Il Focus

Frodi su conti online — la banca è responsabile

n. 64 del 19 ottobre 2016

a cura di Studio Associato Bortolazzi & Borghesani partner BHR Group

BHR Group
Via Antonio Canova, 7
37050 – Oppeano (VR)

Telefono +39 045/8538155
Fax +39 045/7130963
eMail info@bhrgroup.net

Le frodi tramite furto di identità sono numerose, soprattutto in ambito Internet Banking. Per fortuna esistono gli strumenti legali per difendersi. Anche una recente pronuncia del Tribunale di Roma ha confermato l'orientamento indicato dalla Cassazione condannando due banche online alla restituzione del maltolto e al pagamento di 20.000 per danni, in favore di un correntista frodato.
Queste sentenze, finalmente, hanno dato spazio applicativo alle norme – quali il Codice Privacy e il decreto legislativo n. 10/11 sui sistemi di pagamento online – che impongono alle aziende (in particolare gli istituti bancari) di predisporre adeguati sistemi di sicurezza informatica e dimostrare, in caso di illeciti, di non avere alcuna responsabilità. Dunque, il correntista può limitarsi alla denuncia tempestiva dell'illegittima e non riconosciuta operazione bancaria.

FRODE SU CONTI ONLINE

Nel caso oggetto di sentenza, si era verificato un accesso illecito nel conto corrente online, la clonazione della carta di identità del titolare e il furto del numero di cellulare del correntista: con una semplice autocertificazione di smarrimento, si otteneva una SIM Card sostitutiva e si apriva a nome della vittima un conto online presso altro istituto bancario (SIM Swap Fraud). Da qui: cambio di password del primo conto, spostamento del deposito sul secondo e successiva redistribuzione del denaro verso ulteriori conti. Intera operazione svolta in pochi giorni.

RESPONSABILITA' DELLE BANCHE

Il correntista frodato ha disconosciuto tempestivamente le operazioni illecite compiute sul proprio conto, denunciando l'evento e il danno. Le due banche, invece, non sono stati in grado di provare che i loro sistemi di sicurezza fossero efficaci ed i processi conformi alla legge sulla privacy D.lgs. 196/2003, al decreto legislativo sui servizi di pagamento nel mercato interno D.lgs 11/10 e al codice civile art. 2050 attività pericolose e 2049 responsabilità dei padroni e committenti. Anzi, nel giudizio è emerso il contrario.
La prima banca ha rivelato un sistema informatico e protocolli di sicurezza deboli, nonostante i documenti Bankitalia che impongono efficaci misure di sicurezza. I problemi alla SIM dell'utente dovrebbero essere rilevati in automatico dal sistema con sospensione cautelativa dei movimenti in difetto di un assenso del titolare del conto.
La seconda banca si è dimostrata inidonea nell'applicazione delle norme in materia di antiriciclaggio (che impone specifiche procedure di riconoscimento personale soprattutto per i

RESPONSABILITA' DELLE AZIENDE

conti online), soprattutto considerando che il documento di riconoscimento utilizzato presentava delle irregolarità macroscopiche.
Dunque, la frode di per sé è operazione possibile se esistono debolezze informatiche e procedurali a carico degli istituti di credito, i quali avrebbero potuto evitare e bloccare la frode applicando le leggi (oltre a quella sull'antiriciclaggio) e allineandosi alle migliori pratiche di sicurezza nell'ambito bancario.

Sicuramente le banche sono gli obiettivi più frequenti di questi attacchi, ma l'intrusione informatica potrebbe avere come obiettivo anche informazioni aziendali anziché denaro.
Gli strumenti tecnici e normativi per difendersi esistono: ecco perché soltanto dimostrando di averli applicati sarà possibile risultare esenti da responsabilità ed evitare il risarcimento dei danni. Il rispetto di tale impostazione diventerà imprescindibile quando il nuovo Regolamento Privacy diventerà operativo nel 2018. La nuova legge sui dati personali, infatti, ha codificato il principio dell'accountability cioè della responsabilità e della prova in capo al titolare del trattamento.

VERONICA SMIRNOFF