



BANCA D'ITALIA  
EUROSISTEMA

## COMUNICAZIONE UIF DEL 5 FEBBRAIO 2010.

### SCHEMI RAPPRESENTATIVI DI COMPORAMENTI ANOMALI AI SENSI DELL'ART. 6, CO. 7, LETT. B) DEL D.LGS 231/2007 - FRODI INFORMATICHE.

L'utilizzo sempre più diffuso di servizi *on-line* in ambito finanziario e commerciale è stato nel tempo accompagnato dal moltiplicarsi di frodi informatiche in diverse forme e modalità.

All'origine di tali attività illecite vi è la capacità da parte di organizzazioni criminali di entrare in possesso delle credenziali di accesso ai servizi *on-line* di clienti inconsapevoli ovvero di acquisire altre informazioni utili, attraverso modalità diverse (invio massivo di messaggi di posta elettronica, costruzione di falsi siti Internet che riproducono quelli degli intermediari bancari, installazione via internet di software "spia" sui computer dei titolari di rapporti *on-line*, etc.).

Il progressivo diffondersi di servizi e strumenti di pagamento alternativi favorisce il perfezionamento delle frodi informatiche, con particolare riferimento alle operazioni di *phishing*<sup>1</sup>.

In relazione a quanto precede, gli intermediari che offrono alla propria clientela la possibilità di operare *on-line* sono invitati ad attivare efficaci sistemi di monitoraggio e prevenzione dell'operatività effettuata al fine di prevenire tali attività illecite.

Per agevolare tali valutazioni, si fornisce - ai sensi dell'art. 6, comma 7, lettera b) del decreto legislativo n. 231 del 2007 - l'allegato schema operativo, elaborato sulla base dell'analisi finanziaria effettuata su operazioni segnalate per il sospetto di condotte illecite.

Lo schema descrive possibili anomalie che potrebbero essere riconducibili a fenomeni criminali. Nella valutazione assumono centralità le informazioni riguardanti l'origine e la destinazione dei fondi e le effettive finalità economico - finanziarie sottostanti alle transazioni.

Si ricorda che ai fini del corretto adempimento degli obblighi di segnalazione di operazioni sospette, da un lato, non è

---

<sup>1</sup>Il fenomeno si articola generalmente in tre fasi: acquisizione da parte del phisher, con modalità fraudolente, delle informazioni riservate inerenti i dati identificativi e i codici di accesso dell'utente inconsapevole; accredito di singoli bonifici d'importo limitato su conti correnti intestati a persone più o meno consapevolmente coinvolte nella frode; prelievo e trasmissione dei fondi, decurtati della "commissione" promessa a tali soggetti, all'organizzazione criminale, specie su terminali esteri, soprattutto tramite il circuito dei money-transfer. E' stato rilevato che i bonifici fraudolenti possono essere indirizzati a favore di carte prepagate ricaricabili; con ogni probabilità le stesse sono state consegnate dai richiedenti, in uno col relativo codice, all'organizzazione criminale.

necessario che ricorrano contemporaneamente tutti i comportamenti descritti negli schemi operativi; dall'altro, la mera ricorrenza di singoli comportamenti descritti negli schemi non è motivo di per sé sufficiente per procedere alla segnalazione.

Qualora emergano operazioni sospette riconducibili ai fenomeni descritti, è necessario segnalarle con la massima tempestività.

Si raccomanda di procedere, nell'ambito della propria autonomia organizzativa e con le modalità ritenute più idonee, a diffondere le presenti indicazioni operative fra il personale incaricato della valutazione delle operazioni sospette.

**Operatività connessa con le frodi informatiche**

- apertura di conti *on-line* (in particolare da parte di soggetti residenti all'estero) che, dopo un periodo iniziale di inattività, risultano alimentati con bonifici *on-line* di consistente importo ovvero tramite molteplici bonifici *on-line* per importi inferiori alla soglia di registrazione disposti nel medesimo giorno o comunque in un breve lasso di tempo;
- accrediti di bonifici *on-line* disposti da conti intestati a numerose persone fisiche ovvero a persone giuridiche non ricollegabili al profilo economico/finanziario o all'attività del destinatario;
- successivi immediati prelievi in contante ovvero trasferimenti di fondi tramite bonifico presso altro intermediario o presso più intermediari, specie se all'estero e verso Paesi o territori ad alto rischio di riciclaggio o di finanziamento del terrorismo;
- utilizzo di rapporti di recente apertura unicamente per l'esecuzione di operazioni della specie;
- attivazione in un arco temporale molto ristretto di una o più carte prepagate da parte di soggetti esteri;
- ricariche di carte prepagate tramite versamenti di contanti o con bonifici *on-line* di modesto ammontare, seguite, pressoché immediatamente e per l'intero importo della carta, da prelievi di contante effettuati anche all'estero;
- trasferimento all'estero attraverso *money transfer* di somme di importo complessivo rilevante, con più operazioni disposte in ristretti archi temporali, a favore di uno stesso nominativo da parte di una pluralità di soggetti, specie se non riconducibili ai Paesi di destinazione dei trasferimenti;
- operatività complessiva, di consistente importo, concentrata per lo più nei periodi feriali e/o a ridosso dei fine settimana.