Un contesto in continua evoluzione

Necessità di compliance al nuovo quadro normativo sulla sicurezza

- Normativa di **Vigilanza di Banca d'Italia**
- **Raccomandazioni BCE**
- Provvedimento **Garante II**
- Nuova **PSD**

La corretta **gestione** della **sicurezza informatica** e **lotta** al **cybercrime** sono **asset strategici** per l'evoluzione dei **servizi bancari**

La **banca** è interessata da un **fenomeno trasversale** che richiede una capacità di **monitoraggio e prevenzione continui e** un'attività di **cooperazione** nazionale e internazionale con le **altre banche** e con le **Forze dell'Ordine**

Gestione Sicurezza e Frodi Informatiche in banca

Incremento nell'utilizzo dei canali remoti bancari

- **Banche italiane che offrono** servizi via **Mobile: +25% dal 2011 al 2013***
- **Accessi** ai servizi di **Internet Banking****: **873 milioni per clientela Retail in Itali (+ 18,4 %** nel 2013)

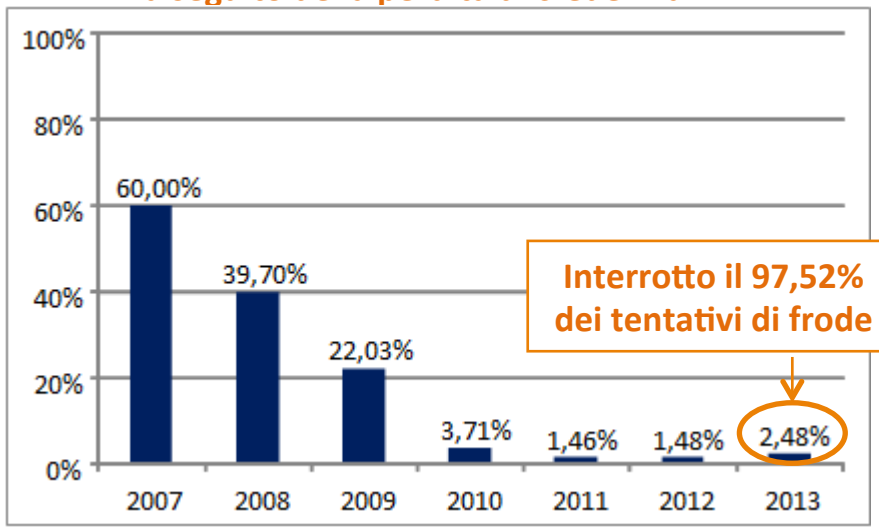
Sofisticazione degli attacchi informatici

- **Minacce tecnologicamente avanzate** e in continua **evoluzione**, basate spesso su meccanismi di **social engineering ➔ 28,1%** di attacchi di tipo **man in the browser**
- **Regia e coordinamento internazionale** di **organizzazioni criminali** dislocate su diversi paesi ➔ **complessità azioni di blocco**

*Fonte: ABI Lab e School of Management – Politecnico di Milano, Osservatorio Mobile Banking
**Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti; elaborazione sul numero medio di accessi per utente attivo

Il fenomeno delle frodi informatiche
Efficacia delle frodi – Confronto segmenti di clientela

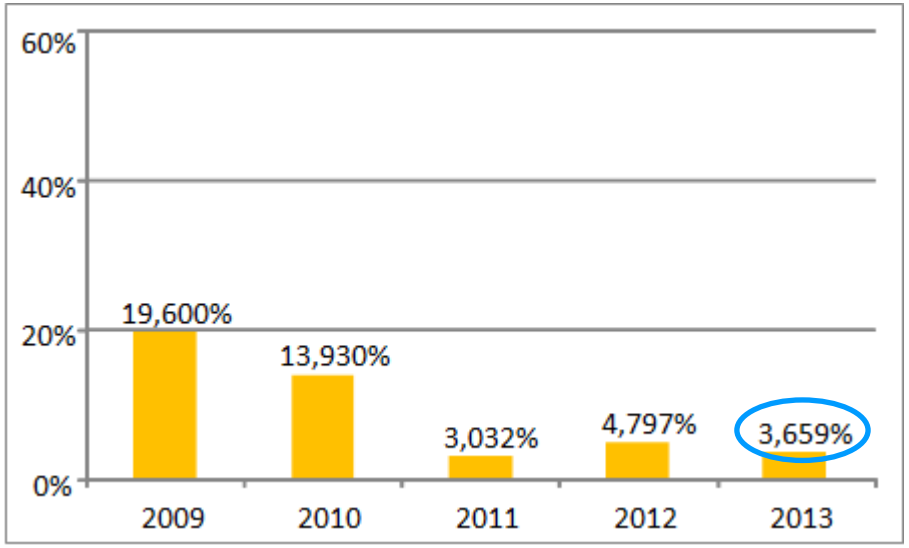
Percentuale di clienti attivi Retail che perde denaro a seguito della perdita di credenziali



- Nonostante il lieve incremento degli episodi di frode, l'**incidenza degli attacchi** rimane comunque **contenuta** (**2,48%**), anche se in lieve **aumento** rispetto al **2012**.
- È sempre più importante **associare** alle **contromisure tecnologiche** di contrasto anche importanti **iniziative di prevenzione** rivolte all'utente

- Dall'analisi svolta emerge un **miglioramento** dell'**efficacia** delle azioni di **contrasto** degli attacchi indirizzati al segmento Corporate: nel 2013, infatti, la percentuale di clienti che ha subito un danno economico a seguito del furto di credenziali è scesa al **3,659%**.
- Per avere una **visione completa** del fenomeno, è opportuno leggere tali informazioni insieme con le analisi sulla **numerosità degli episodi di frode** e sui relativi **volumi anomali** transati.

Percentuale di clienti attivi Corporate che perde denaro a seguito della perdita di credenziali

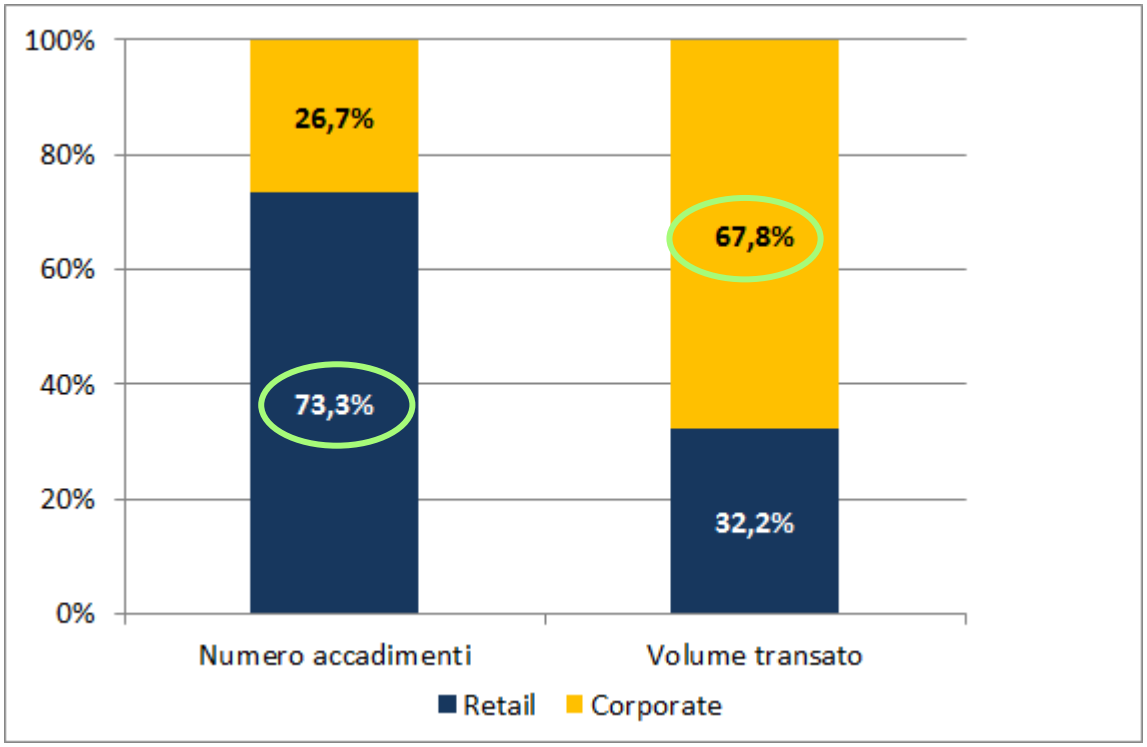


Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

Scenario complessivo transazioni fraudolente
Confronto segmenti di clientela

Totale transazioni anomale (bloccate, recuperate ed effettive)

Confronto Retail e Corporate su numero accadimenti e volume transato



A livello complessivo sul campione:

- Il comparto **Retail** appare soggetto a una **numerosità di attacchi** decisamente **superiore** rispetto al comparto **Corporate,** con un rapporto quasi di **3:1** (73,3% Retail, 26,7% Corporate).
- **La maggiore entità dei volumi economici** transati per l'intero campione di analisi è tuttavia associabile alla clientela **Corporate**, per tutte le fasi della transazione, con un rapporto complessivo di circa **2:1**.

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

L'evoluzione del quadro normativo in materia di sicurezza dei pagamenti

Crescente **attenzione** da parte delle **istituzioni** di riferimento a livello **nazionale** ed **europeo** in merito ai **rischi informatici** e all'esigenza di garantire **elevati livelli di sicurezza** nella realizzazione di **pagamenti da remoto** e nella **gestione dei dati**, come testimoniato dal recente fermento normativo in materia.

- Le **principali evoluzioni normative** con impatti sulla **gestione della sicurezza e del rischio informatico** investono principalmente gli ambiti di:
  - **Sicurezza degli accessi e dei servizi di pagamento**
    - *Payment Service Directive e recepimento a livello nazionale*
    - *Raccomandazioni BCE sulla sicurezza dei pagamenti internet + Assessment Guide BCE*
    - *Raccomandazioni BCE sulla sicurezza dei servizi di accesso ai conti di pagamento*
    - *Raccomandazioni BCE sulla sicurezza dei pagamenti Mobile*
  - **Sicurezza nel trattamento di dati e informazioni bancarie**
    - *Provvedimento Autorità Garante per la Privacy per la circolazione delle informazioni bancarie e il trattamento dei dati bancari*
  - **Valutazione del rischio informatico e correlazione con la gestione del rischio operativo**
    - *Disposizioni di vigilanza prudenziale di Banca d'Italia in materia di sistema dei controlli interni, sistema informativo e continuità operativa*

✓ emanato in corso di emanazione

Attività revisione PSD

- **TEMPISTICHE**
  - Presentato dalla CE il **24 luglio 2013** il primo testo **in bozza** della **nuova versione** della **PSD**
  - Il documento è **stato aggiornato** sulla base di **emendamenti ricevuti**
  - **L'ultima versione approvata dal Parlamento Europeo** risale ad **aprile 2014** ma l'iter di emanazione prevede ulteriori step (coinvolgimento **Consiglio Europeo)**
  - **Non** sono ancora **certi** i **tempi** di **emanazione** del testo definitivo
- **ANALISI DELLA NORMA E DIALOGO CON LE ISTITUZIONI DI RIFERIMENTO**
  - Redazione **Position Paper ABI**
  - Redazione **Position Paper EBF e EPC** con le osservazioni condivise tra tutti i Paesi (Italia compresa per il tramite di **ABI** e **ABI Lab**) partecipanti ai tavoli di lavoro legali e di sicurezza
- **PRINCIPALI PUNTI DI ATTENZIONE SOTTO IL PROFILO DELLA SICUREZZA**
  - **Sicurezza** dei pagamenti in relazione ai **servizi offerti da soggetti terzi (TPP)**
    - Aspetti legati alla **condivisione delle credenziali utente**
    - Identificazione di una **corretta ripartizione delle responsabilità tra PSP e TPP** in caso di operazioni non autorizzate o frodi
    - Necessità di **allineamento con Raccomandazioni SecurePay**
  - **Ripartizione responsabilità** in caso di **pagamenti non autorizzati** e **modalità di rimborso**
    - **Tempistiche** richieste (immediate) per l'erogazione dei **rimborsi, salvo casi di frode**
    - **Mancanza** di una **declinazione** del concetto di **comportamento negligente** e abbassamento limite massimo di perdita per il cliente

Raccomandazioni BCE in materia di sicurezza dei pagamenti Internet

ABI Lab
Tecnologia utile

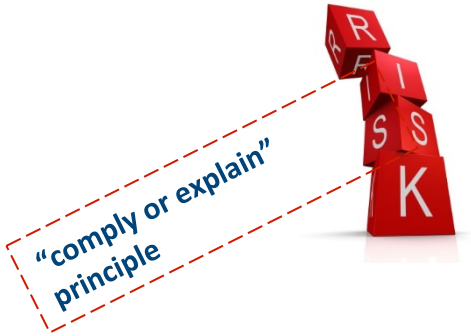
OBIETTIVO GENERALE

- Definire i **requisiti minimi** indirizzati a PSP*, **Autorità di governo** di schemi e sistemi di pagamento ed **e-merchant,** da applicare nell'erogazione di pagamenti tramite cards, credit transfers, e-mandate ed e-money

STRUTTURA del DOCUMENTO

- Le ***14 Recommendations*** sono **organizzate in 3 categorie:**
  - Controlli generali (Racc. 1-5);
  - Controlli specifici e misure di sicurezza per i pagamenti internet (Racc. 6-11);
  - Comunicazione con la clientela e customer awareness (Racc. 12-14);

  composte da *Key Considerations* e *Best Practices.*



TEMPI DI IMPLEMENTAZIONE e DOCUMENTAZIONE A SUPPORTO

- A livello nazionale, **le raccomandazioni sono recepite da Banca d'Italia e inserite nelle Nuove Disposizioni di Vigilanza Prudenziale**, e il termine previsto per l'adeguamento è fissato al **1 febbraio 2015**
- L' «**Assessment Guide**» **BCE** di **febbraio 2014**, indirizzato alle Autorità locali di vigilanza e di sorveglianza per l'attività ispettiva, può essere di **supporto** anche per le **banche** per comprendere le richieste dei supervisori.

IMPATTI PER LE BANCHE

- Secondo quanto previsto dai principi guida fondanti le raccomandazioni, sono previste le seguenti attività:
  - Realizzazione di un **assessment specifico** dei **rischi** connessi all'offerta dei servizi di pagamento online (fornite indicazioni di carattere organizzativo e operativo);
  - Introduzione di strumenti di **strong authentication** in fase di accesso ai servizi on line;
  - Implementazione di **procedure efficaci** in merito all'autorizzazione e monitoraggio delle transazioni per identificare comportamenti anomali e prevenire le frodi;
  - Promozione di **iniziative di sensibilizzazione** della **clientela**.

* Banche, istituti di pagamento, istituti di moneta elettronica, Poste e tramite apposite clausole contrattuali anche agli outsorcer coinvolti

Assessment Guide BCE in materia di sicurezza dei pagamenti Internet – Definizioni chiave (1/2)

ABI Lab
Tecnologia utile

"The initiation of internet payments as well as access to sensitive payment data should be protected by strong customer authentication".

SENSITIVE PAYMENT DATA

Sensitive payment data *are defined as* ***data which could be used to carry out fraud****.*
These include:

i. data enabling a payment order to be initiated:
- *payment account identifiers of the customer stored at the PSP (IBAN or equivalent); the BIC should not be considered sensitive data;*
- *payment card data (PAN, expiry date, CVx2);*

ii. data used for authentication:
- *customer identifiers (e.g. client number/log-in name);*
- *passwords, codes, personal identification numbers (PINs), secret questions, reset passwords/codes;*
- *phone number (mobile or landline, when applicable);*
- *certificates;*

iii. data used for ordering payment instruments or authentication tools to be sent to customers:
- *client's postal address;*
- *phone number, e-mail address;*

iv. data, parameters and software which, if modified, may affect the legitimate party's ability to verify payment transactions, authorise e-mandates or control the account: *such as "black" and "white" lists, customer-defined limits, etc:*
- *"black" and "white" lists, customer-defined limits, etc.*
- *data outlined in (i), (ii) and (iii), depending on applicability and methods used.*

È responsabilità della banca di individuare i tipi di dati di pagamento considerati sensibili

Assessment Guide BCE in materia di sicurezza dei pagamenti Internet – Definizioni chiave (2/2)

ABI Lab
Tecnologia utile

"The initiation of internet payments as well as access to sensitive payment data should be protected by strong customer authentication".

STRONG AUTHENTICATION

Strong customer authentication *is a* ***procedure based on the use of two or more of the following elements*** *– categorised as knowledge, ownership and inherence:*

i. something only the user knows*, e.g. static password, code, personal identification number****;***

ii. something only the user possesses*, e.g. token, smart card, mobile phone;*

iii. something the user is*, e.g. biometric characteristic, such as a fingerprint. In addition,* ***the elements selected must be mutually independent****, i.e. the breach of one does not compromise the other(s).*

At least one of the elements should be non-reusable and non-replicable *(except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data"*

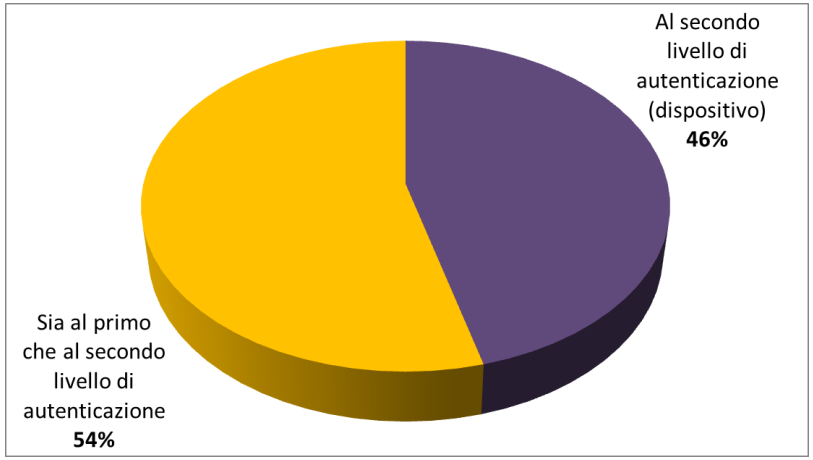
Further guidance on strong customer authentication solutions is provided under Recommendation 7.

From the Forum's perspective, PSPs with no or only weak authentication procedures cannot, in the event of a disputed transaction, provide proof that the customer has authorized the transaction.

Lo scenario italiano
Soluzioni di secondo fattore

Segmento Retail

Secondo fattore di autenticazione*



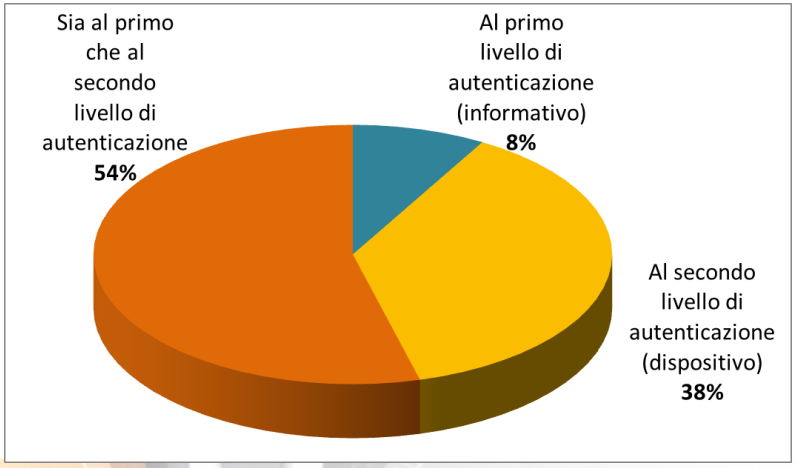
* 24 rispondenti

- **Tutte** le banche intervistate ricorrono a un **doppio livello di autenticazione**.
- **Tutte** le banche mettono a disposizione **almeno una tecnologia di secondo fattore**. In particolare:
  - Il **91,8%** delle banche **obbliga tutti i propri clienti** all'**utilizzo di strumenti di II fattore** (o di almeno uno, a scelta del cliente, se ne vengono forniti diversi).
  - Tra le tecnologie più diffuse, si riportano l'**OTP via hardware disconnesso** (**70,8%**), **l'OTP via SMS** (**37,5%**) e la **tessera a combinazione** (**25%**).

Segmento Corporate

- **Tutte** le banche intervistate ricorrono a un **doppio livello di autenticazione**.
- **Tutte** le banche mettono a disposizione **almeno una tecnologia di secondo fattore**. In particolare:
  - Le **banche che obbligano tutti i propri clienti** all'utilizzo di almeno uno strumento di secondo fattore rappresentano l'**83,4%** del campione.
  - Oltre all'**OTP via hardware disconnesso** (**58,3%**), alla clientela Corporate viene messo a disposizione il certificato di firma digitale (**29,2%**) e l'OTP via SMS (**20,8%**).

Secondo fattore di autenticazione*

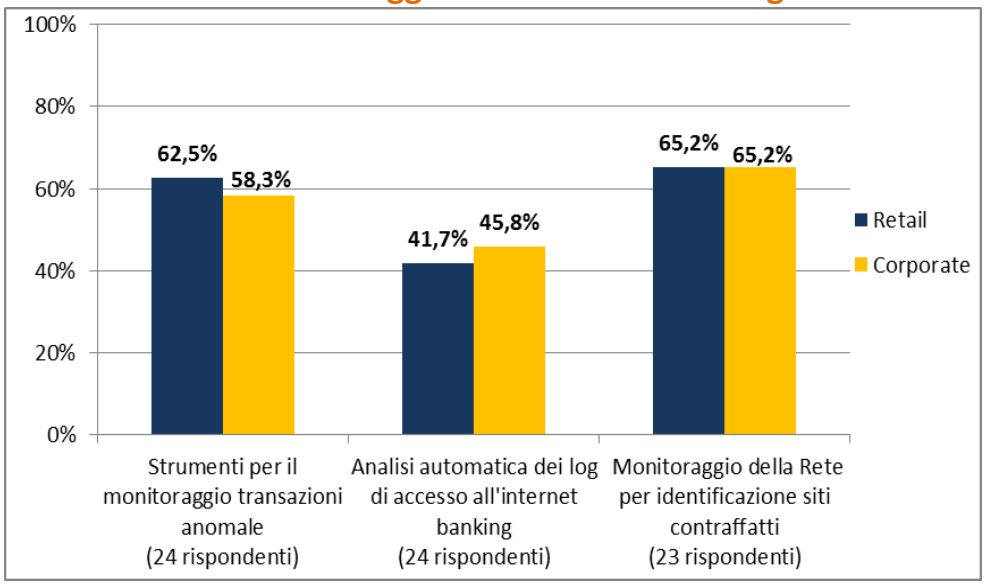


Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

Lo scenario italiano

Strumenti di monitoraggio e comunicazione con la clientela

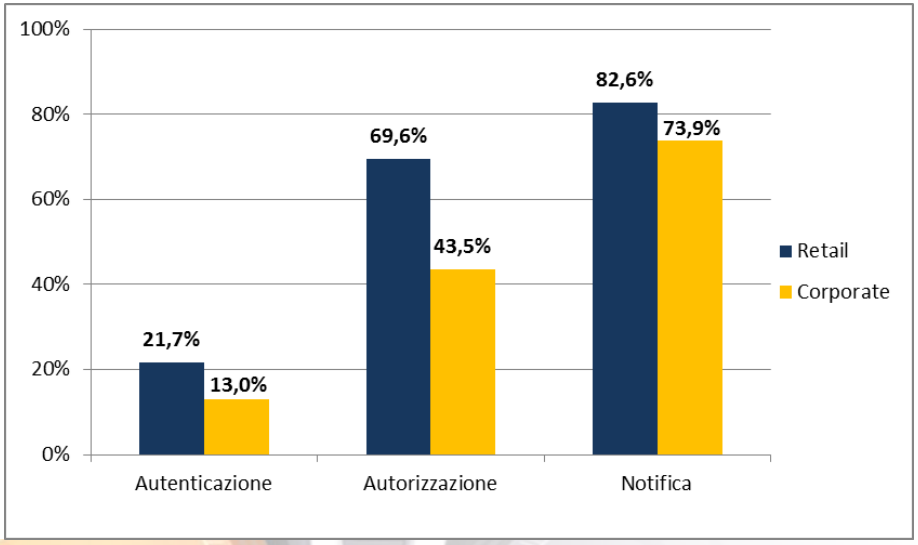
Attività di monitoraggio e dotazione tecnologica



- Sempre più banche si stanno dotando di **strumenti in grado di monitorare** la **rete**, le **transazioni anomale** effettuate e gli **accessi** al portale di Internet Banking da parte della propria clientela, sia **Retail** che **Corporate**.
- È evidente quindi come si mantenga **costante l'attenzione del settore bancario sul contrasto al fenomeno delle frodi informatiche**, anche attraverso l'utilizzo di **strumenti tecnologici** sempre più **evoluti e aggiornati**, in linea con le previsioni normative a livello europeo (Raccomandazioni BCE).

- Tra le **misure di sicurezza** per ridurre l'impatto di eventuali attacchi fraudolenti, particolare **importanza** viene riconosciuta al **canale alternativo di comunicazione** verso la clientela.
- A livello generale, qualche **margine di miglioramento** potrebbe esserci in relazione alla **clientela Corporate**, per la quale il **canale alternativo** di comunicazione **viene messo a disposizione in misura inferiore** rispetto al segmento **Retail**, specialmente in fase di **autorizzazione** delle disposizioni (particolarmente diffusi sono l'invio di SMS o di e-mail).

Utilizzo di un canale alternativo di comunicazione



Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2014, 25 rispondenti

Aggiornamento raccomandazioni BCE sui servizi di accesso ai conti di pagamento

ABI Lab
Tecnologia utile

RIEPILOGO ATTIVITÀ

- *Gennaio 2013:* pubblicazione per **consultazione** delle **Raccomandazioni sulla sicurezza dei servizi di accesso ai conti di pagamento lati ai cd TPP** (Third Party Provider)
- *Aprile 2013:* invio PP ABI e contributo ABI/ ABI Lab a PP EPC in **risposta alla consultazione**
- *Maggio 2013 – Febbraio 2014*: **analisi** da parte del Forum SecurePay delle **38 risposte** ricevute e approfondimento problematiche legate ai servizi offerti da TPP, anche in relazione alla revisione della PSD
- *Marzo 2014*: **pubblicazione** da parte della BCE di «**Public note on security of payment account access services»** http://www.ecb.europa.eu/pub/pdf/other/pubnote201403securitypaymentaccountaccessservicesen.pdf
- *Maggio 2014*: **pubblicazione** della **versione definitiva** delle raccomandazioni, a **utilizzo esclusivo** dell'**EBA** per la definizione di opportune linee guida come previsto dalla PSD2

PRINCIPALI PUNTI DI ATTENZIONE CONTENUTI NEL PUBLIC NOTE

- **Maggiore consapevolezza delle problematiche di sicurezza** dei pagamenti in relazione ai **servizi offerti dai TPP,** con particolare riferimento a
  - Rischi legati dalla **condivisione delle credenziali utente**
  - Utilità di **contratti TPP- PSP** o di **definizione** di **standard operativi sicuri**

Discussione ancora aperta ai tavoli europei

- **Approcci proposti** per garantire elevati livelli di sicurezza ➔ verso un nuovo **standard** condiviso con EBA
  - **Reindirizzamento** sicuro **dell'utente al proprio PSP**, durante il processo di pagamento tramite TPP, in modo da **autenticarsi**
  - **Distribuzione** da parte del TPP **ulteriori credenziali** di autenticazione all'utente

Necessità di allineamento con **PSD2 (nuova versione approvata** in **Parlamento EU** in **aprile 2014)**

Security in e-payments

Tavola Rotonda di confronto, interverranno:

- Gino **Giambelluca,** *Condirettore* **Banca d'Italia**
- Alessio **Santoni,** *e-Banking Manager* **Banca Passadore & C.**
- Andrea **Agosti,** *Responsabile Servizio Security* **OASI Outsourcing Applicativo e Servizi Innovativi – Gruppo ICBPI**
- Agostino **Ghebbioni,** *Direttore Financial Services* **Indra Italia**
- Giorgio **Ferrero,** *Presidente* **PRETA - MyBank**