

[103], Global Technology Audit Guide 3: Continuous Auditing:Implications for Assurance, Monitoring, and RiskAssessment; The IIA; 2005.

[104], Global Technology Audit Guide 5: Managing and Auditing Privacy Risks, The IIA, 2006.

[105], “Insider Threat Study: Illicit Cyber Activity in theInformation Technology and TelecommunicationsSector,” U.S. Secret Service and CERT CoordinationCenter/SEI, January 2008.

[106], Internal Audit 2012: A Study Examining the Future of InternalAuditing and the Potential Decline of a Controls-centricApproach, PricewaterhouseCoopers, 2007.

[107], International Professional Practices Framework. PracticeGuide, Internal Auditing and Fraud. The IIA 2009Lanza, Richard B.; Brooks, Dean; and Goldman, Mort;

[108], The Buyer’s Guide to Audit, Anti-Fraud, and AssuranceSoftware; Ekaros Publishing; 2008.

[109], Lanza, Richard B. and Gilbet, Scott, “Maximizing JournalEntry Testing Through Automation,” ITAudit, Feb.10,2007.

[110], Lanza, Richard B., “Proactive Control Monitoring,”ITAudit, Nov.15, 2003.

[111], Lanza, Richard B., “Proactively Detecting Fraud UsingComputer Assisted Audit Reports,” The IIA ResearchFoundation, 2003.

[112], Management Anti-fraud Programs and Controls: Guidanceto Help Prevent, Deter, and Detect Fraud; AICPA, TheIIA, Association of Certified Fraud Examiners (ACFE),Information System Accountability and Control

[113], Management Accountants, and Society of HumanAuditors, Financial Executives Institute, Institute ofResource Professionals; 2002.

[114], Managing the Business Risk of Fraud: A Practical Guide; TheIIA, ACFE, and AICPA; 2008.

[115], “Sample Fraud Policy,” ACFE Web site, http://www.acfe.com/documents/sample_fraud_policy.pdf.

[116], SOX Section 404: A Guide for Management by InternalControls Practitioners, Second Edition, The IIA, 2008.

[117], U.S. Department of Justice Web site, Computer Crime andIntellectual Property Section, http://usdoj.gov/criminal/cybercrime, 2009.

[118], “Risk Assessment in Practice.” COSO, October 2012

[119], American Institute of Certified Public Accountants. “Management Antifraud Programs andControls.” New York: American Institute of Certified Public Accountants, Inc., 2002.

[120], “Analyze Every Transaction in the Fight Against Fraud: Using Technology for Effective FraudDetection.” ACL Services Ltd., 2008, www.adfor.it/DOWNLOAD/whitepaper/index.asp.

[121], Apostolou, Barbara. Sampling: A Guide for Internal Auditors. Altamonte Springs, Florida: The Institute of Internal Auditors, 2004.

[122], "AS/NZS ISO 31000:2009, "Risk Management—Principles and Guidelines." StandardsAustralia/Standards New Zealand, sherq.org/31000.pdf.
[123], "Assessing the Adequacy of Risk Management Using ISO 31000" (IPPF Practice Guide). AltamonteSprings, Florida: The Institute of Internal Auditors, 2010.
[124], Audit Committee Effectiveness—What Works Best, third edition. Altamonte Springs, Florida: TheInstitute of Internal Auditors, 2005.
[125], "Auditing External Business Relationships" (IPPF Practice Guide). Altamonte Springs, Florida: The Institute of Internal Auditors, 2009.
[126], "Auditing Privacy Risks" (IPPF Practice Guide). Altamonte Springs, Florida: The Institute of Internal Auditors, 2012.
[127], "Auditing Techniques" course. Altamonte Springs, Florida: The Institute of Internal Auditors.
[128], "Auditing the Control Environment" (IPPF Practice Guide). Altamonte Springs, Florida: The Institute of Internal Auditors, 2011.
[129], https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/import-data?redirectedfrom=MSDN
[130], https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/edit-metadata?redirectedfrom=MSDN
[131], https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/execute-r-script?redirectedfrom=MSDN
[132], https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/remove-duplicate-rows?redirectedfrom=MSDN
[133], https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/select-columns-in-dataset?redirectedfrom=MSDN
[134], https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/split-data?redirectedfrom=MSDN

[135], https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/add-columns?redirectedfrom=MSDN

[136], https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/apply-transformation?redirectedfrom=MSDN

[137], azure-machine-learning-algorithm-cheat-sheet-nov2019

[138], Jerome H Friedmann, IMS 1999 Reitz Lecture, "Greedy Function Approximation: a Gradient Boosting Machine"

[139], Transparency_Guida_WHISTLEBLOWING

[141], Costabile, Business integrity e corporate compliance

"[142], Costabile, COMPUTER FORENSICS AZIENDALE FONDAMENTI DELLE BEST PRACTICE AZIENDALI E RUOLO DELLA POLICY AZIENDALE"

[143], Costabile, le prove digitali sulla scena del crimine

[145], Marletto, LUISS _ LTKA _ Rischi operativo e frode in banca

[146], Marletto, LUISS _ LTKA _ Rischio Canale

[147], Stellacci_IL RUOLO CHIAVE DELL'ANTIFRODE IN AMBITO ASSICURATIVO

[148], Fellegara, Fraud Risk Identification

[149], Paraggio,La Gestione delle Frodi nelle Telecomunicazioni

[150], Oracle, LE FRODI NELLA RETE

[151], INTRODUCING AZURE MACHINE LEARNING

[152], Scattereggia, 01 Valutazione delle capacità predittive di un FMS