L'ECONOMIA PER TUTTI

BANCA D'ITALIA PER LA CULTURA FINANZIARIA

Conoscere per scelte finanziarie consapevoli

Gli strumenti di pagamento elettronici

Bologna, 15 ottobre 2025

Francesco Dell'Isola

BANCA D'ITALIA
EUROSISTEMA

L'ECONOMIA PER TUTTI

BANCA D'ITALIA PER LA CULTURA FINANZIARIA

Conoscere per scelte finanziarie consapevoli

1 – La tutela della clientela

- Strumenti di tutela individuale
- L'Arbitro Bancario Finanziario

2 – Gli utilizzi fraudolenti

- Normativa applicabile
- Principali tipologie di frodi

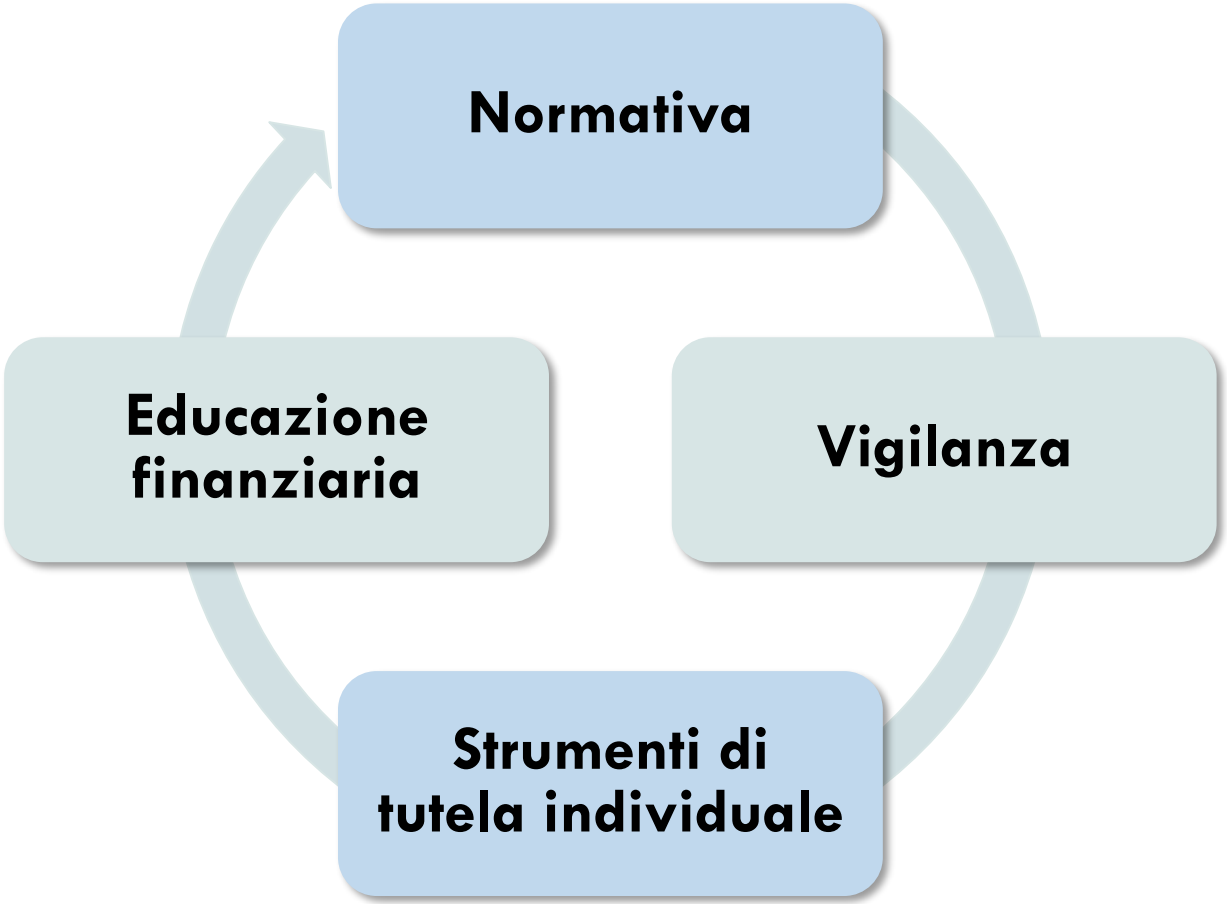
3 – Case study

- Anydesk
- Vishing caller ID spoofing

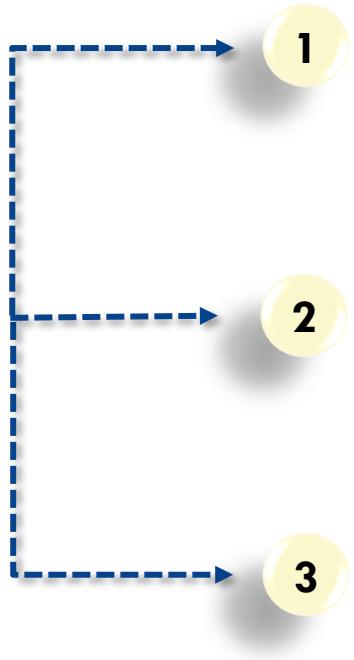
BANCA D'ITALIA
EUROSISTEMA

LA TUTELA DELLA CLIENTELA: PERCHÈ?

LA TUTELA DELLA CLIENTELA: COME?



STRUMENTI DI TUTELA INDIVIDUALE: QUALI?



Esposto alla Banca d'Italia

Reclamo alla banca

Ricorso all'ABF

CHE COS'È L'ESPOSTO? A COSA SERVE?

Segnalazione scritta di comportamenti scorretti tenuti da parte dell'intermediario

Favorisce il dialogo banca/cliente

NON decide nel merito

BANCA D'ITALIA
EUROSISTEMA

CHE COS'È IL RECLAMO? A COSA SERVE?

- Contestazione in **forma scritta diretta alla banca** in relazione a un suo comportamento, anche omissivo

- Risposta scritta di **accoglimento/rigetto** entro **60** giorni (**15** per i servizi di pagamento)

- Solo in caso di **rigetto** o di **mancata risposta** nei termini, si può presentare **ricorso all'ABF**

CHE COS'È L'ABF? A COSA SERVE?

CHE COSA E' L'ABF

L'ABF è un sistema di risoluzione stragiudiziale per le controversie in materia bancaria e finanziaria

SU COSA DECIDE?

Decide su questioni relative a servizi bancari, finanziari o di pagamento

CI SONO LIMITI SUGLI IMPORTI?

- Fina a € 200.000 se si chiede una somma di denaro
- Nessun limite di importo, se si chiede l'accertamento di diritti, obblighi e facoltà

E' NECESSARIO UN AVVOCATO?

No, il ricorso può essere presentato in totale autonomia, attraverso il portale online

QUANTO COSTA?

Solo € 20 che vengono restituiti in caso di accoglimento del ricorso

BANCA D'ITALIA
EUROSISTEMA

IL COLLEGIO ABF

Collegio di Coordinamento

COLLEGIO DI ROMA: Abruzzo, Lazio, Marche, Umbria

COLLEGIO DI MILANO: Friuli-Venezia Giulia, Lombardia, Trentino-Alto Adige, Veneto

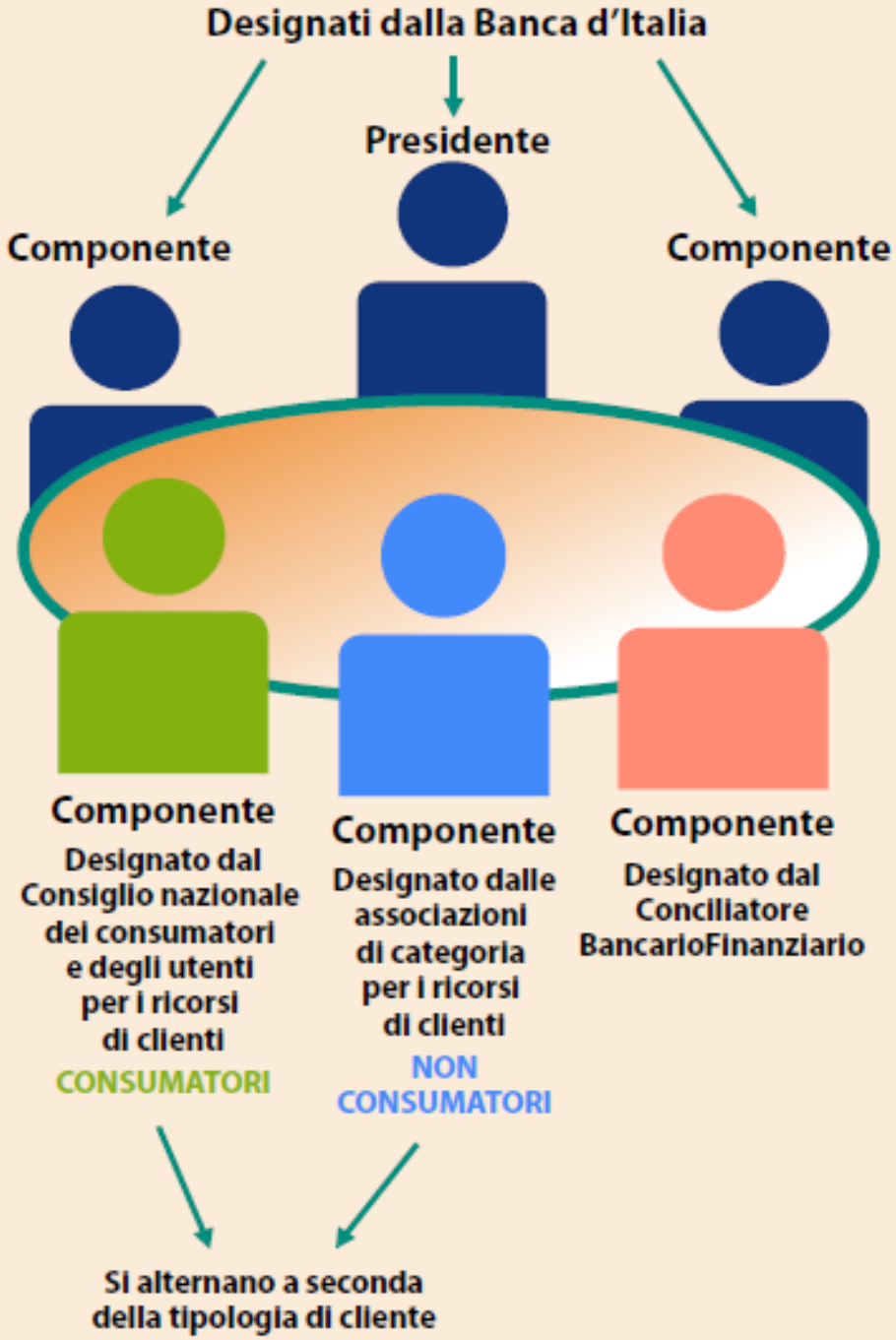
COLLEGIO DI TORINO: Liguria, Piemonte, Valle d'Aosta

COLLEGIO DI BOLOGNA: Emilia-Romagna, Toscana

COLLEGIO DI NAPOLI: Campania, Molise

COLLEGIO DI BARI: Basilicata, Calabria, Puglia

COLLEGIO DI PALERMO: Sardegna, Sicilia



I DATI DEL 2024

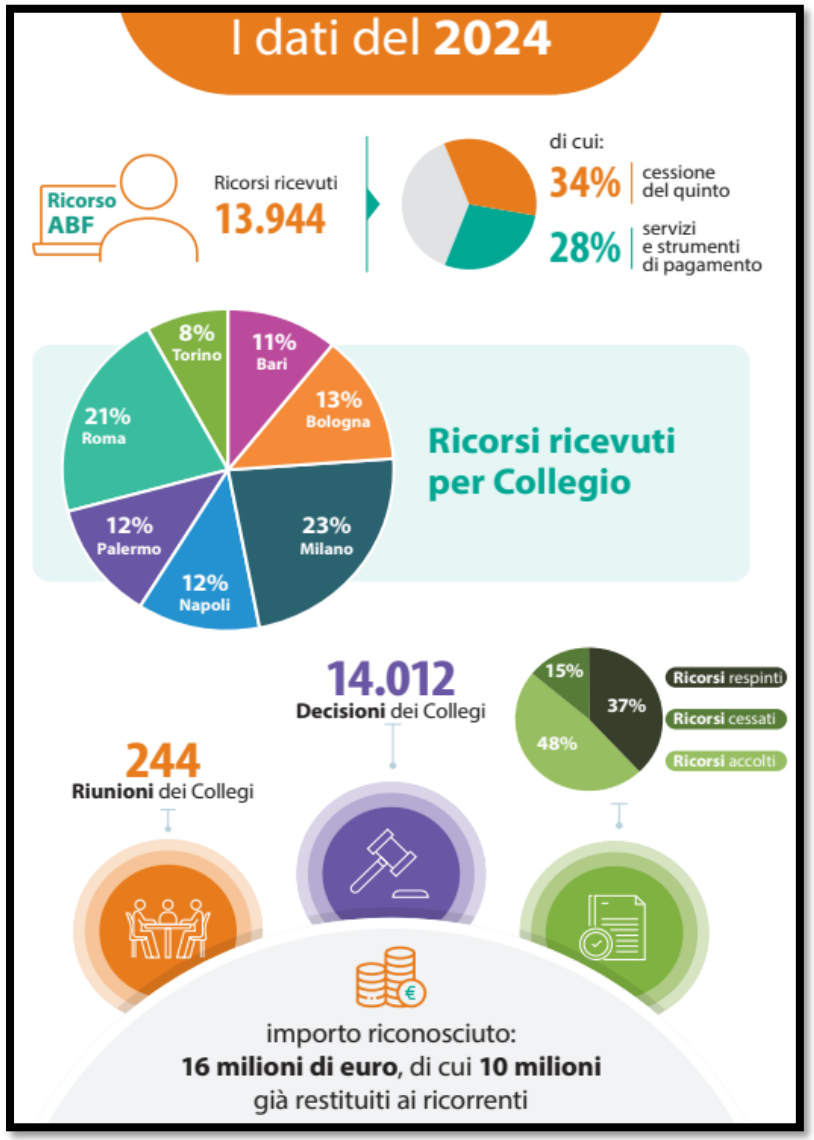


Figura 1.1

Ricorsi ABF annuali ricevuti
(unità)

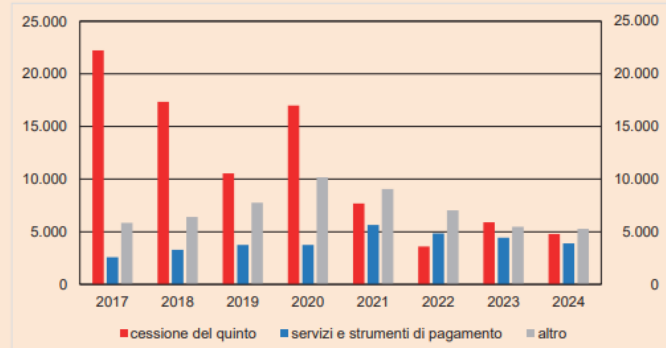


Tavola 1.1

Ricorsi ricevuti per oggetto della controversia: confronto con il 2023
(unità e valori percentuali)

OGGETTO DELLA CONTROVERSIA	2023		2024		Variazione del 2024 sul 2023
	unità	% sul totale	unità	% sul totale	variazione percentuale
Cessione del quinto	5.902	37	4.783	34	-19
Conto corrente	1.382	9	1.637	12	18
Bancomat e carte di debito	1.987	13	1.456	10	-27
Carte di credito	1.588	10	1.183	8	-26
Bonifico	621	4	1.016	7	64
Sistemi di informazione creditizia (SIC)	738	5	769	6	4
BFP	1.154	7	717	5	-38
Credito ai consumatori	383	2	419	3	9
Mutuo	497	3	400	3	-20
Centrale dei rischi	446	3	353	3	-21
Altro	1.119	7	1.211	9	8
Totale ricorsi ABF	**15.817**	**100**	**13.944**	**100**	**-12**
Totale ricorsi escludendo CQS	9.915	63	9.161	66	-8
Totale ricorsi servizi e strumenti di pagamento	4.432	28	3.896	28	-12
Totale ricorsi utilizzi fraudolenti	4.615	29	4.123	30	-11

BANCA D'ITALIA
EUROSISTEMA

OBBLIGHI DELL'UTENTE

Art. 7
D. Lgs. 11/2010

- utilizzare lo strumento di pagamento in **conformità al contratto**
- adottare tutte le ragionevoli misure idonee a **proteggere le credenziali di sicurezza personalizzate**
- comunicare **senza indugio** al PSP lo smarrimento, il furto, l'appropriazione indebita o l'**uso non autorizzato** dello strumento

OBBLIGHI DEL PSP

Art. 8
D. Lgs. 11/2010

- Assicurare che le **credenziali di sicurezza** personalizzate **non siano accessibili** a soggetti diversi dall'utente abilitato
- Mettere a disposizione dell'utente, a titolo gratuito, **strumenti adeguati al blocco** dello strumento di pagamento
- **Impedire** qualsiasi **utilizzo** dello strumento di pagamento **successivo al blocco**
- Tenere **indenne l'utente** dai **rischi** derivanti dalla **spedizione** di uno strumento di pagamento o delle relative credenziali di sicurezza

ONERE DELLA PROVA: SCA E COLPA GRAVE

Il **PSP** deve provare che **l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata** senza anomalie (SCA)

Art. 10
d.lgs. 11/2010

Qualora l'utente **neghi** di aver autorizzato un'**operazione di pagamento**:

Il **PSP** deve dimostrare che l'utente abbia agito in **modo fraudolento**, con **dolo** o con **colpa grave**

BANCA D'ITALIA
EUROSISTEMA

LA STRONG CUSTOMER AUTHENTICATION (SCA)

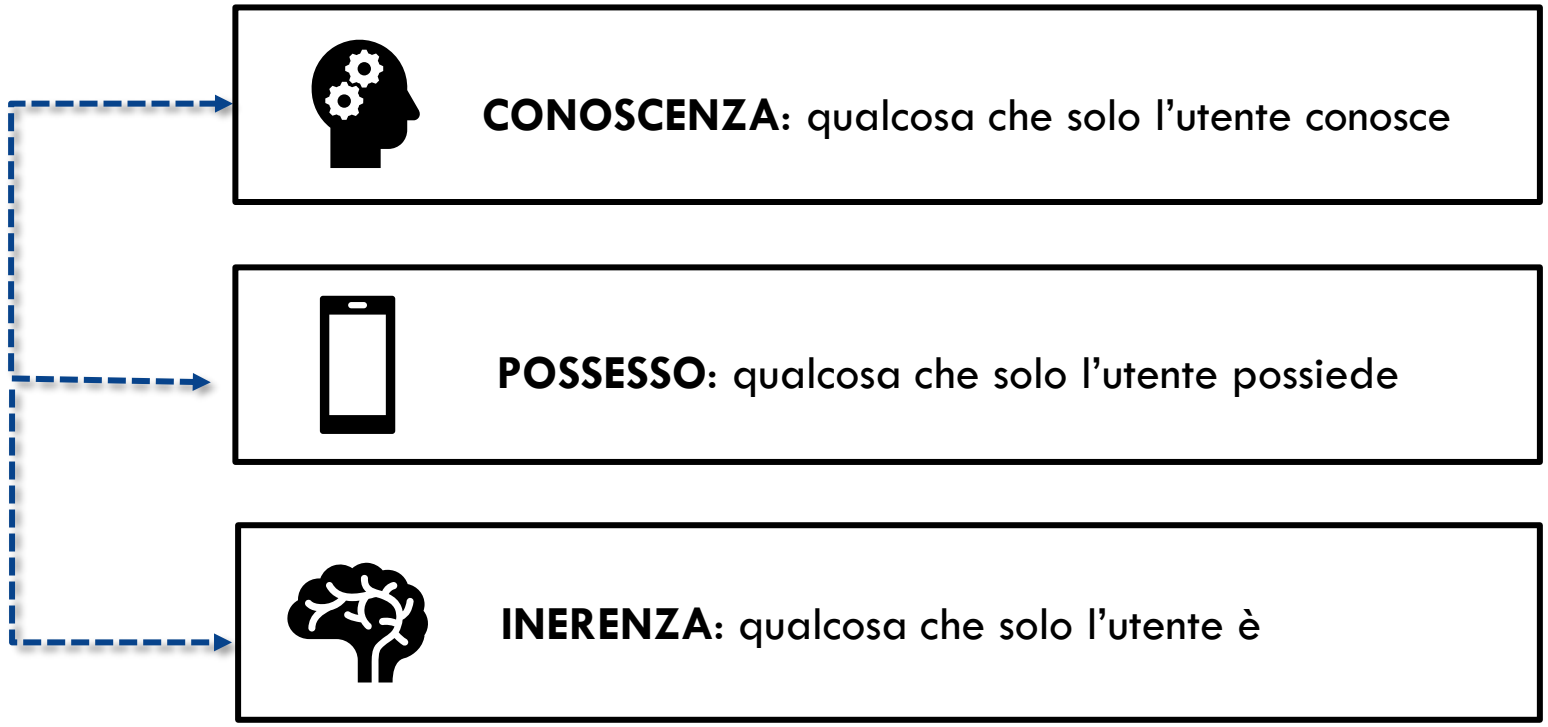
Art. 10-bis
d.lgs. 11/2010

Il **PSP** applica l'autenticazione **forte** quando l'utente:

1. accede al suo **conto** di pagamento on-line
2. dispone **un'operazione di pagamento** elettronico
3. effettua **qualsiasi azione,** tramite un **canale a distanza,** che può comportare un **rischio di frode** nei pagamenti o altri abusi

LA STRONG CUSTOMER AUTHENTICATION (SCA)

L'identità dell'utente deve essere verificata attraverso l'utilizzo di **almeno due** tra i seguenti elementi, che devono essere **indipendenti** tra



LA COLPA GRAVE

«un **comportamento abnorme** e, in quanto tale, **non scusabile**»

È ammessa la prova **in via presuntiva**

Secondo l'Arbitro generalmente sussiste la **colpa grave** dell'utente nei casi di **phishing**, **vishing** e **smishing**

Non è diligente il comportamento di chi risponde a una e-mail/sms di phishing inserendo i dati della propria carta di pagamento!

BANCA D'ITALIA
EUROSISTEMA

COME DECIDE L'ABF?

Il **PSP** ha fornito la prova **dell'autenticazione, corretta registrazione e contabilizzazione** dell'operazione contestata?

- **SI** → Il **PSP** ha dimostrato il la **colpa** grave, il **dolo** o la **frode** dell'**utente**?
  - **SI** → L'**utente** **sopporta tutte le perdite**
  - **NO** → Il **PSP** **sopporta** tutte le **perdite**, al netto della franchigia di € 50,00
- **NO** → Il **PSP** **sopporta tutte le perdite**, salvo la frode dell'utente

BANCA D'ITALIA
EUROSISTEMA

ULTERIORI ELEMENTI DI RILIEVO: L'SMS ALERT

Collegio di Coordinamento, decisione n. 24366/2019

«Fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. Gli effetti della mancata adozione del servizio di alert dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto».

Secondo la **posizione condivisa dell'Arbitro**
è irrilevante la mancata attivazione ovvero il **mancato funzionamento** del servizio di sms-alert (o di servizio assimilabile) nei casi in cui la ricezione dell'alert **non possa in concreto limitare il pregiudizio dell'utente,** ossia nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta ovvero di più transazioni ma a distanza di pochi minuti l'una dall'altra, e complessivamente in un arco di tempo limitato.

ULTERIORI ELMENTI DI RILIEVO: MANCATO/TARDIVO BLOCCO

Dell'utente…

«…la ricorrente non riferisce cosa abbia fatto dopo che la carta è stata trattenuta dall'ATM e, in particolare, se ha tenuto sotto controllo il terminale, quanto meno fino al momento in cui ha bloccato la carta. In conclusione, il Collegio ritiene che, alla luce degli elementi a sua disposizione, dovendosi escludere qualunque ipotesi di clonazione, si possa presumere una condotta gravemente negligente della ricorrente» (Collegio di Torino, decisione n. 6894/2024)

… e del PSP

«Sul punto occorre richiamare la decisione del Collegio di Torino n. 20475/2020 in cui il Collegio ha rilevato la responsabilità dell'intermediario anche per aver consentito un'operazione di pagamento dopo che l'istante aveva disposto il blocco della carta» (Collegio di Torino, decisione n. 8992/2022)

BANCA D'ITALIA
EUROSISTEMA

ULTERIORI ELEMENTI DI RILIEVO: INDICI DEL RISCHIO DI FRODE

sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento (punto 1 della lett. b) dell'art. 8)

tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita (punto 2 della lett. a) dell'art. 8)

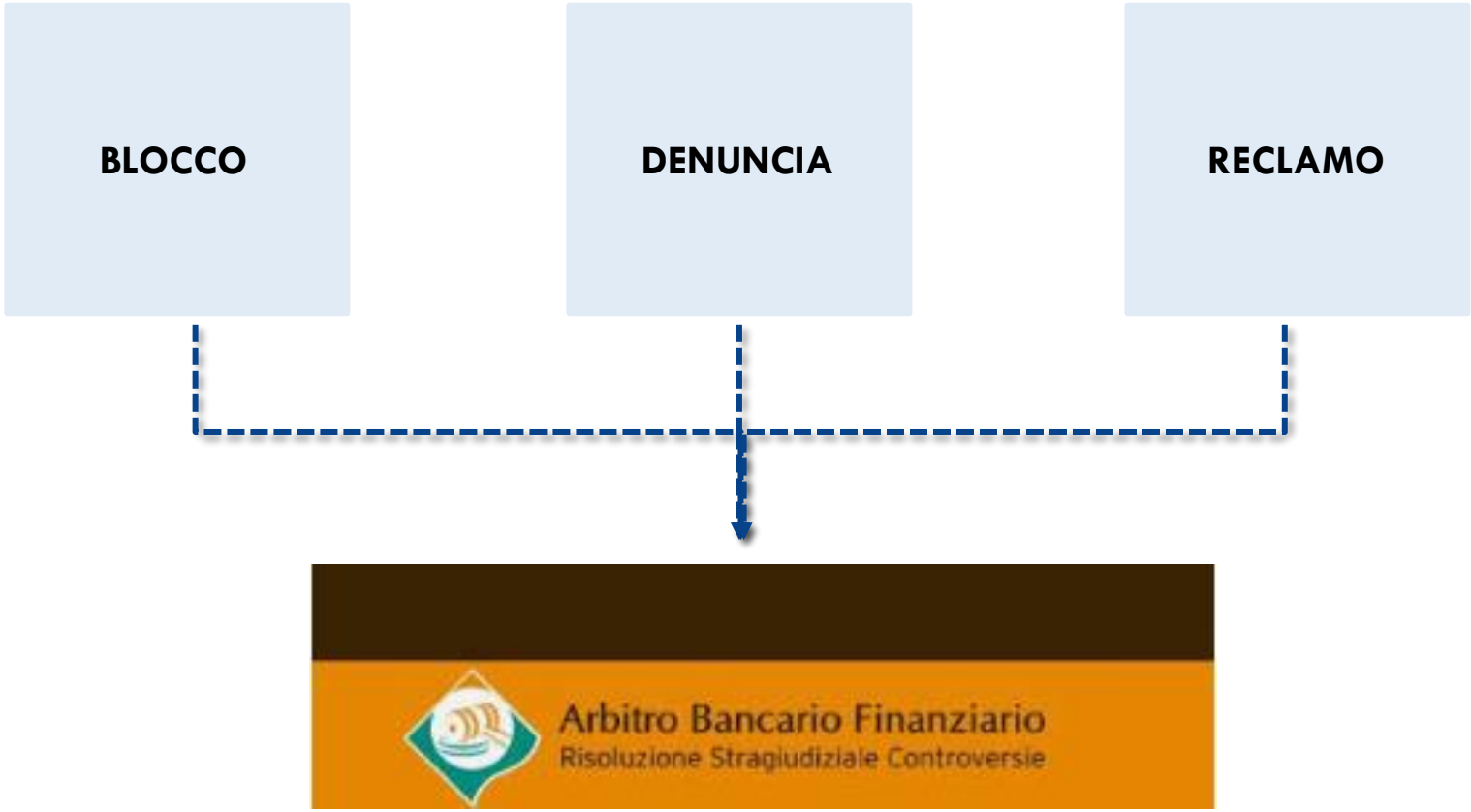
due o più richieste di autorizzazione provenienti da Stati diversi, effettuate, con la stessa carta, nell'arco di sessanta minuti (punto 3 della lett. b) dell'art. 8)

Art. 8, D.M. 112/2007

«Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento»

- i principi del D.M. 112/2007 non hanno un valore precettivo, ma sono espressione di un **generale obbligo di monitoraggio** delle operazioni
- i Collegi possono quindi valorizzare anche indici di frode **ulteriori** a quelli del D.M. 112/2007

COSA FARE IN CASO DI UTILIZZO FRAUDOLENTO DEL PROPRIO STRUMENTO DI PAGAMENTO?



BANCA D'ITALIA
EUROSISTEMA

LE TRUFFE DI SOCIAL ENGINEERING

L'ingegneria sociale (in inglese, social engineering) è lo **studio del comportamento di una persona** al fine di carpire informazioni utili in vista dell'esecuzione di una **frode.**

La tecnica si svolge secondo le seguenti fasi:

Studio

Attacco

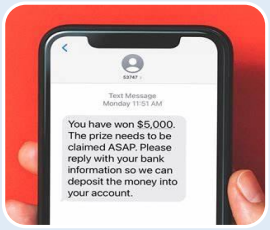
Cattura informazioni

Esecuzione della frode

BANCA D'ITALIA
EUROSISTEMA

PRINCIPALI TIPOLOGIE DI FRODE

PHISHING
Richiesta via e-mail di inserire dati personali attraverso un link a un sito, che di solito è un clone di quello della propria banca



SMISHING
Phishing tramite sms

VISHING
Phishing tramite telefono

BOXING
Il truffatore intercetta le carte di pagamento in occasione del loro invio al cliente tramite il sistema postale

SPOOFING
Il truffatore camuffa il mittente della mail, dell'SMS o della telefonata in modo che sembri provenire dall'intermediario

MAN IN THE BROWSER
Il truffatore intercetta i dati inseriti tramite un virus informatico che si infiltra nel tuo browser. Il virus può modificare transazioni o pagine web in tempo reale

BANCA D'ITALIA
EUROSISTEMA

L'APP «ANYDESK»: COLLEGIO DI BOLOGNA, DECISIONE N. 3608/24

SMS spoofing

Vishing

Download APP

Bonifico

L'APP «ANYDESK»: COLLEGIO DI BOLOGNA, DECISIONE N. 3608/24

Parte ricorrente disconosce un bonifico istantaneo disposto tramite *home banking* in data 3/07/2023 alle ore 12:57, di importo pari a **€ 9.000,00**.

Dalla documentazione prodotta si evince che il malfattore ha eseguito l'**accesso via web** inserendo correttamente la **password** e il **codice OTP**, previo invio dello stesso sull'applicazione della banca installata nel cellulare del ricorrente; ha poi eseguito il bonifico inserendo un secondo codice OTP (quanto al secondo fattore, cfr. Q&A EBA 2018_4141).

A conferma del giudizio di colpa grave […], dopo aver ***cliccato il link*** *ed essere approdata sulla pagina web, la stessa decideva di inserire i propri dati anagrafici ed il proprio numero di telefono. Una volta contattata da un sedicente operatore,* ***ne seguiva poi alla lettera le istruzioni, scaricando l'app "anydesk" e comunicando le credenziali*** *essenziali per eseguire l'accesso. Infine, tutte le notifiche contenenti i codici OTP necessari per eseguire l'accesso e poi per autorizzare il bonifico menzionavano espressamente, e in modo chiaro, l'operazione da autorizzare.* ***P.Q.M. Non accoglie il ricorso***

VISHING CALLER ID SPOOFING: COLLEGIO DI BOLOGNA, DECISIONE N. 1608/25

Vishing (chiamata da numero riferibile alla banca)

Spoofing

Bonifico

VISHING CALLER ID SPOOFING: COLLEGIO DI BOLOGNA, DECISIONE N. 1608/25

Parte ricorrente disconosce un bonifico istantaneo disposto tramite *home banking* in data 3/07/2023 alle ore 12:57, di importo pari a **€ 18.900,00**.

L'accesso all'home banking, eseguito via WEB, è stato autorizzato mediante inserimento del Face ID al ricevimento della notifica push in app. Quanto all'autenticazione del bonifico, pur in assenza di idonea documentazione, il Collegio ha ritenuto provata la SCA valorizzando le dichiarazioni confessorie del ricorrente, che nella denuncia aveva ammesso di aver rivelato al truffatore le credenziali necessarie per autorizzare l'operazione.

La truffa in questione, nota come "*vishing caller ID*", presenta **particolari elementi di sofisticazione e di anomalia**, tali da dover essere contrastati dall'intermediario predisponendo un adeguato sistema di sicurezza dei pagamenti (cfr. Coll. Roma, dec. 8749/2024). In particolare, pur tenendo conto della grave negligenza del cliente, che ha ritenuto verosimile la procedura descritta dal truffatore, ed ha prestato fede a messaggi civetta contenenti gravi errori grammaticali, risulta agli atti lo screenshot della chiamata ricevuta dal ricorrente, **il cui numero, come verificato dal Collegio, corrisponde effettivamente a quello di una filiale dell'intermediario resistente**. Tale circostanza ha contribuito ad alimentare una percezione erronea della medesima operazione in cui si era fraudolentemente inserito il frodatore.

GRAZIE PER L'ATTENZIONE !

edufin.bologna@bancaditalia.it

PER APPROFONDIRE:

L'economia per tutti

https://economiapertutti.bancaditalia.it/

Quello che conta

http://www.quellocheconta.gov.it/it/