Sommario

Premessa

Il" Global economic crime survey 2016" di Price Waterhouse & Coopers", nell'addendum relativo alla situazione italiana, sviluppa una fotografia aggiornata del fenomeno con relativi dati e statistiche. Il report è disponibile in internet https://www.pwc.com/it/it/services/forensic/assets/docs/gecs-2016-es.pdf

Dal citato survey innanzitutto emerge che il fenomeno dei crimini economici è in aumento, rispetto all'anno precedente, sia in Italia che nel mondo con % significative: rispettivamente 41% di aumento a livello Italia, contro 27% a livello globale.

A livello mondiale il 36% delle imprese intervistate ha dichiarato di aver subito almeno una frode, contro il 21% a livello Italia. Nelle varie tipologie di frodi, a livello Italia , la frode più diffusa risulta l'appropriazione indebita, seguita nell'ordine di importanza da: corruzione, cyber crime, frodi contabili, frodi in materia di appalti e acquisti, frodi nell'ambito delle risorse umane, riciclaggio di denaro, frodi fiscali, , frodi creditizie, violazioni della concorrenza, antitrust, spionaggio, violazione della proprietà intellettuale, insider trading.

Come vengono individuate le frodi? Il 36% di esse viene intercettato tramite modalità fuori dal controllo e dall'influenza del management aziendale; in particolare il 24% è stato scoperto dalle forze dell'ordine. Ciò significa che le organizzazioni arrivano spesso in ritardo nell'individuare le frodi e a fronteggiare i danni conseguenti. Dalla stessa survey emerge che meno della metà (47%) delle organizzazioni italiane ha intercettato l'evento fraudolento attraverso un sistema di controllo interno. In particolare risulta inoltre particolarmente debole il sistema delle cd soffiate, cioè il whistleblowing (3%); ciò sembra la conseguenza sia di una scarsa cultura aziendale sia di norme non ancora pienamente efficaci in materia. Un miglioramento è atteso dalle linee guida che l'ANAC (Attività Anti Corruzione) sta emettendo, che dalle nuove norme governative anticorruzione.

Qual è il costo della criminalità economica? Esso è dato non solo dai danni diretti,ma soprattutto dai danni indiretti causati: alla reputazione aziendale e alla forza del marchio, alla motivazione dei dipendenti, alle relazioni commerciali, ai rapporti con le autorità di vigilanza. La corruzione inoltre distorce la concorrenza e frena lo sviluppo.

In Italia l'esecutore delle frodi è un soggetto situato all'interno dell'azienda nel 43% dei casi, esterno all'azienda nel 31%, nei restanti casi non è stato possibile individuare la provenienza dell'attore della frode. L'identikit dell'esecutore delle frodi a livello italiano è di sesso maschile, di età compresa fra 31 e 40 anni,

con una buona esperienza lavorativa alle spalle che va da 3 a 5 anni, posizionato prevalentemente nel middle management.

Al centro di qualsiasi criminalità, a prescindere dal motivo per cui è stata commessa, vi è un comportamento umano. Per tale motivo le aziende dovrebbero promuovere la cultura dell'etica e del rispetto della legalità. In Italia sta emergendo la consapevolezza che le persone e la cultura sono in prima linea di difesa contro le frodi economico – finanziarie. Dalla citata survey di PWC emerge che l'86% delle aziende ha attuato o sta attuando un programma di etica e compliance all'interno dell'azienda. Un programma di compliance deve essere adeguatamente progettato ed in grado di offrire un evidente beneficio per il business. Per questo motivo dovrebbe includere meccanismi che contribuiscano a motivare e premiare le persone misurandone, nella misura del possibile, i risultati. Tale programma dovrebbe quindi comprendere dei codici di condotta aggiornati, deve fondarsi su una chiara politica, affrontando la connessione fra valori, comportamenti e processo decisionale.

Definizioni, norme di riferimento, red flags

E' interessante notare che, agli albori del diritto, chi otteneva un bene altrui con l'uso della forza o della destrezza era ritenuto colpevole, rispettivamente di rapina o di furto e conseguentemente condannato a pena di vario genere e gravità. Al contrario colui che carpiva con l'inganno ricchezze appartenenti a terzi non era considerato colpevole di aver commesso alcun reato.

Negli ultimi anni si è creata una crescente consapevolezza dell'elevata pericolosità e gravità del fenomeno delle frodi aziendali (cd white collar crime), accompagnata da un giudizio critico negativo sulle misure preventive e dissuasive messe in atto dalle autorità e dai governi per contrastare tali azioni illegali, misure giudicate troppo blande, inadeguate e spesso tardive.

Ciò è anche la conseguenza della crescita di tali atti, come appare anche dallo studio di ACFE-(association of certified fraud examiners) 2016-"Report-to-the-nations 2016", rilevabile in: https://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf.

A livello mondiale infatti:

- una tipica organizzazione perde mediamente il 5% dei ricavi come conseguenza di una frode;
- la stima delle frodi annue a livello mondiale è pari a 6,3 Miliardi di $
- la perdita media per organizzazione è di $ 150.000, con il 23% dei casi in cui le perdite superano $ 1 milione

- la durata media di una frode è risultata di 18 mesi;
- le piccole organizzazioni hanno un minor grado di controlli antifrode e pertanto sono più vulnerabili delle organizzazioni di maggiore dimensione.

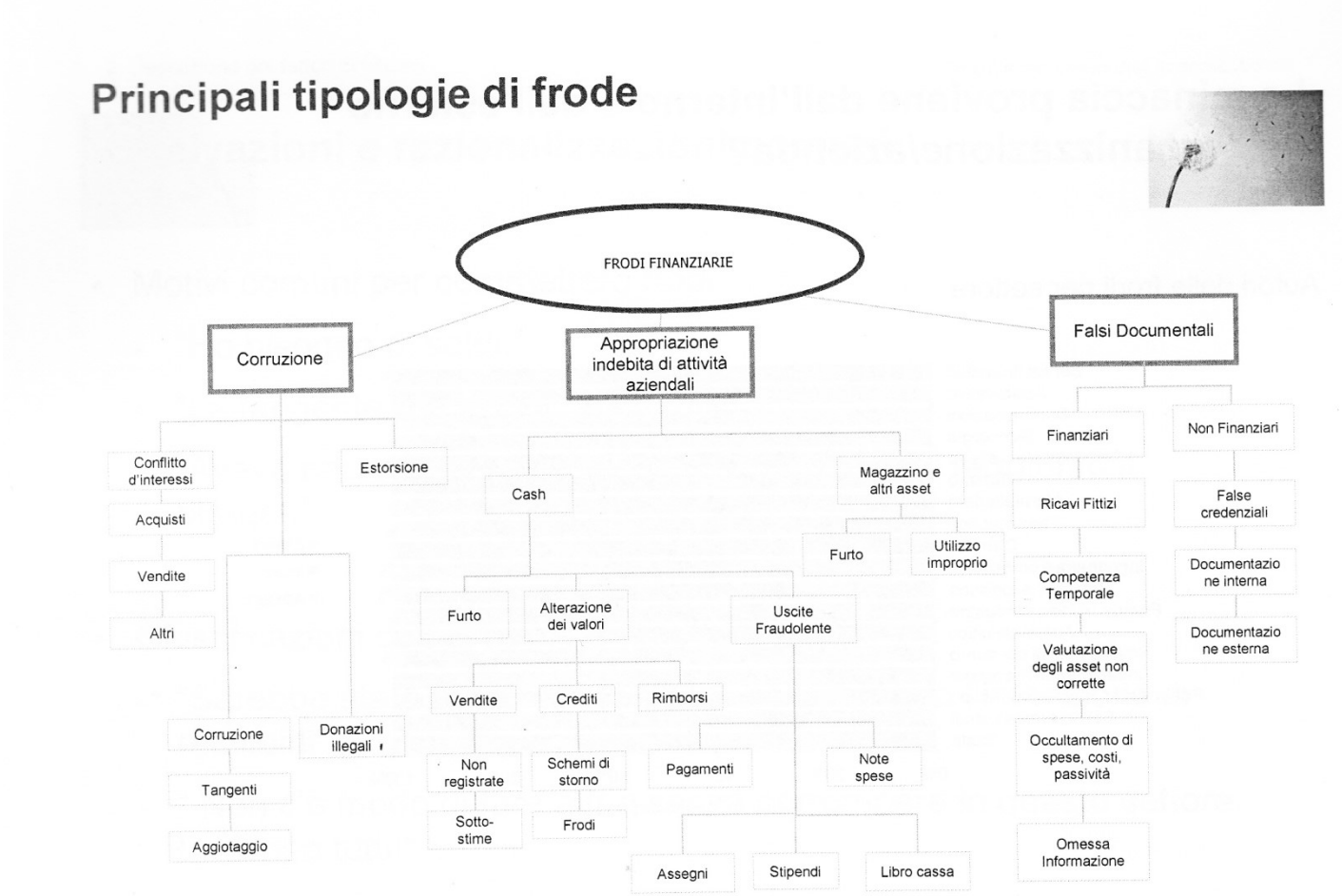
Cercando di definire il termine frode possiamo identificarla come i molteplici mezzi e metodi cui un individuo ricorre intenzionalmente, con l'ausilio di false rappresentazioni, allo scopo di conseguire un vantaggio nei confronti di un terzo. In sostanza si riferisce a qualunque tipo di inganno, comprensivo della manipolazione della verità alla soppressione o occultamento di qualunque fatto o informazione, in conseguenza del quale una parte è costretta a separarsi da una proprietà per meno del valore effettivo, ovvero a corrispondere un corrispettivo maggiore del giusto per averi di proprietà altrui.

Quali sono le principali caratteristiche della frode? La prima è la premeditazione, cioè è necessaria la presenza di un preordinato e organizzato disegno finalizzato al conseguimento del piano illecito. Inoltre chi froda cerca di occultare i predetti schemi; , cioè cerca di dissimulare una sostanza illecita con una forma, almeno all'apparenza, lecita. Terzo elemento, normalmente presente, è che il frodatore tende a sfruttare delle opportunità date ad esempio da particolari competenze o responsabilità di cui è dotato, ovvero dalla vulnerabilità di determinati soggetti o di determinate procedure nell'ambito dell'organizzazione aziendale.

I riferimenti alla nostra legislazione sono sparsi, senza un ordine sistematico, in diversi testi legislativi originati in un ampio arco temporale, in particolare:

- art. 1344 codice civile – contratto in frode alla legge. – "Si reputa altresì illecita la causa quando il contratto costituisce il mezzo per eludere l'applicazione di una norma imperativa".
- art. 515 codice penale – frode nell'esercizio di un commercio – "Chiunque, nell'esercizio di una attività commerciale, ovvero in uno spaccio aperto al pubblico consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita è punito ….. (Omissis)"
- art. 640 codice penale – truffa – "Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito ….(omissis) "
- art 646 cod penale - Appropriazione indebita
- artt. 318 e 319 c.p. e anche art. 319 ter, 320, 321 e 322 c.p. sul fenomeno della corruzione in ambito pubblico; art 2635 cod civile sulla corruzione fra privati
- legge 6 novembre 2012, n. 190 - "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione" (cd Legge Severino);
- decreto Legislativo 25 maggio 2016, n. 97 - "Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza"
- bancarotta semplice e bancarotta fraudolenta, artt 216, 217 e segg della Legge fallimentare
- false comunicazioni sociali, artt 2621 e segg. cod civile

Di seguito si riassume in uno schema le principali tipologie di frode, proposta da ACFE (Association of Certified Fraud Examiners), con qualche adattamento nella traduzione in italiano:



Come si può vedere dal prospetto le frodi possono essere distinte in tre macrocategorie: (a) Corruzione; (b) Appropriazione indebita di attività(asset misappropriation), (c) Falsi documentali.

Esaminiamo separatamente le tre categorie

Corruzione, concussione, estorsione

La corruzione può essere definito come un reato di solito connesso alla pubblica amministrazione, consistente nel derogare e nell'indurre a derogare ai doveri d'ufficio in cambio di denaro o di altri vantaggi personali. In realtà il fenomeno della corruzione può riguardare anche il settore privato, oltre a quello pubblico, in Italia tale reato ha ancora trovato una sua allocazione solo recentemente con il Decreto legislativo, 15/03/2017 n° 38.

Differenza fra corruzione e concussione. Nella corruzione in senso generico il pubblico ufficiale o l'incaricato di pubblico servizio percepiscono l'utilità in seguito ad un accordo con il privato, viceversa, nella concussione il pubblico ufficiale sfrutta la propria posizione di supremazia o potere per costringere o comunque indurre il privato a corrispondere o promettere denaro o altre utilità. Le due fattispecie criminose sono, pertanto, l'una l'opposto dell'altra. La giurisprudenza si è a questo proposito interrogata sul criterio che consenta di stabilire quando la dazione è frutto di accordo (corruzione) e quando invece è frutto di costrizione o induzione (concussione).

La corruzione è spesso abbinata a situazioni di conflitto di interesse. Il conflitto di interessi è una condizione che si verifica quando viene affidata un'alta responsabilità decisionale a un soggetto che abbia interessi personali o professionali in contrasto con l'imparzialità richiesta da tale responsabilità.

Non bisogna dimenticare che la corruzione crea legami e vincoli di debito e di riconoscenza; difficilmente si presenta come azione isolata e fine a se stessa: Il corruttore diviene corrotto per sdebitarsi e il corrotto, a sua volta, si tramuta in corruttore per ottenere un beneficio da quanto occultato, innescando così una spirale perversa, ove peraltro il confine fra cortesia, riconoscenza e illecito diviene labile.

Si ha invece estorsione quando il reato è commesso da chi, con violenza o minaccia, costringa uno o più soggetti a fare o a non fare qualche atto al fine di trarne un ingiusto profitto con altrui danno.

Collegato al fenomeno della corruzione c'è la costituzione di "fondi neri", spesso collegati a costituzione di conti esteri. Questo è un dato criminologicamente rilevante in un crescente numero di paesi occidentali, e fra questi l'Italia non può certo dirsi fra gli ultimi Attraverso fondi non contabilizzati in bilancio si creano somme sfruttabili da amministratori sleali per operazioni illecite, volte a favorire indebitamente la rispettiva impresa societaria

Può anche essere utile avere un'idea di come si colloca l'Italia nel mondo, con riguardo al fenomeno della corruzione. Per far ciò si può fare riferimento ai report emessi da Trasparency International – Italia. Trasparency calcola il fenomeno corruttivo in base al cd indice di percezione del fenomeno, che per sua natura non può essere rilevato in alcuna statistica ufficiale , considerando anche che la corruzione emersa e perseguita in sede giudiziaria è solamente la punta di un iceberg. Dal 2012, anno dell'approvazione della Legge Severino, l'Italia ha migliarato, scalando 12 posizioni, passando dalla 72^, all'attuale 60^ (su un totale di 176 paesi nel mondo). Il nostro Paese segna quindi un miglioramento, ma ancora troppo poco per poterci dire soddisfatti.

Il rapporto 2016 di Trasparency International è rintracciabile:
https://www.transparency.org/whatwedo/publication/corruption_perceptions_index_2016

Appropriazione indebita di attività aziendali

Il delitto di appropriazione indebita ex art. 646 c.p. appartiene alla categoria dei "delitti contro il patrimonio", ed è il reato perpetrato da chiunque, per procurare a sé o ad altri un ingiusto profitto, appropriandosi del denaro o della cosa mobile altrui, della quale abbia, a qualsiasi titolo, il possesso.

Nella pratica aziendale l'appropriazione indebita si concretizza: (a) come sottrazione di denaro (cash misappropriation) alla società per proprio vantaggio, effettuando pagamenti dai conti della società a proprio

beneficio, mediante finte consulenze ovvero pagamenti fittizi a fornitori, ovvero alterando a proprio vantaggio valori dei crediti o delle vendite; (b) come alterazione o utilizzo improprio del magazzino ovvero di altre attività, quali cespiti o strumenti della manutenzione (non cash misappropriation). In entrambe i casi l'autore della frode sfrutta a proprio vantaggio vulnerabilità presenti nella struttura organizzativa aziendale.

Fra le due categorie, cash e non cash misappropriation, la prima è di gran lunga la più frequente. Ciò è dovuto alla maggiore occultabilità del denaro (e migliore gestibilità), in assenza di terzi con funzione di ricettatori che aiutino a piazzare e rendere liquido il bene sottratto.

L'appropriazione indebita nell'attività aziendale può avvenire:

- nei processi di vendita, prima che i corrispettivi della cessione siano registrati nella contabilità aziendale (skimming);
- nei processi di trasformazione e gestione (furti, utilizzi impropri);
- nei processi di acquisto (beni o servizi non forniti, falsi rimborsi)

Cerchiamo di indicare i più frequenti schemi di frode:

- alterazione di valori che si concretizza in una, appropriazione di denaro prima che la relativa disponibilità sia registrata nei libri contabili della società; questi schemi dunque avvengono principalmente durante le diverse fasi della vendita;
- furto cioè frodi in cui il denaro viene sottratto dopo che la disponibilità è stata iscritta nei libri contabili; in questi casi il denaro viene fisicamente prelevato dalla cassa o dai depositi bancari;
- uscite fraudolente: rientrano in questa categoria tutti gli schemi di frode in cui l'impresa è indotta a sostenere un costo di un bene o servizio inesistente ovvero di un valore superiore al reale. Fra queste è possibile distinguere:
    - pagamenti: l'impresa paga, a fronte di fatture emesse per l'acquisto di beni inesistenti, ovvero fatture con prezzi alterati;
    - stipendi: viene corrisposto lo stipendio a persone inesistenti o che non ha diritto a percepire gli importi pagati (falsi straordinari, false presenze);
    - rimborsi spese: quando vengono erogati rimborsi per spese fittizie o maggiorati rispetto al loro valore effettivo;

- assegni: in questo caso si ha l'alterazione o la falsificazione di assegni aziandali;
- libro cassa: alterazione delle scritture contabili allo scopo di occultare un prelievo fraudolento di circolante.

Falsi documentali

Il falso documentale tipico consiste nell'omettere o nascondere costi e/o passività, attraverso finte o irregolari scritture contabili. Scopo di queste frodi è ingannare i destinatari del bilancio di esercizio (finanziatori, banche, investitori in genere) informazioni non veritiere e corrette in merito all'effettiva consistenza patrimoniale ovvero all'effettiva redditività di un'impresa. Queste frodi vengono normalmente perpetrate dai massimi vertici aziendali, che hanno accesso alla stesura dei documenti di sintesi aziendali.

E' il tipo di frode che ha immediato impatto sul conto economico; infatti l'omissione delle stesse impatta direttamente sui livelli di profitto e di margine operativo lordo. Può anche riguardare semplicemente una non corretta valutazione di alcuni asset.

Gli schemi di frode utilizzati possono essere classificati nelle seguenti categorie:

- falsificazione o alterazione di documenti, registrazioni contabili o transazioni economiche e finanziarie;
- non veritiera o omessa rappresentazione di fatti o eventi , come pure di ogni informazione aziendale utile per la redazione del bilancio di esercizio e dei documenti di sintesi annuali;
- deliberata scorretta applicazione e /o interpretazione dei principi contabili;
- intenzionale o missione o alterata presentazione di tutte le informazioni che accompagnano la presentazione di dati quantitativi;
- utilizzo aggressivo di tecniche contabili per il conseguimento di politiche di bilancio.

Le categorie nelle quali è possibile commettere le frodi in oggetto sono le seguenti:

- vendite fittizie o alterate: transazioni, quantità, prezzi; la realizzazione di tale schema presuppone una opportuna predisposizione di tutti i documenti idonei a simulare le vendite oggetto di frode; a volte tali frodi sono condotto con parti correlate;
- differenze contabili temporali, normalmente fra un esercizio e l'altro; in sostanza registrazioni contabili in tempi non corretti con effetti volutamente anticipati o posticipati sulle risultanze contabili ai fini del bilancio di esercizio; a prima vista tale frode sembrerebbe meno grave di altre, in quanto la registrazione viene solamente spostata di data; la realtà è spesso più complessa, si pensi ad esempio il caso di una vendita condizionata che viene anticipata rispetto al verificarsi della condizione, in tal caso non è detto che la vendita avvenga poi veramente nel successivo periodo; si pensi anche alla possibile presenza di accordi extracontrattuali intenzionalmente messi in atto per modificare la reale natura dell'operazione (cd side letters o side agreements); spesso tali pratiche sono connesse al riconoscimento di premi o bonus al management legati alle vendite o ai risultati economici
- errata valutazione delle attività, si tratta di sopravvalutazioni o sottovalutazioni, ottenute mediante scorrette metodologie di stima o classificazioni non appropriate; premessa a tale fattispecie è il rilevare la crescente complessità delle transazioni aziendali che si è verificata negli ultimi decenni richiedendo pertanto una serie di norma interpretative per la loro contabilizzazione, che sono normalmente contenute, oltre che nella legge, nei principi contabili, sia nazionali che internazionali; rimanenze finali, crediti, attività materiali e soprattutto immateriali, strumenti finanziari, sono le voci che normalmente si prestano a manipolazioni nella loro contabilizzazione; è anche da aggiungere che in molti casi non è semplice distinguere fra applicazione di principi contabili in modo eccessivamente aggressivo e presenza di una vera e propria frode
- alterazione di passività o spese, normalmente mediante una omessa contabilizzazione; valgono per le passività le considerazioni svolte nel precedente punto relativo alle attività; gli scopi perseguiti con tali

pratiche alterano l'equilibrio economico-finanziario, occultando o posticipando debiti o passività e alterano l'equilibrio economico, non registrando o capitalizzando costi; una pratica che è stata rilevata spesso consiste nella non corretta contabilizzazione di fondi rischi o di fondi spese future stanziati in bilancio (cookie jars è il termine usato), infatti la determinazione di tali valori è spesso legata a fattori contingenti o soggettivi di difficile verificabilità e quindi si presta all'autore di frodi;

- scorretta informativa, divulgazione insufficiente o omissione di informazioni sia qualitative che quantitative, a completamento e spiegazione dei valori contabili evidenziati; in questi casi la frode non riguarda gli importi rappresentati in bilancio ovvero l'applicazione di corretti principi contabili ma piuttosto le modalità secondo cui i fatti aziendali sono rappresentati e commentati in bilancio; la casistica di tali frodi è molto ampia, a titolo di esempio rappresentativo si può indicare: (a) la mancata o non corretta rappresentazione di informazioni relative a passività potenziali o possibili rischi futuri; (b) l'omessa segnalazione di fatti significativi avvenuti dopo la chiusura del bilancio, ma prima della sua approvazione; (c) l'occultamento della presenza di operazioni con parti correlate; (d) la non corretta contabilizzazione di eventi straordinari alla normale gestione aziendale;

Segnali di allarme (red flags)

L'esperienza inoltre insegna di tenere alta la guardia quando si presentano una serie di fattori quali:

- transazioni rilevanti in chiusura dell'esercizio;
- transazioni occasionali / straordinarie;
- transazioni non coerenti con lo sviluppo del business aziendale;
- transazioni con prezzi non in linea con il mercato o con transazioni analoghe;
- transazioni realizzate al di fuori dei previsti poteri di delega;
- transazioni in assenza della relativa regolazione finanziaria;
- beneficiari dei pagamenti diversi dalla controparte della transazione;
- pagamenti effettuati su conti esteri, in paesi diversi da quelli della controparte,
- occasionalità di alcune controparti;
- controparti mascherate con fiduciarie;
- lacunosità documentale attestante l'effettività della prestazione resa;
- incongruenze di date a livello documentale,
- lacunosità a livello di tracciabilità dei valori / prezzi a cui sono state realizzate le transazioni;
- eccessivo ricorso a dettagli extracontabili;
- differenze significative di marginalità a livello di offerte / proposte e dati consuntivati;
- ritardi nella trasmissione dei dati;
- informazione generica e vaga a fronte di specifiche richieste;
- informazioni non concordanti fornite da soggetti diversi;
- scostamenti inattesi fra consuntivi e budget;
- scostamenti significativi fra dati consuntivi e trend storici;
- andamento discontinuo e apparentemente inspiegabile di margini economici

- settore in crisi o presenza di contrazione della domanda;
- forte incremento dei costi capitalizzati;
- management della società poco attento alla corretta applicazione dei principi contabili da applicare;
- pressioni del mercato sui risultati aziendali in un ambiente altamente competitivo;
- strumenti di incentivazione del management basati sui risultati di breve periodo.
- crescita del conto acquisti da fornitori in assenza di crescita delle vendite;
- costante crescita dell'utilizzo di fondi per il finanziamento della cassa contante;
- mancata riconciliazione sistematica dei conti utilizzati come contropartita dei pagamenti;
- crescita anomala di acquisti di beni o servizi da determinati fornitori, ovvero in particolari zone territoriali o su richiesta di determinate funzioni;
- mancanza di contratti con fornitori o mancanza di riscontro;
- mancanza della segregazione delle funzioni; cioè il principio usato per ridurre i rischi,di frode o errore, che consiste nel separare, affidando i compiti a persone differenti, le operazioni di registrazione, verifica, autorizzazione, custodia delle attività,periodici controlli di verifica in tutte le transazioni economiche
- mancanza di opportuni controlli interni in grado di monitorare l'operato delle diverse funzioni aziendali; si ricorda che un sistema di controllo interno ha come obiettivo e priorità il governo dell'azienda attraverso l'individuazione, valutazione, monitoraggio, misurazione e mitigazione/gestione di tutti i rischi d'impresa, coerentemente con il livello di rischio scelto/accettato dal vertice aziendale per il perseguimento degli obiettivi aziendali.

L'uso di strumenti societari per i possibili schemi di frode

Premessa

Gli schemi di frode si avvalgono molto speso della creazione di strutture societarie articolate e complesse, appositamente costituite allo scopo. La casistica in proposito è molto estesa, di seguito alcune fattispecie "base" utilizzate:

a) utilizzo di società esterne all'area di consolidamento con l'obiettivo di convogliare le attività di valore dubbio, normalmente attraverso conferimento o cessione di rami d'azienda;
b) utilizzo di società, normalmente offshore, verso le quali far defluire pagamenti di prestazioni fittizie, allo scopo di costituire fondi neri;
c) utilizzo di società esterne all'area proprietaria, allo scopo di trasferire assets per proteggerli nei confronti dei creditori, soprattutto nell'ipotesi che la società madre vada poi verso una procedura concorsuale;
d) l'utilizzo di società appositamente costituite che dopo pochi anni di attività vengono chiuse e messe in liquidazione, allo scopo di attuare frodi fiscali (le cd frodi carosello):
e) utilizzo di società veicolo, ma di fatto riconducibili alla società madre, per occultare fatti e/o illeciti al di fuori del perimetro di consolidamento;
f) utilizzo di società estere al fine di operare operazioni di insider dealing che sarebbero perseguite dalla normativa nazionale;
g) utilizzo di società all'esterno dell'area di consolidamento per realizzare politiche aggressive di manipolazione di dati societari: tranfer price, channel stuffing; con il trasfer price si modificano artificialmente i prezzi con transazioni fra le società del gruppo influendo così su magazzino, vendite e utili; con il channel stuffing si gonfiano vendite e utili inviando ai distributori più merce (considerandola venduta) di quella che essi sono in grado di piazzare presso i clienti;
h) utilizzo di società allo scopo di "money laundering" di fondi provenienti da attività illecite;

i) utilizzo di società terze allo scopo di realizzare operazioni, la cui sostanza è totalmente diversa da quella evidenziata e contabilizzata nella società di origine.

Risultano infine di comune applicazione pratiche volte a favorire l'anonimato dei soggetti imprenditoriali coinvolti in operazioni illecite, che appunto si vogliono mascherare. Esistono al proposito paesi esteri che consento la creazione di appositi centri finanziari offshore. Per centri finanziari offshore si intendono paesi e giurisdizioni caratterizzati dal fatto che attraggono un numero elevato di attività di tipo "non residente". Tale circostanza implica la presenza di talune ovvero di tutte le seguenti caratteristiche:

1. una leggera ovvero inesistente imposizione sui redditi derivati da attività di investimento;
2. l'assenza di ritenute alla fonte;
3. un regime giuridico particolarmente favorevole , in quanto consente una facile e rapida costituzione di società;
4. un regime di supervisione e controllo leggero e flessibile;
5. un semplice e diffuso utilizzo di trust e di altri strumenti societari similari;
6. l'irrilevanza del requisito della presenza fisica per società e istituzioni finanziarie;
7. un elevato livello di segretezza su qualunque informazione relativa al cliente;
8. l'inutilizzabilità di tali regimi e condizioni di favore da parte dei soggetti residenti.

Per un approfondimento dell'utilizzo di strutture societarie, al fine di perpetrare attività illecite, vedasi il documento redatto dall'OCSE dal titolo "Behind the veil. Using corporate entities for illicit purposes" 2001. Di questo documento è stata effettuata una sintesi e traduzione /adattamento alla lingua italiana dalla Fondazione Luca Pacioli "Oltre il velo societario. L'utilizzo di strutture societarie per finalità illecite. Il rapporto dell'OCSE" 2003

Con il termine "abuso societario" si intende la costituzione e l'utilizzazione di uno schema societario al fine di realizzare concretamente operazioni illecite, ovvero tesaurizzare, occultandoli alle autorità, i proventi derivanti da attività illecite.

Tutti gli strumenti esaminati dal rapporto OCSE (società di capitali,e di persone, società fiduciarie, trust e fondazioni) sono talora oggetto di utilizzazione abusiva a scopo di riciclaggio di proventi da reato, corruzione, dissimulazione di attività patrimoniali per frodare i creditori, e di altre attività illecite.

Lo studio giunge alla conclusione che le entità giuridiche che danno luogo ai più frequenti casi di abuso sono quelle che assicurano ai loro beneficiari il grado più elevato di anonimato. Per questo motivo l'OCSE chiede ai governi, e alle altre autorità competenti, di adottare efficienti strumenti legislativi e non, che possano consentire di ottenere le necessarie informazioni sui beneficiari effettivi di tali società, nonché di scambiare tali informazioni a livello transnazionale.

Alcuni paesi consentono alle società costituite nella loro giurisdizione, di avvalersi di strumenti che schermano la proprietà, come ad esempio: (a) i titoli al portatore, (b) i nominee shareholders, cioè l'intestazione fiduciaria delle azioni a terzi, (c) i nominee director, cioè gli amministratori professionali che operano su istruzioni dettagliate dei soci, (d) i corporate director, cioè gli amministratori di società che sono a loro volta società, (e) le flee clause, cioè le clausole di fuga, che consentono alla società di trasferire agevolmente la sede o di mutare agevolmente la legge applicabile, (f) le lettters of wishes, cioè le indicazioni di desiderio tipiche dei trust, con le quali il disponente invita il trustee a compiere certi atti. Alcune giurisdizioni inoltre proteggono l'anonimato, adottando uno stretto segreto bancario, che proibisce a notai, commercialisti, pubblici registri, avvocati, istituzioni finanziarie di rivelare informazioni sull'effettivo beneficiario.

Al fine di combattere efficacemente il fenomeno, occorre che tutti i paesi stabiliscano efficaci misure che consentano alle autorità di ottenere tempestivamente informazioni sui beneficiari economici e sui soggetti di fatto controllanti, scambiando le relative informazioni a livello nazionale e internazionale.

Le tipologie societarie più frequentemente soggette ad abusi

I tipi di strutture societarie più frequentemente utilizzate sono quelle che consentono un elevato livello di anonimato, costituendo così uno schermo fra le operazioni effettuate e i reali esecutori delle stesse e/o i beneficiari delle transazioni. Strutture societarie come le società per azioni, i trust, le fondazioni, e in misura più limitata le società personali, sono infatti spesso utilizzate proprio per massimizzare l'anonimato.

In tutto il mondo le società di capitali e in particolare le società con titoli di tipo azionario, sono le più importanti e diffuse strutture societarie, mediante le quali vengo esercitate le attività imprenditoriali. In molte giurisdizioni le società di capitali si distinguono in Public limited company e in Private limited company. Nelle prime i titoli azionari sono liberamente trasferibili e non vi è limite al numero degli azionisti. Ciò consente alle Public limited company di emettere titoli al portatore e di distribuire i titoli verso il grande pubblico, d'altro lato a queste società vengono richieste normalmente forme di pubblicità delle informazioni finanziarie ed economiche e forme di controllo da parte delle autorità competenti. Nelle seconde è possibile di norma emettere normalmente azioni nominative (sebbene qualche legislazione contenga delle eccezioni; inoltre in molte legislazioni è possibile utilizzare azionisti fiduciari, bypassando di fatto il problema della nominatività. Occorre anche menzionare che le LLC (limited liabilitiy company), le cui azioni sono quotabili in borsa, nelle quali è possibile l'emissione di titoli al portatore. Diversi studi hanno mostrato come sia le Private limited company che le Limited liability company sono state utilizzate a fini fraudolenti, soprattutto in operazioni di riciclaggio.

Inoltre nelle giurisdizioni offshore (cd OFC) esistono le International business corporation (IBC) e le Exemp company (EC), le quali vengono costituite a costi molto bassi e sono in genere esenti quasi completamente da imposte, sia sugli utili che sul capitale. Sia le IBC che le EC sono molto diffuse e consentono di effettuare, oltre alle operazioni lecite, molte specie di operazioni illecite, grazie allo schermo di anonimato e riservatezza di cui sono circondate (titoli al portatore e intestazioni fiduciarie).

Un'altra forma societaria che consente di gestire operazioni illecite sono i trust. I trust sono utilizzate per scopi legittimi nel caso di gestione di patrimoni intestati a minori, a soggetti colpiti da incapacità o più semplicemente da persone inesperte della gestione economico – finanziaria. I trust sono anche utilizzati,

sempre per scopi leciti, al fine di gestire organizzazioni dedite alla beneficienza e più recentemente per gestire operazioni di cartolarizzazione, ovvero piani di incentivazione a favore dei dipendenti.

Nei trust esiste la separazione fra la titolarità giuridica e la spettanza economica dei beni che formano oggetto del trust medesimo. In esse infatti il disponente (settler) trasferisce la proprietà di determinati beni ad un soggetto (persona fisica o giuridica) detto trustee. Quest'ultimo diviene titolare e deve gestire i beni secondo delle regole generali definite nell'atto costitutivo del trust, nell'interesse esclusivo del o dei settler, i quali di norma non sono identificabili, se non tramite il trustee; nella maggior parte delle giurisdizioni infatti non è previsto alcun obbligo di rendere nota l'identità del settler, beneficiario ultimo della gestione dei beni. Per essere sicuri che il trustee esegua le operazioni secondo le disposizioni contenute nell'atto costitutivo, diverse legislazioni danno la possibilità di nominare un guardiano, di solito persona di fiducia del settler, che può revocare in qualunque momento la figura del trustee, nominandone un altro.

I trust possono essere utilizzati in modo improprio per nascondere l'esistenza di attività all'amministrazione finanziaria, ai creditori, all'ex coniuge; i trust costituisco inoltre il mezzo più utilizzato per coloro che cercano di nascondere la propria identità. Essi sono anche utilizzati per operazioni di riciclaggio, ovvero al fine di effettuare operazioni fraudolente. Ricordiamo che, una volta che le attività vengono trasferite ad un trust costituito off shore, di fatto risulta molto difficile, in ogni caso molto costoso, risalire al proprietario dei beni conferiti nel trust.

Un modello di persona giuridica che si avvicina al trust è l'istituto della fondazione, previsto da molti ordinamenti giuridici. In questo caso la proprietà dei beni è della fondazione, non esistono né proprietari né azionisti ed i beni sono destinati al perseguimento di un certo scopo. La fondazione è gestita da un Board of director. In alcune legislazioni lo scopo della fondazione può essere solo di pubblica utilità, mentre in altre (fra cui l'Italia) è ammesso il perseguimento di una finalità privata.

Le probabilità che una fondazione sia utilizzata a fini illeciti aumentano ove sia presente una inadeguata disciplina legislativa, ovvero una inadeguata attività di supervisione e controllo, quando tutto ciò sia anche collegato ad un elevato grado di anonimato, come accade in molte legislazioni OFC.

I meccanismi utilizzati per ottenere l'anonimato

La possibilità di occultare la propria identità è un problema fondamentale per coloro che intendono compiere attività illecite attraverso l'uso di strumenti societari. Oltre ai veicoli societari identificati nel paragrafo precedente, l'anonimato dei beneficiari della frode può essere rafforzato con l'utilizzo di una

miriade di altri strumenti, in particolare si esaminano: le azioni al portatore, gli azionisti fiduciari, gli amministratori fiduciari.

Con le azioni al portatore la persona che ha fisicamente il possesso del certificato deve essere ritenuto il legittimo proprietario dell'azione. Le azioni al portatore non contengono infatti il nome del portatore e non sono soggette a registrazione; le azioni al portatore si trasferiscono attraverso la consegna del relativo certificato, mentre le azioni nominative sono trasferite mediante atti in forma scritta. In certe giurisdizioni e in determinati contesti commerciali, le azioni al portatore sono molto appetibili al fine di perseguire fini illeciti, quali: riciclaggio o evasione fiscale.

Le azioni al portatore sono esposte al pericolo di abusi in quanto sono in grado di occultare effettivamente la proprietà di una società, con il loro elevato grado di anonimato. Infatti le società che emettono titoli al portatore sono di norma esentate dal mantenere un registro delle azioni emesse, riducendo drasticamente le informazioni a disposizione delle autorità inquirenti nel caso di indagine giudiziaria.

Gli azionisti fiduciari (nominee shareholders) sono utilizzati in molte giurisdizioni. Con questa pratica viene di fatto meno l'utilità di registri degli azionisti, in quanto gli azionisti ivi individuati potrebbero non essere gli effettivi proprietari delle partecipazioni. Per ovviare a tale inconveniente alcune legislazioni (in Gran Bretagna il Company act del 1985) prevedono che venga rivelata l'identità dell'effettivo proprietario, pena la sospensione del diritto di voto, ovvero la sospensione del pagamento dei dividendi.

Gli amministratori fiduciari. L'uso di "prestanome" come amministratori sovente ha l'obiettivo di nascondere l'identità degli effettivi beneficiari. Il prestanome infatti figurerà come amministratore in tutti i documenti ufficiali della società, ma eseguirà tutte le incombenze e prenderà le decisioni importanti sulla base di istruzioni ricevute dai beneficiari effettivi della società, che sono di fatto i veri amministratori della società. In alcune legislazioni tale pratica viene limitata con alcuni accorgimenti. In Irlanda ad esempio, viene imposto un limite massimo degli incarichi di amministratore fiduciario, fissato in 25 incarichi. In Gran Bretagna il Companies act del 1985 richiede alla società di comunicare l'identità degli "amministratori-ombra".

Un'ulteriore pratica è quella di consentire a persone giuridiche di ricoprire la carica di amministratore. Molte amministrazioni consentono questa possibilità (fra queste i Paesi bassi e la Gran Bretagna). Gli amministratori persone giuridiche consentono di perpetrare abusi societari, soprattutto nel caso in cui il sistema giuridico di riferimento non riesce ad attribuire responsabilità derivate dalla coperture della carica di amministratore alle persone fisiche finali, alle quali sono in definitiva imputabili eventuali illeciti societari. Si ricorda che in Italia la pratica di nominare amministratori persone giuridiche non è consentita.

In alcune giurisdizioni infine possibile nominare alcuni intermediari professionali (avvocati, notai, etc) nella costituzione e gestione di società. Spesso tali intermediari sono anche utilizzati per accendere conti correnti bancari per conto dei propri clienti, consentendo così ai "beneficial owners" di rimanere anonimi. Avvocati notai e altri professionisti, tenuti al segreto professionale nei confronti della propria clientela, costituiscono intermediari particolarmente ricercati, in quanto con essi è possibile mantenere l'anonimato degli effettivi beneficiari

Le tipologie di attività illecite con l'uso di strumenti societari

Le attività illecite non necessariamente coincidono con le frodi aziendali. Così ad esempio il riciclaggio di denaro, ovvero l'evasione fiscale sono attività illecite, ma non vengono normalmente classificate come frodi. In questo paragrafo si esaminano pertanto tutte le attività illecite, possibili con l'uso degli strumenti societari esaminati nei paragrafi precedenti.

Il riciclaggio di denaro

Il riciclaggio è il processo attraverso il quale i proventi derivanti dall'attività illecita sono sottoposti ad una "trasformazione" o "ripulitura" (laundering), in modo che, alla fine del processo, essi posano apparire come proventi derivanti da attività lecite. In pratica il riciclaggio costituisce l'ultimo stadio della realizzazione di molte attività illecite. Tra i reati retrostanti è possibile identificare, ma l'elenco non è esaustivo: il traffico di droghe, il traffico di esseri umani, , l'estorsione, la corruzione, la concussione., l'insider trading, il traffico di armi, le frodi sulle carte di credito, l'evasione fiscale, il sequestro di persona a scopo di estorsione.

Il riciclaggio comprende tre fasi:

1. Il "placement", attività che consiste nell'introduzione dei proventi illeciti nel sistema finanziario, spesso fuori dal territorio nazionale in cui il reato retrostante è compiuto;
2. Il "layering", attività che consiste nel processo di separazione dei proventi dal fatto-reato che ha dato loro origine realizzato con l'esecuzione di un certo numero di transazioni e attraverso l'uso di vari strumenti, anche societari, normalmente collocati indifferenti giurisdizioni;
3. la "integration", attività che consiste nella reintroduzione del denaro, così riciclato, nel regolare circuito economico.

La necessità di riciclare denaro può provenire da qualunque reato sia in grado di generare profitti. Il riciclaggio è pertanto un reato che interessa tutte le giurisdizioni. I riciclatori comunque preferiscono avvalersi di paesi che, per una serie di ragioni, consentano minori rischi di individuazione. Sistemi caratterizzati da rigide norme sul segreto, da meccanismi di supervisione e controllo superficiali, dalla possibilità di utilizzare strumenti societari protetti da un forte anonimato, naturalmente esercitano sui riciclatori una forte attrazione. Gli schemi di riciclaggio più frequentemente utilizzati prevedono l'utilizzo di società, sia on shore che off shore allo scopo di allungare il più possibile la catena delle transazioni intermedie eseguite allo scopo di "annebbiare" il flusso di denaro illecito. Al fine di attribuire allo schema una maggiore parvenza di legittimità e di ridurre il rischio di individuazione, i riciclatori cercano normalmente di utilizzare società già esistenti che hanno consolidati rapporti con il settore bancario e finanziario di giurisdizioni off shore, attraverso il settore bancario e finanziario nazionale.

Concussione e corruzione

Alcune società possono essere utilizzate in transazioni relative ad attività di concussione o corruzione. Gli amministratori fiduciari ovvero apposite "shell company" possono essere utilizzate nelle transazioni fra coloro che pagano e coloro che ricevono tangenti. Anche le fondazioni e i trust possono essere utilizzati per celare proventi derivanti da attività di corruzione / concussione.

Occultamento di beni ai creditori o altri soggetti

Le società possono anche essere utilizzate allo scopo di occultare beni ai creditori o altri soggetti: il coniuge, gli eredi, l'amministrazione fiscale. Il grado di protezione di certi strumenti societari può efficacemente essere utilizzato per nascondere l'esistenza o la proprietà di beni, al fine di tenerli fuori da concrete possibilità di aggressione da parte di determinarti soggetti. E' anche accaduto che detto meccanismo sia stato utilizzato in casi di bancarotta, in tal caso i fondi sono fuorusciti dalla giurisdizione nazionale, attraverso società di comodo, in altre giurisdizioni in cui era praticamente impossibile stabilire chi fosse il beneficial owner.

L'evasione e gli altri illeciti fiscali

Numerose pratiche fiscali illecite possono essere utilizzate attraverso società e trust collocati in giurisdizioni accomodanti. Ad esempio un contribuente che desideri deviare una parte dei redditi derivanti dall'attività esercitata in una determinata giurisdizione, potrebbe costituire una società in un'altra giurisdizione allo scopo di emettere fatture false nei confronti della prima.. Il contribuente registrerà le

fatture e farà apparire i pagamenti effettuati in relazione alle false fatture come costi sostenuti, riducendo così il proprio reddito imponibile.

Ugualmente il rimpatrio di tali attività può essere effettuato attraverso l'uso di strumenti societari. Inoltre l'uso di azioni al portatore, e di altri strumenti analoghi che garantiscono un elevato grado di anonimato, rende molto difficile la oro corretta individuazione.

Le frodi al mercato e l'aggiramento degli obblighi di informativa
Gli strumenti esaminati nei paragrafi predenti possono anche essere utilizzate per commettere frodi nei confronti del mercato (quale l'insider trading) e per aggirare gli obblighi di informativa previsti dalla legge nazionale. Inoltre le persone fisiche sono in grado di sfruttare il vantaggio loro concesso da determinati soggetti societari, al fine di nascondere le loro capacità di controllo su società quotate, al fine di manipolare il mercato.

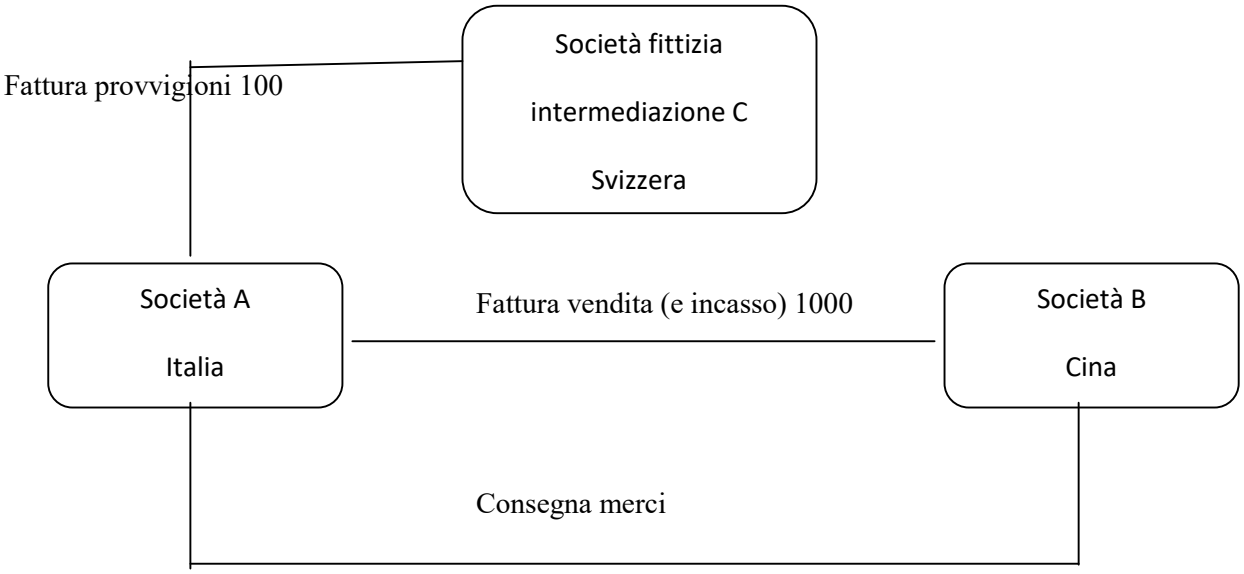
Tematiche particolari ed approfondimenti

In un paragrafo precedente sono stati indicati gli schemi di frode" base", secondo una suddivisione che prende i singoli illeciti separatamente. Gli schemi di frode nelle realtà aziendali sono quasi sempre più complessi e prevedono la mescolanza si diverse tipologie che si combinano fra di loro.

Si ricorda anche che spesso le frodi si avvalgo di strutture societarie create "ad hoc", come ampiamente illustrato in un paragrafo precedente, al fine di realizzare la frode.

Di seguito vengo indicati alcuni schemi di frode che si riscontrano in pratica.

Gli schemi di fatturazione fittizia
Tali schemi si concretizzato nella interposizione, fa due parti commerciali di una società con transazioni fittizie. Si veda il seguente schema:



Nell'operazione indicata nel grafico, la società A italiana, dirotta parte del valore (100) della transazione su un paese estero (Svizzera), attraverso una società fittizia d'intermediazione.

Una variante dell'operazione prevede una fatturazione dalla società italiana A alla società svizzera C dell'importo di (1000 – 100) = 900 e una fatturazione dalla società svizzera C alla società cinese B di 1000. La consegna delle merci avviene naturalmente sempre fra la società italiana A e la società cinese B. L'effetto dell'operazione è sempre il medesimo, cioè si dirotta 100 su una società fittizia C svizzera.

Queste operazioni avvengo normalmente fra società che appartengono allo stesso gruppo con lo scopo di dirottare quote di ricchezza verso società estere.

A volte tuttavia il dirottamento di ricchezza avviene su una società esterna al gruppo (cd società raptor), magari di proprietà del gruppo dirigente del gruppo medesimo. In alcuni casi le società raptor vengo costituite ed utilizzate per effettuare operazioni di maquillage sul bilancio della società madre.

Gli schemi back to back

Con tali operazioni si mettono in atto una serie di operazioni tra più soggetti societari, in modo che la forma del l'operazione appaia diversa dalla effettiva sostanza, che può essere compresa solamente collegando tutte le operazioni della catena fra i vari soggetti coinvolti.

Fra le diverse fattispecie di utilizzo di questo meccanismo, è possibile indicare:

1. il socio persona fisica preferisce ottenere un finanziamento bancario dando a garanzia disponibilità della società, anziché versare direttamente denaro nelle casse della società;
2. società che ricorrono al back to back per far risultare sul proprio bilancio la presenza di disponibilità liquide, mentre tali liquidità , dopo adeguati passaggi societari, sono messe a garanzia di prestiti;
3. soggetti criminali che utilizzano depositi back to back, e successivi prestiti, per ripulire il denaro e reimpiegarlo in attività lecite (money laundering);
4. società finanziarie che concedono prestiti a soggetti terzi, affinché questi pongano in essere operazioni nell'interesse della società finanziaria, senza che questa appaia direttamente (es. acquisto di altre società, acquisto di azioni per una scalata)

Una configurazione diffusa è la frode basata sul cd. loan back. Nel loan back un soggetto criminale, deposita denaro proveniente da attività illecite in un paese con regolamentazione a maglie larghe; tale

denaro è quindi convertito in prestiti a favore di società non off-shore ove sono utilizzati per attività lecite. In tal modo viene spezzato il filo conduttore della provenienza del denaro.

Le frodi carosello

Tali frodi sono ricorrenti in Italia nel campo dell'IVA intracomunitaria.

Con tale frode la società italiana acquista da una società in un altro paese UE (ad esempio Germania) in esenzione da IVA, in quanto gli acquisti intracomunitari n sono esenti. Successivamente vende la medesima merce ad una società italiana, applicando l'IVA. L'IVA non viene mai versata e la società italiana scompare dopo 1 – 2 anni, in modo da evadere la possibilità di eventuali controlli del fisco. Quest'ultima società di fatto non esercita alcuna attività ma produce solo fatture (cd società cartiera)

La frode si chiama carosello, in quanto gli ideatori della frode, dopo aver chiuso la società cartiera, ne aprono successivamente un'altra in un movimento circolare continuo, realizzando così la frode dell'IVA incassata e mai versata.

Con questo meccanismo è possibile all'ultimo operatore avere la merce a prezzi contati dell'IVA e quindi vendere i prodotti a prezzi bassi, turbando così il meccanismo della concorrenza a livello comunitario.

Le frodi con parti correlate

Per la definizione ed una trattazione sulla figura delle parti correlate vedasi il mio articolo: http://www.angelofiori.it/le-operazioni-con-parti-correlate-nelle-pmi/.

Le operazioni con parti correlate, in cui le relazioni di correlazione non sono adeguatamente esplicitate, può originare operazioni fraudolente. Esse sono le più disparate, tuttavia la casistica più frequente riguarda:

a. operazioni di acquisto di beni / servizi a condizioni più onerose di quelle di mercato;
b. operazioni di vendita di beni /servizi a condizioni meno vantaggiose di quelle praticate sul mercato;
c. operazioni di finanziamento, in cui le condizioni del prestito sono sopra o sotto le normali condizioni mercato, a seconda che trattasi di prestiti dati a ricevuti;
d. operazioni di investimento a condizioni anomale rispetto al mercato

Si precisa che meno o più conveniente, rispetto al mercato, può riferirsi a qualunque delle condizioni contrattuali: prezzi, servizi accessori, anticipi e dilazioni di pagamento, qualità dei beni o dei servizi.

Falsificare i bilanci con sistemi di frode

Spesso strutture societarie fittizie vengono messe in atto al solo fine di manipolare i valori di bilancio: per modificare gli utili, per evitare svalutazioni di asset, per nascondere l'effettivo indebitamento del gruppo; queste società a volte sono utilizzate come "discariche contabili" per abbellire i bilanci.

Ciò avviene normalmente con società "terze" al gruppo e quindi non rientranti nell'area di consolidamento, ma di fatto correlate alla capogruppo o ad alcune società del gruppo, ove la correlazione viene adeguatamente nascosta. Spesso si ricorre alle cd Special Purpose Entity, società create appositamente, ma non rientranti nel bilancio consolidato.

Le transazioni interessate sono numerose, fra queste è possibile elencare:

- compravendita fittizia di beni o servizi;
- operazioni societarie straordinari: conferimenti / cessioni di rami azienda al fine di realizzare plusvalenze di dubbia origine;
- prodotti derivati;

- operazioni di finanza strutturata: quali cartolarizzazioni di asset trasferiti a società-veicolo esterne al gruppo;
- operazioni di finanziamento.

Si segnala ancora l'abuso di utilizzare per queste operazioni società collegate, anziché società controllate, al fine di beneficiare dell'applicazione del metodo del patrimonio netto in sede di consolidamento, evitando così il consolidamento integrale di attività e passività.

Lo schema Ponzi

La tecnica prende il nome da Charles Ponzi, un immigrato italiano negli Stati Uniti che divenne famoso per avere applicato una simile truffa su larga scala nei confronti della comunità di immigrati prima e poi in tutta la nazione. Ponzi non fu il primo a usare questa tecnica, ma ebbe tanto successo da legarvi il suo nome. Con la sua truffa coinvolse infatti 40 000 persone e, partendo dalla modica cifra di due dollari, arrivò a raccoglierne oltre 15 milioni. In tempi moderni tale schema è tornato alla ribalta nel 2008, sempre negli USA , con Bernard Madoff

Gli schemi piramidali di tipo Ponzi, concepiti con finalità fraudolente, sfruttano un meccanismo in cui il denaro impegnato dalle prime vittime del sistema deve essere compensato dal denaro versato da nuovi soggetti che entrano a far parte dello schema. Trattasi di un tipo di frode molto antico, in cui il guadagno non deriva da transazioni di prodotti o servizi, ma dal continuo afflusso di nuovi capitali. . Le vittime sono attratte dalla promessa di alti guadagni. In realtà il denaro versano dai nuovi investitori è utilizzato per remunerare chi è al vertice della piramide (cioè i vecchi sottoscrittori).

Piramidi di questo genere sono destinate, prima o poi, ad essere scoperte, è sufficiente infatti il calo della fiducia da parte dei risparmiatori, ovvero dei ritardi nei pagamenti e il continuo afflusso di capitali, rallenta e/o si interrompe. Lo scopo ultimo di chi organizza questi sistemi è di arricchirsi e ad un certo punto di defilarsi, lasciando i risparmiatori con significative perdite in conto capitale.

Due sono i principali argomenti per i quali questo meccanismo di frode è destinato, prima o poi, a fallire:

1. il numero dei potenziali partecipanti è limitato e la relativa piramide non può alimentarsi all'infinito;
2. il profitto non si genera dall'investimento, ma con il conferimento di denaro da parte di un nuovo partecipante; pertanto il profitto di uno si tramuta in una perdita per l'altro.

Contratti di licenza o royalty audit

Come noto esistono contratti di licenza, in base ai quali il titolare di un asset immateriale (marchi, brevetti, etc) concede ad una terza parte, licenziataria del diritto, di sfruttare il diritto medesimo in limiti

contrattualmente previsti, in cambio di un corrispettivo economico. Il contratto di licenza può tuttavia originare frodi e illeciti di varia natura, derivanti da inadempimenti intenzionali di clausole contrattuali da parte del licenziatario.

Vediamone alcuni:

- il licenziatario può alterare il royalty report e i documenti ad esso sottostanti, al fine di dichiarare un importo di royalty inferiore a quello realmente dovuto; questi a loro volta possono concretizzarsi in:
    - omissioni nel royalty report,
    - omissioni contabili a monte del royalty report,
    - errori di calcolo volontari;
- illecito sfruttamento della risorsa licenziata, utilizzata per scopi e/o con modalità che vanno oltre i limiti contrattuali, provocando danni di immagine, oltre ai danni economici; questi a loro volta possono concretizzarsi in:
    - mancato rispetto del listino ufficiale,
    - manipolazioni contabili,
    - applicazione di un non corretto cambio valutario,
    - applicazione di deduzioni errate o non previste ai fini del calcolo del fatturato netto,
    - errori di calcolo volontari;
- errori dovuti ad una non corretta (intenzionale) interpretazione delle clausole contrattuali;
- messa in atto di operazioni commerciali "estranee" all'ambito dell'applicazione del contratto di licenza, ad esempio trasferimento del marchio (art 23 DLgs. 30/2005 Codice della proprietà industriale), ovvero contraffazione del marchio (art 473 e 474 codice penale)

Procedure concorsuali e frodi aziendali

I reati più comuni, che fanno capo al Titolo VI della Legge fallimentare, riguardante le disposizioni penali (artt 216-241 L: F.) riguardano, nello schema di classificazione indicato in un precedente paragrafo, l'appropriazione indebita e il falso documentale. Altre fattispecie, non incluse nel sistema di classificazione, possono riguardare operazioni compiute con grave imprudenza e quello che comportano un aggravamento del dissesto.

Tutti questi reati sono riepilogati nella seguente tabella:

Bancarotta patrimoniale	Fraudolenta	L'imprenditore che "ha distratto, occultato, dissimulato, distrutto o dissipato in tutto o in parte i suoi beni ovvero, allo scopo di recare pregiudizio ai creditori, ha esposto o riconosciuto passività inesistenti" (art. 216 co. 1 num. 1 L.F.). Gli amministratori, i direttori generali, i sindaci,e i liquidatori di società dichiarate fallite, i quali hanno commesso alcuno dei fatti previsti nell'art 216 LF, nonché 1. Hanno cagionato, o concorso a cagionare, il dissesto della società, commettendo alcuno dei fatti previsti dagli artt. 2621, 2622, 2626, 2627, 2628, 2629, 2633 e 2634 del cod. civile; 2. Hanno cagionato con dolo o per effetto di operazioni dolose il fallimento della società (art 223 co. 2num. 1 e 2 L.F.)
	Semplice	L'imprenditore che, fuori dei casi previsti dall'art 216 L.F.: 1. "Ha fatto spese personali o per la famiglia eccessive rispetto alla sua condizione economica; 2. Ha consumato una notevole parte del suo patrimonio in operazioni di pura sorte o manifestamente imprudenti; 3. Ha compiuto operazioni di grave imprudenza per ritardare il

		fallimento; 4. Ha aggravato il proprio dissesto, astenendosi dal richiedere la dichiarazione del proprio fallimento o con altra colpa grave 5. Non ha soddisfatto le obbligazioni assunte in un precedente concordato preventivo o fallimentare." (art. 217 co. 1) Gli amministratori, i direttori generali, i sindaci e i liquidatori di società dichiarate fallite, i quali hanno commesso alcuno dei fatti previsti dall'art. 217 L.F., nonché "hanno concorso a cagionare od aggravare il dissesto della società con inosservanza degli obblighi ad essa imposti dalla legge" (art. 224 co. 1 num. 2 L.F.)
Bancarotta documentale	Fraudolenta	L'imprenditore che " ha sottratto, distrutto o falsificato, in tutto o in parte, con lo scopo di procurare a sé o ad altri un ingiusto profitto o di recare pregiudizio ai creditori, i libri o le altre scritture contabili o li ha tenuti in guisa da non rendere possibile la ricostruzione del patrimonio o del movimento degli affari" (art 216, co. 1 num 2). Gli amministratori, i direttori generali, i sindaci e liquidatori di società dichiarate fallite, i quali hanno commesso alcuno dei fatti previsti dall'art 216 (art. 223, co. 1).
	Semplice	L'imprenditore che " durante i tre anni antecedenti alla dichiarazione di fallimento ovvero all'inizio dell'impresa, se questa ha avuto una minore durata, non ha tenuto i libri o le scritture contabili, prescritti dalla legge o li ha tenuti in maniera irregolare o incompleta" (Art. 217 co. 2). Gli amministratori, i direttori generali, i sindaci e i liquidatori di società dichiarate fallite, i quali hanno commesso alcuni dei fatti previsti dall'art 217 (Art. 224 co. 1)
Bancarotta preferenziale		Il "fallito che, prima o durante la procedura fallimentare, a scopo di favorire, a danno dei creditori, taluno di essi, esegue pagamenti o simula titoli di prelazione" (Art. 216 co. 3). Gli amministratori, i direttori generali, i sindaci e i liquidatori di società dichiarate fallite, i quali hanno commesso alcuno dei fatti previsti nell'art 216 (Art, 223 co. 1)

Può essere anche utile indicare di seguito le tipiche fattispecie, rilevate presso in Tribunale fallimentare di Milano, in merito ai reati fallimentari e societari (artt. 216 e segg. L.F.).

1. Sottrazione e distruzione di attività da parte del fallito, mediante condotte che realizzano il reato di cui all'art 216 L.F.
    a. materiale asportazione di beni o prelevamento del corrispondente valore in numerario,
    b. impiego di tali beni o liquidità per scopi del tutto estranei all'oggetto sociale e, più in generale, alla concreta gestione aziendale;
    c. assunzione a carico dell'impresa di obbligazioni o di oneri estranei alla gestione, quali:
        i. emissione di cambiali e autorizzazione di tratte, prive di effettivo rapporto sottostante
        ii. prestazione di garanzie (concessione di ipoteca, assunzione di fideiussione) per soggetti distinti ed estranei all'azienda, senza la corrispondente instaurazione di un rapporto obbligatorio fra enti e la fallita
        iii. locazione di immobili dell'impresa, della stessa azienda o dei suoi rami, di beni costituenti la più parte del patrimonio sociale a terzi estranei con condizioni contrattuali (in ordine alla durata, al canone, etc) palesemente sbilanciate a favore del locatario.
2. Distruzione o dissipazione consapevole e volontaria di beni del fallito, mediante condotte, che pure realizzano i suddetti reati, quali:
    a. eccesso di prodigalità personale o nell'interesse altrui;

   b. erogazione di spese, anche in ambito aziendale, ma con carattere di totale inutilità, assoluta improduttività, lusso esteriore, non giustificate da alcuna esigenza commerciale.
3. Esecuzione di pagamenti in favore di taluni creditori; la cd bancarotta preferenziale di cui all'art 218 L. F. . Si noti che la fattispecie delittuosa richiede:
   a. che ci sia consapevolezza di versare in stato di insolvenza;
   b. che il fallito non abbia agito in stato di necessita, dovendo ad esempio far fronte ai creditori più aggressivi, dotati di titoli più facilmente azionabili, etc:
   c. che sussista la volontà di favorire taluni creditori i danno degli altri e che, pertanto, il fallito non abbia agito all'interno di un piano di salvataggio dell'impresa imprudente (e, nel caso allora ricorrerebbe il reato di cui all'art 217 1° co. Num. 3), ma non dolosamente preordinato "in odio" ai creditori.
4. L'art. 223 II co. L.F. stabilisce che sono puniti con sanzioni di cui all'art. 216 (e pertanto trattasi di reati di competenza del Tribunale) gli amministratori, i direttori generali, i sindaci e i liquidatori della società:
   a. che hanno commesso alcuno dei reati previsti dagli artt. del cod. civile ivi elencati. Tra essi particolarmente significativo è il delitto di cui all'art 2621 del cod. civile, per il quale sono puniti:
      i. coloro che espongono nei bilanci e nelle altre comunicazioni sociali (leggasi "atti sottoposti a regime di pubblicità societario") circostanze false, in ordine alle condizioni economiche d'impresa;
      ii. coloro che, in mancanza o difformità del bilancio approvato o in base ad un bilancio falso, ripartiscono sotto qualunque forma, utili i non distribuibili.
   b. Che hanno cagionato con dolo, o per effetto di operazioni dolose, il fallimento della società; condotta materiale (legata da un nesso causa-effetto con il dissesto) che potrebbe sostanziarsi:
      i. In ripetute truffe o appropriazioni indebite in danno dei creditori;
      ii. In frode fiscale o in evasione delle imposte, che già sia di per sé penalmente rilevante, ai sensi della L. 7-8-1982 num. 516;
      iii. in qualsiasi altra attività che pur rivestendo i caratteri dell'illecito penale, ma rappresentando comunque una evidente violazione dei doveri derivati dalla legge e/o dal mandato della società, sia stata consapevolmente posta in essere dall'imprenditore per provocare una situazione d'insolvenza,dalla quale sia poi derivato, come logica ed inevitabile conseguenza, il fallimento.
5. I reati di cui al predenti punti 1, 2, 3, 4 sono di competenza del Tribunale; sussistono inoltre altri reati minori, di competenza del Pretore:
   a. bancarotta semplice, di cui all'art 217 L.F.;
   b. ricorso abusivo al credito, di cui all'art. 218 L.F.;
   c. denuncia di crediti inesistenti ed altre inosservanze di cui all'art 220 L.F.:
   d. altre ipotesi previste dal cod. civile ed elencate nell'art 223 II co. num.1.
6. Esistono inoltre una serie di fatti indiziari collegati all'azione penale. Fra questi:
   a. furti, appropriazioni indebite, distrazioni in danno apparente del fallito da parte di dipendenti, dichiarati infedeli, o di terzi estranei alla gestione dell'impresa o di ignoti, specialmente se avvenuti con modalità inconsuete o tali da generare legittimi sospetti o perplessità;
   b. poste di bilancio anomale e indicative di attività sospette, in particolare, perché indicative di possibili artifici e falsificazioni funzionali alla vera e propria distrazione patrimoniale:
      i. le sottofatturazioni o le sopravvalutazioni di magazzino (naturalmente se per valori significativi);
      ii. la mancanza clamorosa di poste di bilancio che avrebbero dovuto senza ombra di dubbio iscritte;

iii. la scoperta, comunque, di una contabilità "in nero", anche se, a dire del fallito, sarebbe stata tenuta ai soli fini di evasione fiscale;
iv. la sproporzione significativa e ingiustificata tra perdite avvenute pre-dissesto e il volume di fatturato;
v. la sproporzione rilevante fra il volume degli affari e gli utili conseguenti, specialmente se ci si trova in presenza di una struttura aziendale che era solida e ben organizzata, di un imprenditore che si era dimostrato capace e attivo, di prodotti e servizi che avevano conquistato un apprezzabile settore di mercato;
vi. la rilevante e altrimenti inspiegabile movimentazione "per cassa" (e, pertanto, in effettivo contante) dei relativi conti del libro giornale o dei libri fiscali;
vii. più in generale, i consistenti flussi in entrata e in uscita, per contanti, emergenti dalla documentazione bancaria;

c. presenza di altra attività imprenditoriale, palese od occulta, intrapresa dal fallito o da persone ad esso legate o coinvolte a vario titolo nel dissesto, specialmente se si tratta di attività simili a quella del fallito, in parte o in tutta coincidenza nei locali, mezzi d'impresa, personale interno, strutture commerciali di vendita o di distribuzione
d. acquisto da parte del fallito, in proprio o con interposta persona, di beni immobili ovvero di beni mobili di rilevante valore, con mezzi economici apparentemente sproporzionati al relativo tenore di vita, con strumenti di pagamento "sospette";
e. rilevazione da parte di soggetti economici estranei all'impresa di consistenti partite di merci in misura significativamente superiore all'ordinario livello di vendite, ovvero di interi rami d'azienda, in tempi, modi e situazioni (prezzo troppo contenuto, vicinanza al fallimento, equivoci rapporti fra impresa venditrice terzo acquirente) genericamente "sospetti".

I reati informatici (cyber crimes) e frodi informatiche

I reati informatici, o "computer crimes", possono essere definiti come il risvolto negativo dello sviluppo tecnologico dell'informatica e della telematica. Lo sviluppo delle tecnologie informatiche ha infatti permesso di disegnare nuovi scenari da qualche decennio a questa parte. Negli ultimi decenni la maggior parte delle attività umane svolte manualmente o attraverso apparecchiature meccaniche, hanno lasciato il passo a più efficienti implementazioni digitali.

Dal connubio informatica-reti telematiche originano inoltre ampie possibilità per la crescita delle aziende e delle comunità in genere. Da ciò si sviluppano attività quali ad esempio l'e-commerce, l'e-government, l'home-banking, il trading online e tante altre attività che consentono di rendere più efficiente la società nel suo complesso, ma al contempo la rendono estremamente net-centrica. Con ciò si vuole sottolineare il fatto che la maggior parte delle attività sociali, lavorative e di svago passano oggi attraverso reti telematiche

L'evoluzione e la diffusione delle tecnologie informatiche e telematiche degli ultimi anni hanno reso il computer, con frequenza sempre maggiore, strumento o oggetto di attività illecita. Di conseguenza, il legislatore è dovuto intervenire, anche sul piano penale, attraverso l'introduzione di nuove fattispecie criminose definite computer crimes o reati informatici.

Per rendere più agevole la comprensione dei provvedimenti normativi previsti dalla legislazione italiana, appare conveniente suddividere in macrocategorie le diverse aree: a) Frodi informatiche; b) Falsificazioni; c) Integrità dei dati e dei sistemi informatici; d) Riservatezza dei dati e delle comunicazioni informatiche.

Frodi informatiche;

Il delitto di Frode informatica, disciplinato dal libro II, titolo XIII, art. 640 ter c.p., è stato introdotto dalla legge n. 547 del 1993. Si parla qui di un reato consistente nel trarre in inganno un elaboratore elettronico, al fine di ricavarne un guadagno economico (per sé o per altri complici), a danno di un soggetto terzo (solitamente il detentore dell'elaboratore elettronico). Si tratta perciò di un'estensione del reato di truffa descritto all'art. 640 c.p.

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 ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante."

Tra i reati che più frequentemente vengono compiuti, e che ricadono, tra gli altri, all'interno della "frode informatica", vi sono le cd. pratiche di phishing e quelle di diffusione di appositi programmi truffaldini, definiti Dialer.p

Il phishing altro non è che un'attività finalizzata ad estorcere dati personali (in prevalenza legati alle carte di credito od ai conti bancari) attraverso una richiesta esplicita al suo legittimo possessore. Il principale metodo per porre in essere il phishing è quello di inviare una mail simile a quella che verrebbe inviata da un regolare istituto (banca, sito d'aste, provider, ecc. e con relativo logo identificativo), nella quale si riportano vari tipi di problemi tecnici (aggiornamento software, scadenza account, ecc.) che motivano l'utente a cliccare sul link riportato nella mail per andare ad aggiornare i propri dati personali. Chiaramente il link non porta al "vero" sito dell'istituzione, ma ad un sito fasullo ed opportunamente creato dall'autore del reato di phishing, che si impossesserà così dei dati inseriti dall'utente.

A tal scopo l'ABI (Associazione Bancaria Italiana) ha stilato una lista di 10 punti chiave nella prevenzione del phishing:

1. Diffidate di qualunque e-mail che vi richieda l'inserimento di dati riservati riguardanti codici di carte di pagamento, chiavi di accesso al servizio di home banking o altre informazioni personali;

2. è possibile riconoscere le truffe via e-mail con qualche piccola attenzione: generalmente queste email non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati; fanno uso di toni intimidatori; non riportano una data di scadenza per l'invio delle informazioni;

3. nel caso in cui riceviate un'e-mail contenente richieste di questo tipo, non rispondete all'e-mail stessa, ma informate subito la vostra banca;

4. non cliccate su link presenti in e-mail sospette, in quanto questi collegamenti potrebbero condurvi a un sito contraffatto, difficilmente distinguibile dall'originale;

5. diffidate inoltre di e-mail con indirizzi web molto lunghi, contenenti caratteri inusuali, quali in particolare @;

6. quando inserite dati riservati in una pagina web, assicuratevi che si tratti di una pagina protetta: queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con “https://” e non con “http://” e nella parte in basso a destra della pagina è presente un lucchetto;

7. diffidate se improvvisamente cambia la modalità con la quale vi viene chiesto di inserire i vostri codici di accesso all'home banking;

8. controllate regolarmente gli estratti conto del vostro conto corrente e delle carte di credito per assicurarvi che le transazioni riportate siano quelle realmente effettuate. In caso contrario, contattate la banca e/o l'emittente della carta di credito;

9. le aziende produttrici dei browser rendono periodicamente disponibili on-line e scaricabili gratuitamente degli aggiornamenti (le cosiddette patch) che incrementano la sicurezza di questi programmi;

10. Internet è un po' come il mondo reale: come non dareste a uno sconosciuto il codice PIN del vostro bancomat, allo stesso modo occorre essere estremamente diffidenti nel consegnare i vostri dati riservati senza essere sicuri dell'identità di chi li sta chiedendo. In caso di dubbio, rivolgetevi alla vostra banca.

Il dialer è un piccolo programma (pochi kilobyte) appositamente scritto per dirottare la connessione Internet dell’ignaro utente verso un altro numero telefonico, spesso di tariffazione internazionale e comunque sempre molto più caro rispetto alla comune chiamata telefonica al numero POP del proprio provider. Attraverso l’utilizzo del dialer il guadagno è multiplo; operatori di telefonia, società produttrici dei dialer, webmaster. E’ però da precisare che l’utente finale (singolo o azienda che sia) viene colpito dal dialer solo nel momento in cui effettivamente lo scarica e lo installa sul proprio computer. Il dialer infatti è un normalissimo programma e come tale deve preventivamente essere installato per poter essere eseguito. Una volta installato sarà il dialer che automaticamente sostituirà il numero ordinario di connessione con un numero a tariffazione maggiorata.

Falsificazioni

La seconda macrocategoria, quella delle falsificazioni, è regolamentata dal Codice Penale attraverso l’art. 491-bis contenuto nel Titolo VII “dei delitti contro la fede pubblica”, Capo III “della falsità in atti”:

art. 491-bis (“Documenti informatici”):

“Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private.

A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli."

l documento informatico acquista effettiva valenza legale con la legge 59/1997 (art. 15 comma 2). Per poter però essere valido un documento deve poter essere autenticato e se ne deve poter attribuire la paternità. A tale scopo interviene la firma digitale, e nel D.P.R. 513/97 art. 1 lettera "b" se ne da una definizione: s'intende "per firma digitale, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici". Con la firma digitale dunque si attesta anche l'integrità ed il non ripudio del documento (quindi si scongiura la falsità materiale), in quanto nella procedura di firma digitale viene generato un particolare codice crittografico derivante dalla "mescolanza" dei dati identificativi del mittente con il contenuto vero e proprio del documento (hash); qualora al momento della ricezione vi sia corrispondenza tra i codici crittografici ottenuti, si avrebbe conferma dell'integrità del documento e dell'autenticità del mittente.

Integrità dei dati e dei sistemi informatici

Il Codice Penale regolamenta poi una terza macrocategoria, che riguarda l'integrità dei dati e dei sistemi informatici, attraverso vari articoli, tra cui il 635-bis del codice penale sul "danneggiamento di sistemi informatici e telematici", contenuto nel Titolo XIII "dei delitti contro il patrimonio", Capo I " dei delitti contro il patrimonio mediante violenza alle cose o alle persone"; art. 635-bis ("Danneggiamento di sistemi informatici e telematici"):

"Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni. Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni."

Aggravante del reato "danneggiamento di sistemi informatici e telematici" è l'art. 420 c.p. "attentato a impianti di pubblica utilità" contenuto nel Titolo V "dei delitti contro l'ordine pubblico". Il Codice Penale interviene anche estendendo l'art. 392 ("Esercizio arbitrario delle proprie ragioni con violenza sulle cose"), ai sistemi informatici (comma 3).

Bisogna infine sottolineare l'art art. 615-quinquies ("Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico"):

"Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a euro 10.329."

Con l'art. 615-quinquies si mira a reprimere la "diffusione di programmi diretti a danneggiare o interrompere un sistema informatico", tutti i programmi cioè rientranti sotto la categoria di malicious software (o malware).

Riservatezza dei dati e delle comunicazioni informatiche

Ultima macrocategoria dei reati informatici è quella inerente la riservatezza dei dati e delle comunicazioni informatiche. In tale ambito il Codice Penale interviene con l'intento di reprimere forme di intrusione nella sfera privata altrui. Il primo provvedimento previsto dalla legge 547/93 in materia di riservatezza dei dati e delle comunicazioni informatiche è quello adottato con l'art. 615-ter del Codice Penale "accesso abusivo ad un sistema informatico o telematico", Titolo XII "dei delitti contro la persona", Capo III "dei delitti contro la libertà individuale", Sezione IV "dei delitti contro la inviolabilità del domicilio".

art. 615-ter ("Accesso abusivo ad un sistema informatico o telematico"):

"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio."

Con questo articolo si vuole tutelare il sistema informatico, inteso qui come vera e propria estensione del domicilio dell'individuo, al fine di proteggerlo da accessi non autorizzati e da permanenza non gradita

Altre disposizioni del Codice Penale in materia di riservatezza dei dati e delle comunicazioni informatiche, le si possono riscontrare nell'art. 615-quater.

art. 615-quater ("Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici"):

"Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.

La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater."

Sempre in riferimento alla macrocategoria sulla riservatezza dei dati e delle comunicazioni informatiche, il Codice Penale individua nell'art. 621 (Titolo XII "dei delitti contro la persona, Sezione V "dei delitti contro la inviolabilità dei segreti") un ulteriore forma di protezione della riservatezza dei propri documenti.

art. 621 ("Rivelazione del contenuto di documenti segreti"):

"Chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto deriva nocumento, con la reclusione fino a tre anni o con la multa da euro 103 a euro 1.032.

Agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi. Il delitto è punibile a querela della persona offesa."

Più nello specifico dell'ambito informatico entrano gli artt. 617-quater, 617-quinquies e 617-sexies (Titolo XII "dei delitti contro la persona", Sezione V "dei delitti contro la inviolabilità dei segreti"), i quali tutelano la riservatezza delle comunicazioni informatiche proprio come nello stesso Codice Penale sono tutelate le comunicazioni per mezzo di apparecchiature telefoniche, telegrafiche ed epistolari attraverso gli artt. 617 e ss. Il fine ultimo di tali articoli è comunque quello espresso attraverso l'art. 616 c.p. sulla "Violazione, sottrazione e soppressione della corrispondenza", sostenuto, tra l'altro, anche dall'art. 15 della Costituzione Italiana sulla libertà e segretezza della corrispondenza e della comunicazione.

La prevenzione delle frodi

La governance del rischio di frode

Il primo aspetto fondamentale è lo sviluppo di un impianto organizzativo atto a gestire il rischio di frode.

Il sistema di gestione può essere sviluppato su una serie di componenti articolate;.le componenti del sistema, sono:

- Impegno del CdA e del top management: 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 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.
- 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 visione del documento che delinea il codice di comportamento accettandone i contenuti.
- Conflitto d'interessi: dovrebbe essere sviluppato un processo aziendale, che faccia emergere e consenta di prevenire e gestire possibili conflitti di interesse di dipendenti, dirigenti e quadri 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) 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.
- Analisi del contesto normativo: tutte le attività ricomprese in un programma di fraud governante: 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, ecc.

La valutazione dei rischi 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 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.

Questo processo diventa più efficace quanto più ampio è il coinvolgimento delle diverse funzioni aziendali in un team dedicato, 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 persone con le necessarie abilità, competenze e conoscenze.

Si potrà quindi avere un gruppo di lavoro (anche virtuale) con figure professionali di: (a) contabilità e finanza; (b) unità di business; (c) risk management; (d) security; (e) legale; (f) internal audit; (g) information technology; (h) human resources; (i) sales; (l) consulenti e specialisti interni e esterni.

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

- 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 costibenefici, da intraprendere per mitigare il rischio di frode.

Al fine di minimizzare la possibilità di accadimento di eventi fraudolenti si dovrebbero sviluppare e implementare dei processi e delle procedure di prevenzione delle frodi e di rilevazione degli eventi sospetti o accaduti.

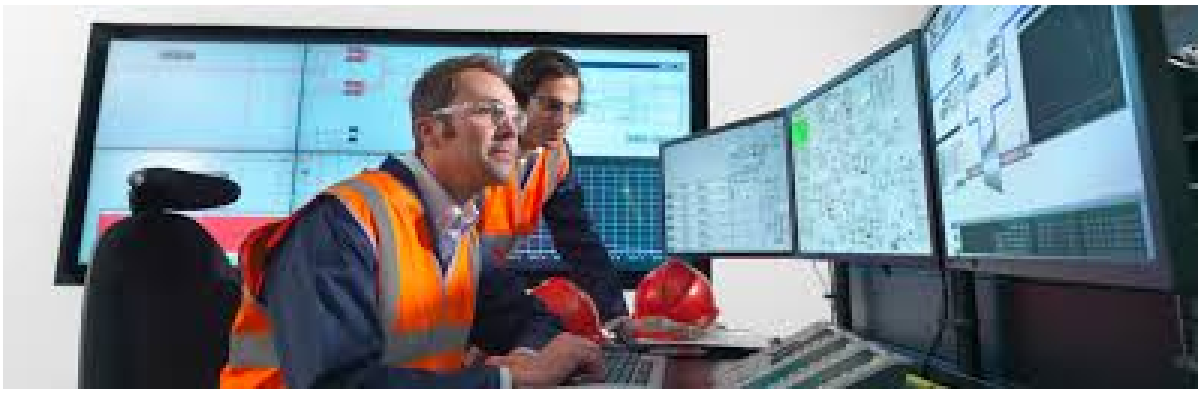
La prevenzione del rischio di frode

La prevenzione del rischio di frode riguarda le procedure, le politiche, la formazione e la comunicazione, la fraud detection invece riguarda sistemi e metodologie di rilevamento di comportamenti sospetti o atti fraudolenti una volta che sono stati compiuti. Naturalmente, l'implementazione di un sistema efficiente di fraud detection agirà come deterrente, operando, quindi, da fattore di prevenzione.

Tra i principali strumenti di controllo per la prevenzione delle frodi i più efficaci si sono rivelati i seguenti:

- Procedure HR: effettuare controlli e investigazioni sul background di un candidato in fase di assunzione, richiedere certificati dei carichi pendenti e del casellario giudiziario, effettuare formazione in funzione antifrode, sviluppare valutazioni della performance e programmi di compensazione che premino la fedeltà e il comportamento corretto dei dipendenti e dei dirigenti.
- Limiti all'autorità: la predisposizione di livelli di autorità commisurati ai livelli di responsabilità aiuta a limitare il rischio di frode. In particolare sistemi autorizzativi di controllo e segregazione di responsabilità sviluppano un ambiente meno soggetto ad attività fraudolente.
- Controlli sulle transazioni con parti terze: instaurazione di sistemi di controllo sulle transazioni con parti terze all'azienda, come a esempio fornitori.

Il controllo e il monitoraggio



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 basate su rilevazione di allerta da sistemi di ethic-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: 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.

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" 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""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"

Le investigazioni

La fase di investigazione si esplica nei seguenti stadi:

- ricezione dell'allerta di frode, rilevato grazie alle procedure per il controllo delle frodi;
- valutazione del fatto alla base dell'allerta: seguendo le procedure stabilite, si dovrebbe valutare l'allerta ricevuto, valutando la tipologia ed entità dell'evento/comportamento segnalato, la/le persone coinvolte, le eventuali conseguenze per l'organizzazione, decidendo come proseguire la fase di indagine;
- valutazione dei costi in relazione all'evento fraudolento e al contesto legale, normativo, etico;
- analisi delle possibili responsabilità aziendali e delle possibili conseguenze economiche, reputazionali e legali a carico dell'azienda;
- conduzione delle investigazioni: è la parte maggiormente specialistica e sensibile, pertanto è opportuno che venga espletata da personale specialista, in conformità alla legislazione in vigore (codice privacy, statuto dei lavoratori, codice penale, ecc.) e con criteri ispirati alle investigazioni criminali. La fase di investigazione comprende la conduzione di interviste (ipotetico attore, persone coinvolte, figure neutrali, ecc.), la raccolta di documenti utili, come a esempio documenti interni (file personali, registro telefonate, registrazioni video-sorveglianza, ecc.) e documenti esterni (registri pubblici, rapporti detective privati), e l'analisi degli elementi raccolti;
- reporting dei risultati: il team di investigazione effettua il reporting alle parti interessate, come a esempio direttori di unità di business, CdA, senior management ingenerale, in base alla tipologia di frode investigata e alle previsioni organizzative e legali;

- azioni correttive: sulla base dei riscontri dell'investigazione, le figure e le funzioni aziendali competenti sviluppano le azioni di risposta al fatto fraudolento, che possono comportare, a titolo meramente esemplificativo: l'adozione di provvedimenti di natura civile (sospensione o risoluzione di contratto), la denuncia per le fattispecie a rilevanza penale, sanzioni amministrative e disciplinari.

È importante notare come vi siano alcuni fattori rilevanti per l'esecuzione delle investigazioni che risaltano, per questa fase del processo di gestione del rischio di frode, il ruolo della funzione di security aziendale:

- fattore tempo: le investigazioni potrebbero dover essere svolte entro tempi stabiliti dalla normativa di riferimento, o dover essere svolte in tempistiche brevi al fine di minimizzare i danni per l'organizzazione;
- notificazione/rapporti con le Forze di polizia: se la fattispecie di frode sotto investigazione ha rilevanza penale, o comunque giuridica, vi sarà il coinvolgimento e l'interfaccia con le Forze di polizia.
- confidenzialità: capacità di mantenere confidenziale il fatto alla base dell'investigazione, l'investigazione stessa e il reporting finale, includendo nel processo solo quelle figure/funzioni che necessitano di essere coinvolte/informate;
- aspetti legali: la attivazione della procedura di investigazione implica aspetti legali rilevanti;
- compliance: le investigazioni, come già indicato, devono essere svolte in conformità alla normativa vigente;
- sicurezza delle prove e degli elementi rilevanti: questi dovrebbero essere protetti e salvaguardati al fine di evitare manomissioni e/o distruzioni;
- obiettività: l'investigazione va svolta con obiettività.

Le funzioni aziendali coinvolte

Si sottolinea come la frode rappresenti, in ambito aziendale, un rischio trasversale e profondamente eterogeneo. Può essere compiuto internamente o esternamente all'azienda, e quindi comportare, a esempio, la fuga di notizie commerciali sensibili, infedeltà aziendale attraverso l'accaparramento di risorse economiche dell'azienda, e così via. Ancora, la frode può coinvolgere risorse, comportando perdite, economiche e finanziarie, o, come osservato negli ultimi anni, essere perpetrata attraverso frodi informatiche, che puntano alla distruzione/sottrazione di dati aziendali (protezione dei dati sensibili e personali, ex codice della privacy).

In quanto tale, il rischio di frode coinvolge molteplici funzioni aziendali, che hanno un impatto e/o effetti su di esso, tra le quali: (a) internal audit; (b) security; (c) funzione di enterprise risk management; (d) finanza; (e) contabilità; (f) ufficio legale; (g) unità operative e di business; (h) ICT; (i) Human resources.

Un programma di gestione delle frodi si pone quindi in maniera trasversale su tutte le funzioni aziendali. Tale programma deve prevedere un adeguamento del modello organizzativo aziendale esistente, ampliandone i contenuti, senza creare sovrapposizioni di competenza o fenomeni di ridondanza in termini di policy e codici aziendali. È quindi necessario prevedere un coordinamento organizzativo che sappia relazionarsi funzionalmente (e non necessariamente gerarchicamente) con tutte le funzioni aziendali garantendo il funzionamento di uno specifico piano di comunicazione (comprensivo della condivisione di obiettivi e informazioni), di controllo e monitoraggio continuo.

Questa risorsa (o funzione organizzativa) deve avere un'elevata sensibilità verso le esigenze di protezione degli asset aziendali e profonde competenze ed esperienze nella gestione dei rischi. Inoltre al responsabile di un programma di fraud governance deve essere garantito il pieno committment da parte del top management e un adeguato budget economico. Pertanto, il processo può essere affidato: (a) alla funzione di security, (b) all'internal audit, (c) alla funzione legale, (d) al risk management, oppure ancora essere suddiviso in aree di responsabilità fra di esse. La necessità che si pone è, inoltre, di sviluppare un sistema di

gestione antifrode che riesca a essere omogeneo e sinergico, facendo cooperare tutte le funzioni aziendali coinvolte attraverso una chiara suddivisione delle aree di responsabilità.

I metodi investigativi

Premessa, attivazione del processo

E' evidente che quando esistono segnali di possibili frodi aziendali, la tempistica costituisca un fattore essenziale, ogni atteggiamento dilatorio è infatti da evitare. Nel contempo è necessario che:

- esistano processi consequenziali e procedure idonee ad evidenziare problemi legati possibili frodo aziendali;
- quanto emerso sia giudicato e valutato da soggetti competenti in grado di apprezzarne la potenziale entità e gravità

Nel processo di valutazione occorre rispondere alle seguenti domande, al fine di giungere ad una decisione di iniziare un'azione investigativa in modo tempestivo e consapevole:

- Come è avvenuta la segnalazione?
- Si tratta di elementi che possono impattare su singoli eventi, oppure rientrano nel quadro di operazioni più articolate e continuative?
- Le relative attività sono ancora in corso, oppure si riferiscono a eventi conclusi?
- Quali sono le aree e i processi coinvolti?
- Quali e quanti soggetti potrebbero essere a conoscenza ed eventualmente coinvolti?
- Esistono precedenti in azienda, ovvero si è a conoscenza di eventi similari in altre imprese dello stesso settore, area geografica, dimensione, etc?
- Quale potrebbe essere l'impatto sia economico che reputazionale per l'organizzazione?
- Si potrebbe configurare la violazione di norme, regolamenti, principi?

Ulteriore importante elemento necessario è la riservatezza. Si deve infatti . (a) evitare che gli autori della possibile frode siano messi in allarme e attivino contromisure di contrasto e occultamento; (b) favorire nel contempo un regolare flusso della normale attività aziendale.

La scelta dell'attore che si deve occupare delle necessarie indagini può cadere sia su un soggetto esterno, esperto nel settore delle frodi aziendali, sia un soggetto interno ad un adeguato livello di competenze e dotato di sufficiente autorità.

Comunicazione

Una corretta comunicazione fra i diversi attori coinvolti è elemento primario per il regolare flusso della attività investigativa ed evita l'insorgere di incomprensioni, fraintendimenti che possono sorgere e che condizionerebbero l'esito dell'attività investigativa.

L'attività del soggetto incaricato, se esterno, deve essere inquadrata e regolamentata in una lettera d'incarico. Se interno deve comunque essere inquadrata i un contesto di istruzioni emesse, preferibilmente informa scritta.

I punti principali che inquadrano, definisco e circoscrivono l'incarico sono i seguenti:

- Le ragioni dell'attività richiesta, cioè gli indizi e le presunzioni circa la presenza di fattispecie illecite o fraudolente.
- Le modalità di svolgimento del lavoro: le tipologie di analisi che dovranno essere effettuate, le verifiche che andranno compiute, etc.
- L'oggetto dell'incarico, precisando i confini che lo delimitano.
- Le eventuali limitazioni.
- Lo scopo perseguito: ad esempio a supporto di azioni legali.
- Il tempo previsto per portare a termine il lavoro.
- Il personale incaricato di svolgere le indagini e le verifiche da effettuare.
- Il referente cui riportare le varie fasi dell'attività svolta
- La forma in cui saranno esplicatati i risultati del lavoro sviluppato.
- I limiti e le eventuali prescrizioni sulle conclusioni raggiunte

Attività preliminari

Ci sono diverse attività preliminari allo svolgimento dell'incarico vero e proprio.

Innanzitutto è necessario fare chiarezza circa l'esatto tenore della problematica da affrontare, anche alo scopo di tracciare un primo approssimativo quadro dei soggetti coinvolti e delle documentazione da esaminare. Occorre inoltre mettere a fuoco l'orizzonte temporale entro il quale si opera. Anche gli aspetti logistici hanno la loro importanza: l'estensione dell'indagine in termini spaziali, ma tenendo anche conto degli aspetti linguistici e culturali. Non vanno infine trascurati gli aspetti legislativi e regolamentari.

E' necessario inoltre che il soggetto incaricato dell'indagine, interno e esterno che sia, conosca l'organigramma aziendale e si sappia muovere all'interno di esso.

La scelta del personale da dedicare alle indagini è prioritaria e da essa può dipendere l'esito delle indagini stesse.

Importante è inoltre inquadrare il perimetro e il trattamento e la efficace conservazione di tutta la messe di documentazione in possesso all'azienda che possono essere utili all'indagine.

Avvio delle indagini

Giova sottolineare che l'esistenza di molteplici fatti e documenti attestanti la presenza di un atto non regolare, non rappresentano, di per sé, una prova sufficiente a dimostrare l'atto criminoso. Bisogna infatti dimostrare l'intenzionalità:. E infatti proprio l'intenzionalità a rappresentare la linea che separa l'errore dalla frode

Al fine di dimostrare la precisa volontà di un individuo a perpetrare una frode è necessario disporre di elementi probativi in merito al fatto che questi abbia: (a) commesso un particolare atto; (b) occultato il medesimo; (c) tratto da questo un beneficio. Ora i tre elementi debbono coesistere perché si abbia la

ragionevole certezza che siamo in presenza di una frode. Infatti, ad s esempio il fatto che coesistano il punto (a) e il punto (b), potrebbe semplicemente dire che siamo in presenza di un individuo che abbia compiuto un'azione erronea o incauta e che tenti occultarla con qualche strattagemma

Bisogna anche sottolineare che l'incaricato all'indagine, interno o esterno che si, deve attestare la realtà in base alle prove raccolte, senza dare giudizi di merito sulle persone o sulle procedure.

Può essere utile in questa sede richiamare la differenza fra dato e informazione. Il dato è un elemento o una misura di un fenomeno percepibile senza alcuna mediazione di tipo logico, qualitativo o cognitivo, Si tratta dunque di un elemento grezzo. L'inserimento del dato nell'ambito di un contesto logico, il relazionarlo con altri, il completarlo o elaborarlo, contribuisce a trasformare il dato in una informazione fruibile per un processo cognitivo. Compito dell'incaricato alle indagini per frodi aziendali è pertanto trasformare, attraverso una intelligente operazione di collegamento e contestualizzazione, i dati ottenuti in informazioni utili ai fini dell'indagine.

C'è un ulteriore aspetto che è d'obbligo sottolineare. Il soggetto incaricato di svolgere l'indagine per appurare le frodi , parte quasi sempre da ipotesi , che condizionano il lavoro che deve svolgere. Queste iniziali ipotesi a volte si basano sugli scarsi indizi iniziali avuti: spesso limitati a denunce, sospetti o a indicazioni del responsabile aziendale che da il via alle indagini. La formulazione delle ipotesi è pertanto il momento fondamentale di ogni attività investigativa, momento al quale va dedicata tutta la competenza e perizia necessarie. In che modo dunque il soggetto incaricato delle indagini può formulare efficaci ipotesi investigative, senza incorrere in errori di metodo.

Gli approcci strategici per affrontare la sopracitata problematica, si basano sostanzialmente su tre diversi criteri (o approcci) di base.

<u>Approccio situazionale.</u>

Si tratta dell'approccio più comune e anche quello che istintivamente ciascuno di noi è portato a seguire. Sulla base degli elementi di cui si dispone, il soggetto addetto alle indagini cerca di farsi un'idea del caso che sta affrontando, formulando una prima ipotesi. Egli pertanto esaminerà le incongruenze, , le anomalie (di tipo contabile, organizzativo, caratteriale, etc), comportamenti individuali, le dichiarazioni (denunce, segnalazioni, delazioni, etc) e ogni altra notizia che ritiene utile allo scopo

<u>Approccio teorico-teorico</u>

Questo approccio si fonda sullo sfruttamento della generalizzazioni effettuate da studiosi, ricercatori e professionisti esperti. E' bene tuttavia tenere presente che l'utilizzo acritico di un tale approccio potrebbe fuorviare l'utilizzatore nella sua azione investigativa, portandolo a trascurare informazioni rilevanti e conducendolo inconsapevolmente a dare prevalenza alle generalità del modello, rispetto alle peculiarità delle fattispecie da esaminare.

Per questo motivo è bene abbinare all'approccio teorico, il confronto con precedenti storici dalle caratteristiche simili. Tale bagaglio di conoscenze può provenire sia dall'esperienza del responsabile incaricato delle verifiche sia dalla lettura di testi, case histories, articoli, saggi etc

<u>Approccio induttivo</u>

Questo approccio prevede che si proceda direttamente allo svolgimento dell'incarico senza preoccuparsi di collocare i dati disponibili all'interno di precostruiti schemi logici. Si confida infatti nel presupposto che , facendo affidamento sulle grandi potenzialità dei nuovi sistemi di elaborazione dati, sia possibile risalire

alle presenza di fattori ed elementi logici di correlazione fra i medesimi e da ciò pervenire induttivamente nella formulazione di ipotesi da cui partire.

Questo approccio risulta molto dispendioso e può richiedere tempi lunghi nonché competenze specialistiche e software dedicati

Evidenze

Per evidenza si intendono, in questo contesto, le informazioni che forniscono la diretta e immediata percezione di un accadimento. Giova anche ricordare in questa sede la differenza fra dato e informazione: il dato è elemento o misura di un fenomeno percepibile senza alcuna mediazione di tipo logico, o cognitivo. Un dato diviene informazione a seguito della sua contestualizzazione, cioè il suo inserimento nel suo contesto logico.

Colui che si occupa delle indagini raccoglie e inserisce in un quadro logico-contestuale le evidenze acquisite, a riprova di una ipotesi investigativa formulata.

Le evidenze possono avere differente natura e quindi essere la documentazione su supporto cartaceo, da dati su sopporto elettronico, da informazioni orali. Queste possono poi essere sia di fonte interna che di fonte esterna rispetto all'azienda investigata.

Le informazioni, per essere evidenze ai fini dell'indagine, devono possedere le seguenti tre caratteristiche:

1. Devono avere rilevanza rispetto al caso. Esse devono dimostrare in forma chiara, precisa e non ambigua l'esistenza di un fatto, un'azione, una relazione, una transazione, un accorso.
2. Devono essere valide. In altri termini occorre accertare anche la completezza dell'informazione (con riferimento a importi, quantità, numerazione, date, firme, etc), e la sua autenticità tanto nel contenuto che nella fonte di provenienza.
3. Devo essere sufficienti. L'informazione deve essere infatti direttamente collegabile all'obiettivo perseguito nell'indagine.

Conclusione indagini e report finale

Le conclusioni finali dovrebbero essere in grado di fornire adeguata risposta ai seguenti interrogativi: (a) quale attività è stata compiuta, (b) chi l'ha realizzata, (c) con quali modalità si è concretizzata, (d) dove ha avuto luogo, (e) quando è avvenuto il fatto, (f) per quali ragioni.

Si precisa peraltro che la relazione finale non sempre perviene a conclusioni tali da fornire le prove che una determinata azione fraudolenta sia avvenuta ovvero non sia avvenuta. Essa si limita infatti a fornire l'esito delle ricerche compiute e le conclusioni cui si è pervenuti sulla base delle evidenze raccolte.

In sintesi il rapporto deve contenere i seguenti aspetti minimali:

I. Identificazione del committente e oggetto dell'incarico, eventualmente riprendendo gli argomenti già sviluppati nella lettera d'incarico.
II. Procedure di verifica svolte e limitazioni incontrate nel corso del lavoro, con eventuale riferimento a standard professionali.
III. Risultanze delle analisi svolte. Questa rappresenta la parte principale del report. La stesura deve essere particolareggiata e precisa, facendo ricorso ad ogni strumento, anche di tipo grafico, per mostrare correlazioni, legami o flussi in modo chiaro e diretto.
IV. Sintesi conclusive nei casi particolarmente complessi ed estesi. Questa parte va tuttavia vagliata attentamente per il rischio di omissione di particolari importanti o per il rischio di pervenire a conclusione non sufficientemente supportate dalle evidenze disponibili
V. Elenco degli allegati: Gli allegati devono infatti fornire un elenco preciso di tutte le evidenze riscontrate
VI. Firma di chi ha condotto l'indagine e ne ha avuto la responsabilità

Bibliografia

- Frodi aziendali – Giuseppe Pogliani, Nicola Pecchiari, Marco Mariani – EGEA 2012
- Global economic crime survey 2016" di Price Waterhouse & Coopers
- Ernst & Young_14th_Global_Fraud_Survey – 2016
- ACFE-(association of certified fraud examiners) 2016-"Report-to-the-nations 2016"
- Fondazione Luca Pacioli "Oltre il velo societario. L'utilizzo di strutture societarie per finalità illecite. Il rapporto dell'OCSE"