
Phishing, sicurezza home banking, carte di credito: i primi pronunciamenti dell'Arbitro Bancario Finanziario (ABF)

By Massimo D'Alesio

Published: 30/04/2010 - 10:36

L'Arbitro Bancario Finanziario ([ABF](#)) è il nuovo **organismo indipendente e imparziale** per la risoluzione stragiudiziale delle controversie tra banca e clientela previsto dall'articolo 128-bis del Testo unico bancario (TUB), introdotto dalla legge sul risparmio (legge n. 262/2005), e reso operativo grazie alle disposizioni di Banca d'Italia del 18 giugno 2009, pubblicate Gazzetta Ufficiale, Serie Generale, del 24 giugno 2009.

L'Arbitro Bancario Finanziario è articolato sul territorio nazionale in tre Collegi: uno a Milano, uno a Roma e uno a Napoli.

Dal 28 aprile 2010 le decisioni dell'ABF vengono rese note sul proprio sito web; proprio dalla lettura di quanto già pubblicato emergono indicazioni di particolare rilievo per quanto riguarda il phishing, la clonazioni di carte di credito e bancomat, la sicurezza ed affidabilità dei sistemi informativi bancari; la maggior parte delle decisioni assunte sono infatti nettamente a favore dei consumatori (anche se con qualche distinguo tra i vari collegi); va rimarcato inoltre che i reclami analizzati e su cui si è deliberato si riferiscono al quadro normativo antecedente al primo marzo 2010, data di entrata in vigore della **Direttiva sui Sistemi di pagamento** (PSD - *Payment Services Directive*); direttiva che intende favorire lo sviluppo di strumenti di pagamento evoluti, alternativi al contante, aumentando le garanzie per il cliente in caso di uso fraudolento degli strumenti stessi.

Il quadro appare chiaro: nell'ambito dei servizi sui sistemi di pagamento le banche devono quindi adottare processi, strumenti e sistemi di controllo non solo adeguati ma **"avanzati"**; in caso di perdite dovute a truffe elettroniche (ad esempio il phishing) **la direttiva infatti "prende le parti" dei consumatori**, ragion per cui la banca deve essere in grado di dimostrare non solo di aver adottato **"tutte le precauzioni"**, ma anche di aver istituito **"presidi di sicurezza adeguati allo scopo e resi accessibili dall'evoluzione scientifica e tecnologica"**.

Casi di phishing

La decisione **n. 46/10** (qui in [pdf](#)), resa dal Collegio di Milano dell'ABF nella seduta del 21 gennaio 2010, relativo ad un caso di phishing ha ravvisato un concorso di colpa tra la banca, per violazione dell'obbligo di diligente custodia dei patrimoni dei clienti, ed il correntista, per incauta custodia dei codici di accesso al servizio.

Ancora più clamorosa la **decisione n. 33/10** (qui in [pdf](#)) resa dal Collegio di Roma dell'ABF nella seduta del 12 gennaio 2010. Anche qui un caso di phishing in cui il correntista ammette candidamente di aver risposto ad una mail all'apparenza proveniente dalla banca nella quale gli veniva richiesto di digitare i codici di accesso e dispositivi relativi al proprio conto corrente on line; ebbene l'ABF ha deciso che il cliente va rimborsato del 75% delle perdite subite in quanto **"il corretto adempimento dell'obbligo di diligenza presuppone l'adozione di tutte le precauzioni e l'istituzione di tutti i presidi di sicurezza adeguati allo scopo e resi accessibili dall'evoluzione scientifica e tecnologica"**. In pratica l'ABF ha ravvisato una colpa nel comportamento della banca perché non ha fornito alla clientela dispositivi automatici per la generazione di password (token, chiavette, digipass...) ravvisando in ciò una violazione dell'obbligo di diligenza, in quanto manca l'adeguamento dei presidi **"agli ultimi ritrovati ed alle più recenti acquisizioni della scienza e della tecnologia"**.

Furto di Bancomat con annesso codice PIN

Secondo l'ABF (decisione n. 50/10, qui in [pdf](#), Collegio di Milano, seduta del 16 febbraio 2010) in caso di furto di bancomat con contestuale sottrazione del PIN (cioè pur nel caso che "l'ubicazione del codice personale segreto (sia) facilmente relazionabile alla carta"), "la banca è tenuta a mantenere indenne il titolare della carta da tutte le perdite derivanti da operazioni fraudolente effettuate in un momento successivo alla notifica (del furto alla banca ndr)";

Il quadro giuridico in ambito frodi informatiche presso gli intermediari finanziari

Appare particolarmente interessante quanto scrive il Collegio di Napoli (decisione n. 87/10, qui in [pdf](#)): "Invero l'intermediario aderendo in ciò ad uno stile consuetudinario sembra assumere che in virtù della clausole contrattuali che obbligano l'utente alla custodia dei codici di accesso, ogni accesso al sistema che implichi l'uso di detti codici da parte di terzi, implica una violazione dei doveri di custodia e quindi ricade nell'area di responsabilità contrattuale del cliente. Senza voler negare che l'uso di codici di accesso da parte di terzi sia un dato di fatto dotato di rilevanza, si deve tuttavia chiarire come **la deduzione logica sopra riferita non appaia corretta.**" Nel caso in questione, il cliente contestava operazioni effettuate sul suo conto corrente online attraverso i corretti codici di accesso. Il Collegio ne deduce che "una frode informatica è stata perpetrata"; tuttavia l'intermediario non è in grado di dimostrare "l'uso dei codici (da parte) del cliente, limitandosi ad asserire che essi erano stati utilizzati. (...) Si tratta di verificare quale delle due parti del rapporto debba sopportarne le conseguenze pregiudizievoli"; In conseguenza di tale ragionamento l'ABF ha deliberato che la banca deve rimborsare il cliente del 50% del danno subito.

Articolo scritto da **Massimo D'Alesio** - PROMETEO Management Consulting mdalesio@prometeomc.it

Articoli collegati

- [Banca d'Italia: rese note le prime decisioni adottate dall'ABF](#)
- [AIRA – Resoconto del convegno del 19 aprile 2010: "PSD – Payment Service Directive"](#)

Link utili

- Sito Arbitro Bancario Finanziario ([ABF](#))
- Banca d'Italia, [le nuove regole per l'offerta di servizi di pagamento](#)
- Approfondimento sul **phishing** in ambito bancario:
- [Aspetti economici del crimine online di Tyler Moore.](#)

[Richard Clayton e Ross Anderson](#) (traduzione in italiano) - 23 settembre

2009

- [Ross Anderson: "Chiudere la falla del phishing](#)

[– frodi e rischi nei sistemi di pagamento non bancari"](#),

traduzione italiana

- [Ross Anderson, Tyler Moore: quanto tempo un sito di phishing rimane attivo?](#)