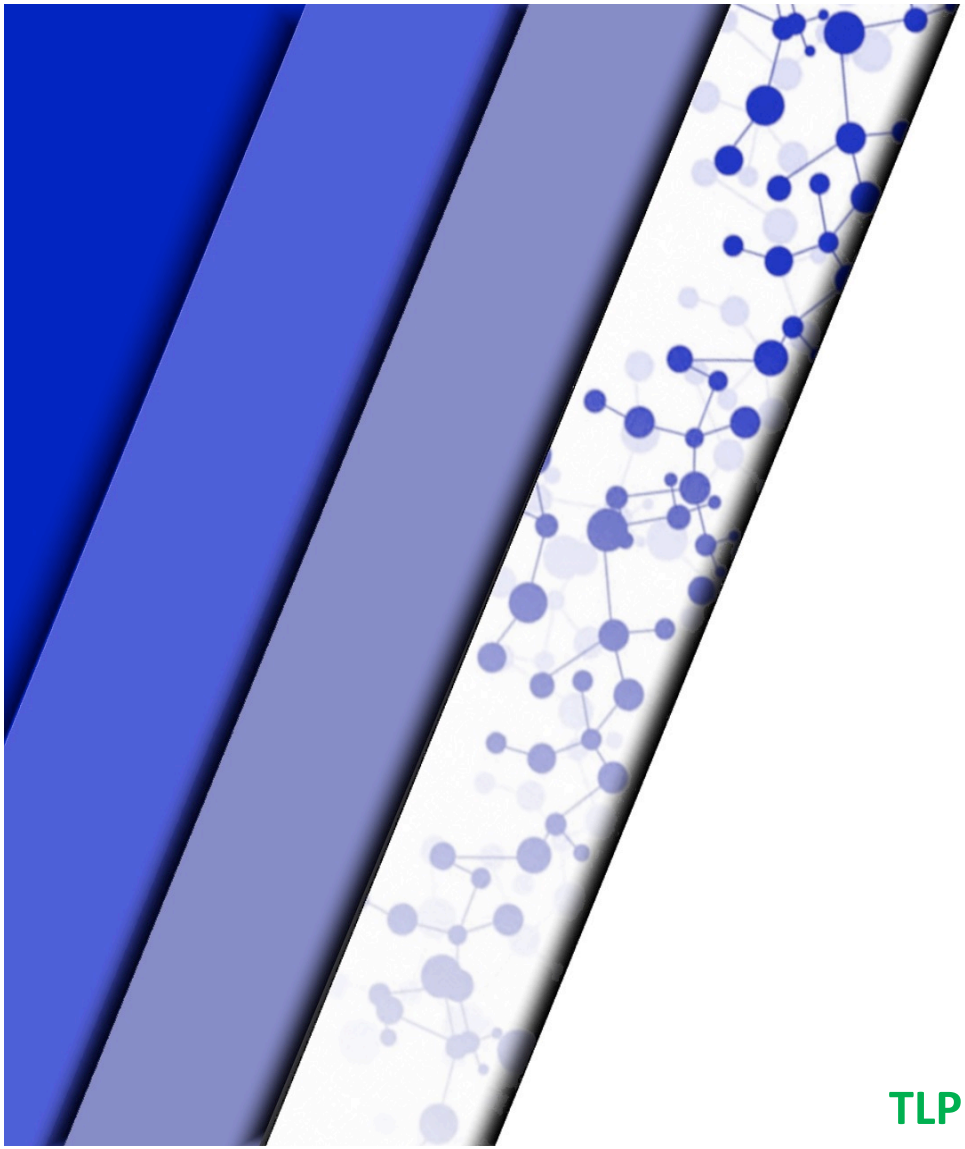


CERTFin

Sicurezza e Frodi in Banca
Report 2022

19 maggio 2022

BANCHE & SICUREZZA

Mario Trinchera
Technical Coordinator

TLP: GREEN

Report Sicurezza e Frodi 2022
…in Sintesi

La clientela retail è nettamente il target preferito

del totale degli attacchi

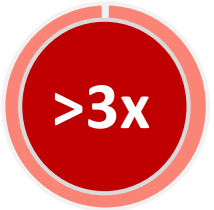
Significativo decremento del numero di transazioni anomale…

Rispetto allo scorso anno

…e del controvalore complessivo delle frodi

Rispetto allo scorso anno

…ma, rispetto all'epoca pre-pandemia, tale cifra è più che triplicata



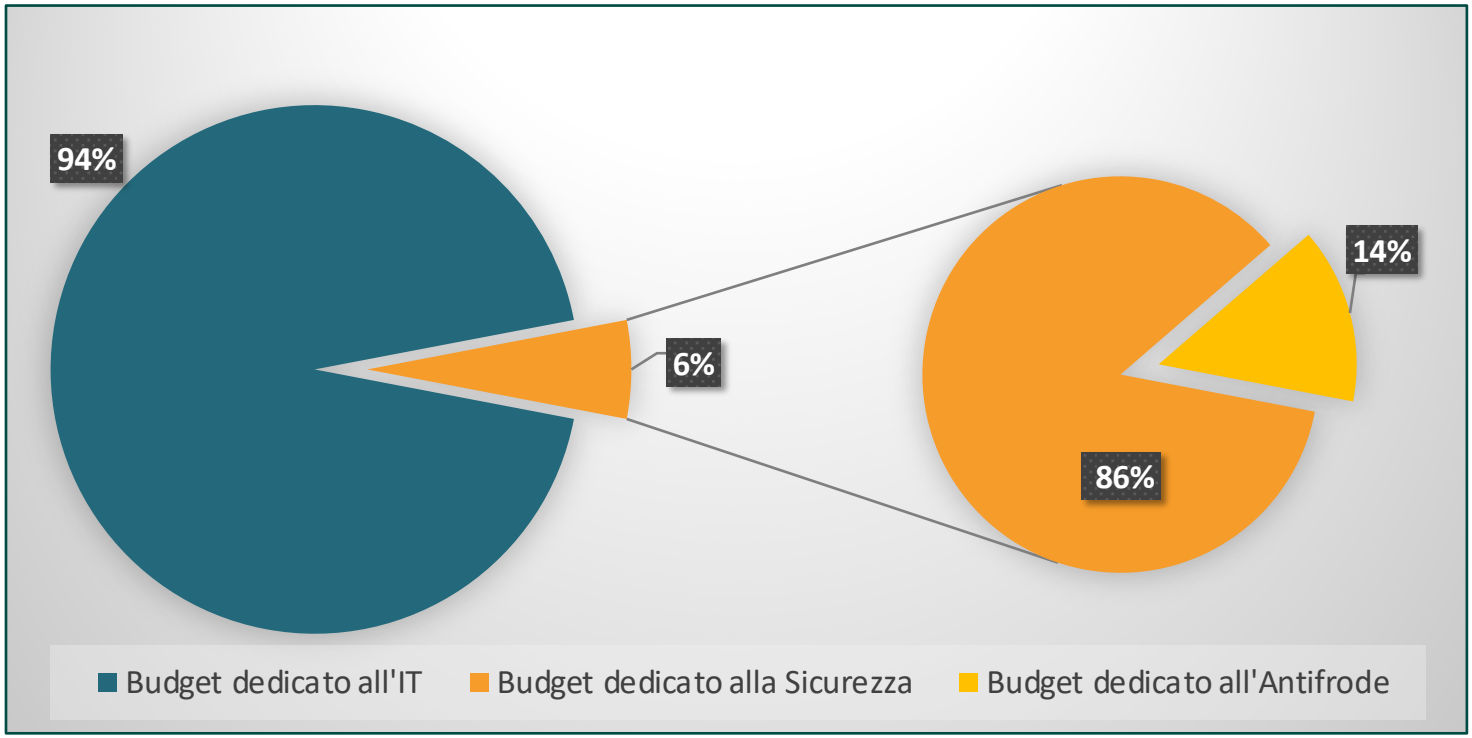
Rispetto al 2019

Notevole il controvalore in euro delle frodi «recuperate»

Milioni di euro

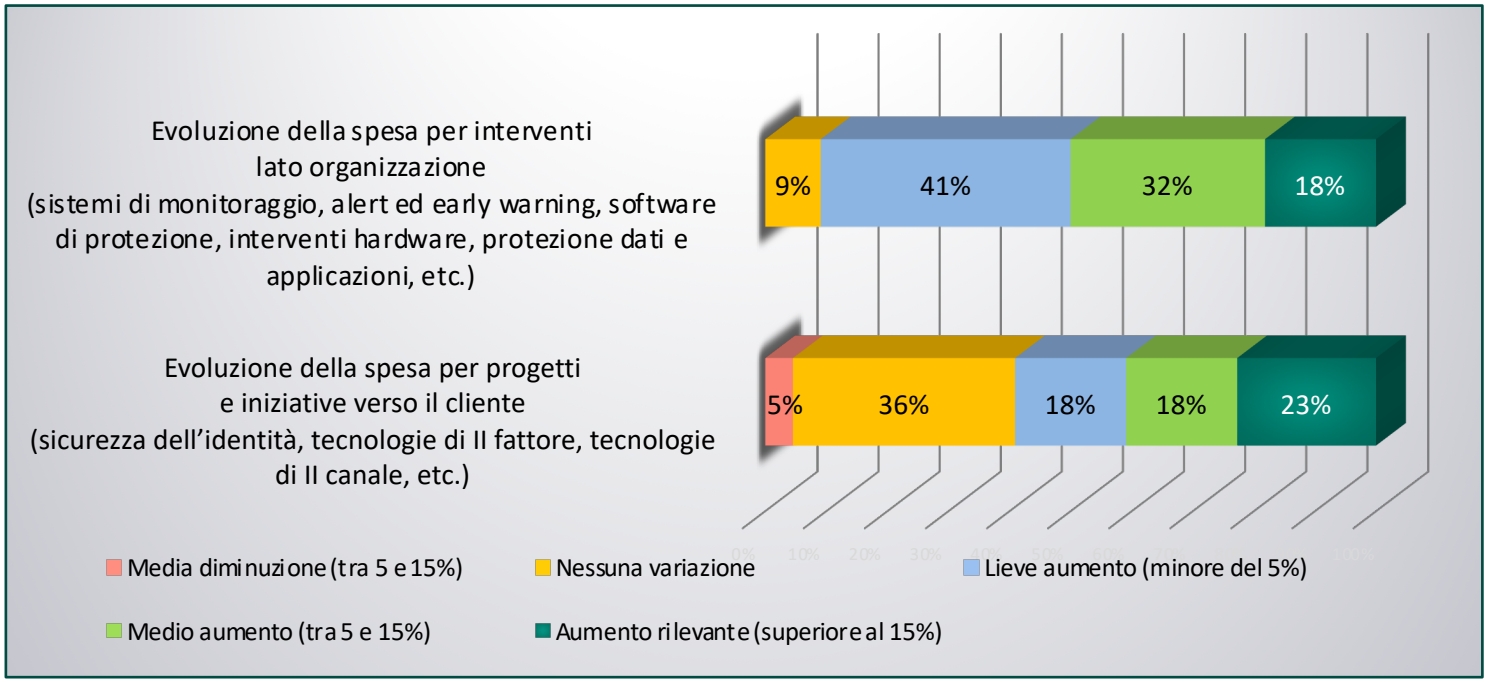
Budget dedicato alla Sicurezza

Distribuzione percentuale



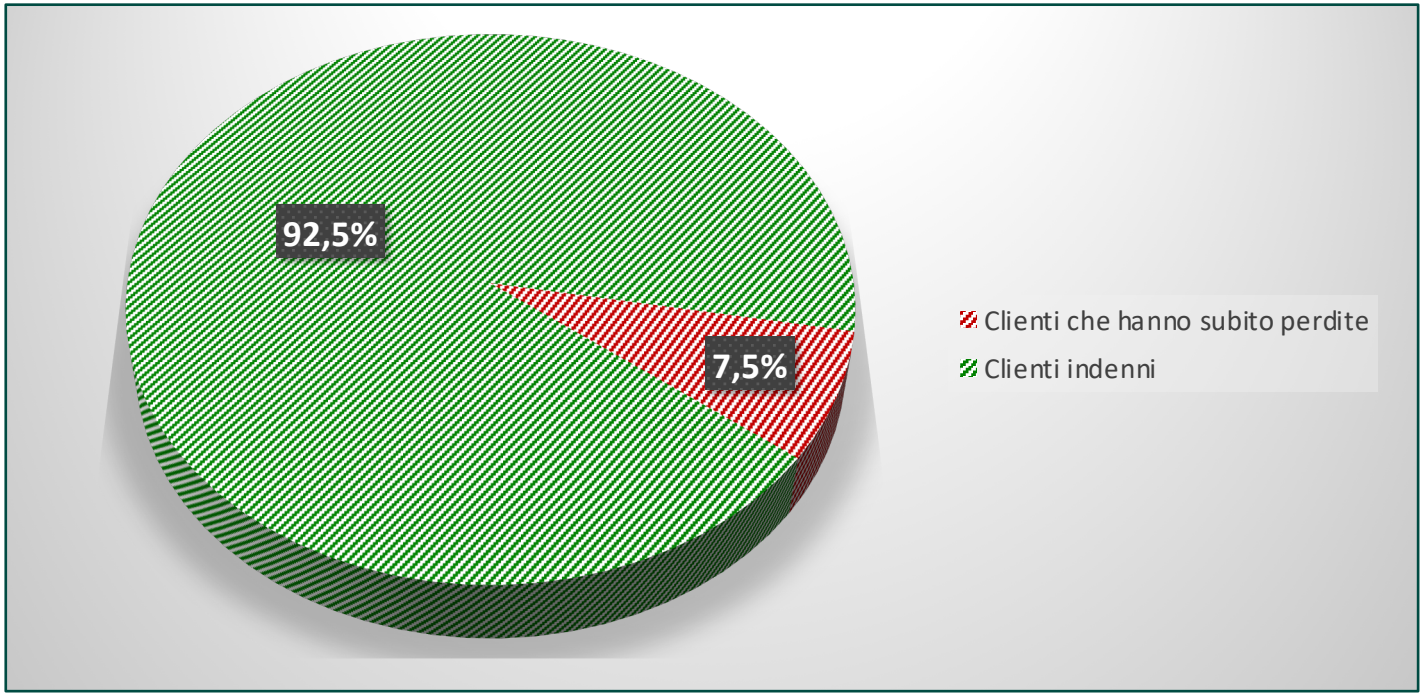
Budget dedicato alla Sicurezza

Evoluzione del livello di spesa dedicata alla sicurezza



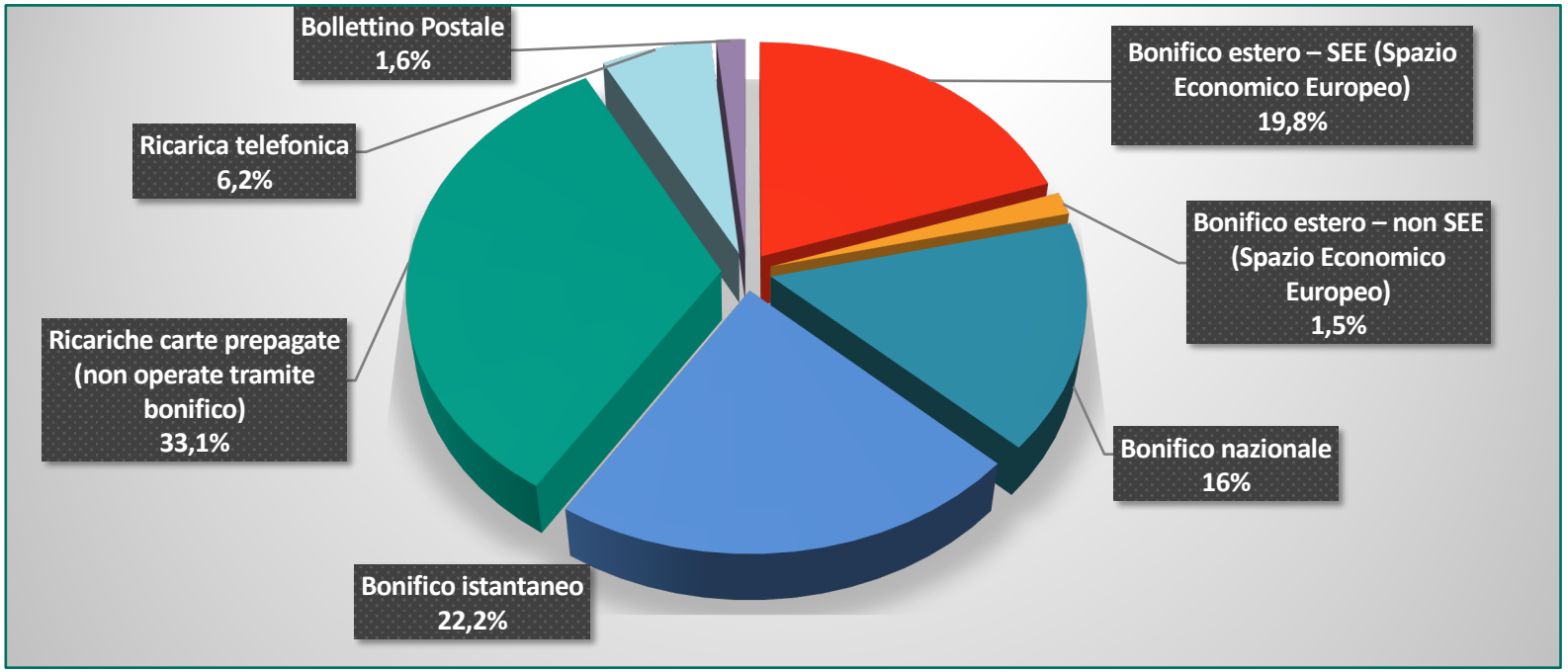
Furto di credenziali

Percentuale clienti vittime di furto di credenziali
(clientela Retail)



Transazioni Fraudolente Effettive

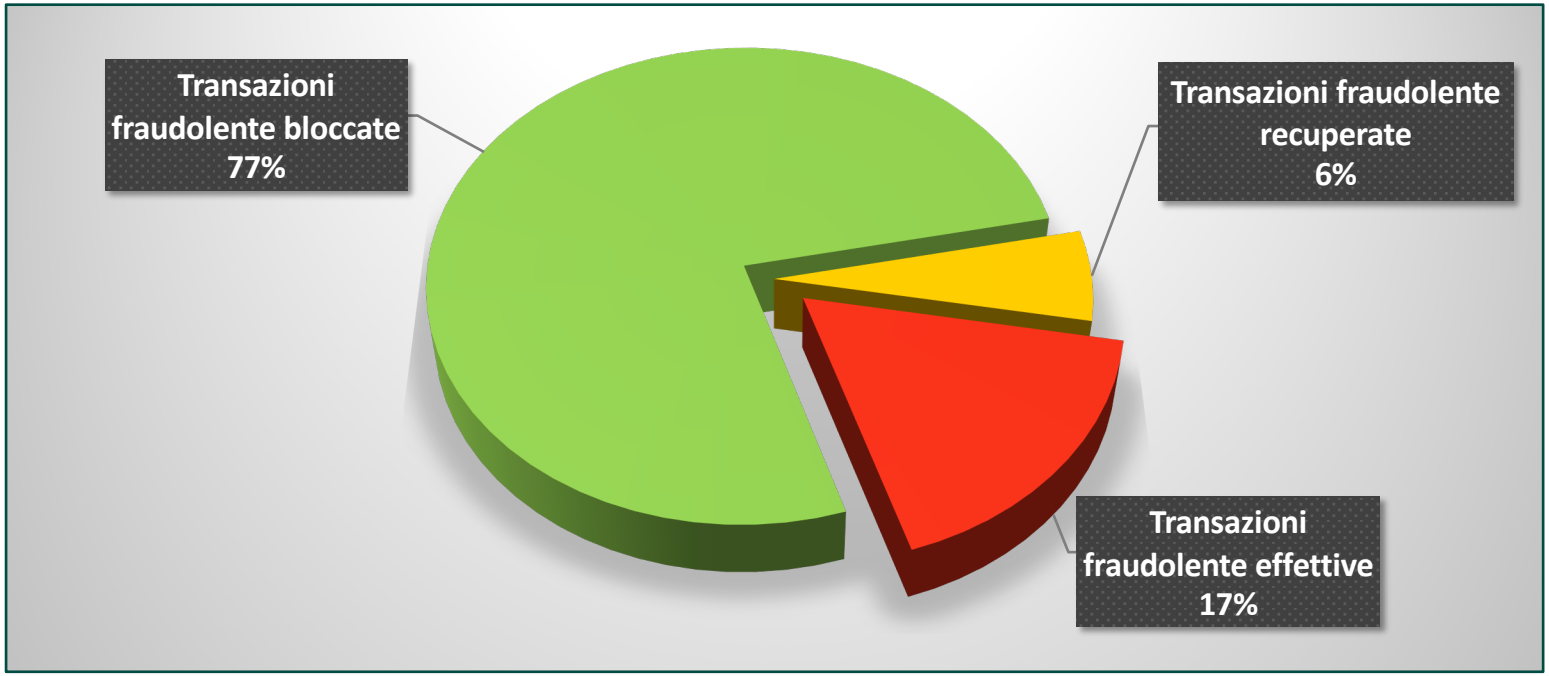
Ripartizione percentuale per tipologia – analisi sul numero di accadimenti
(segmento Retail)



Transazioni Anomale

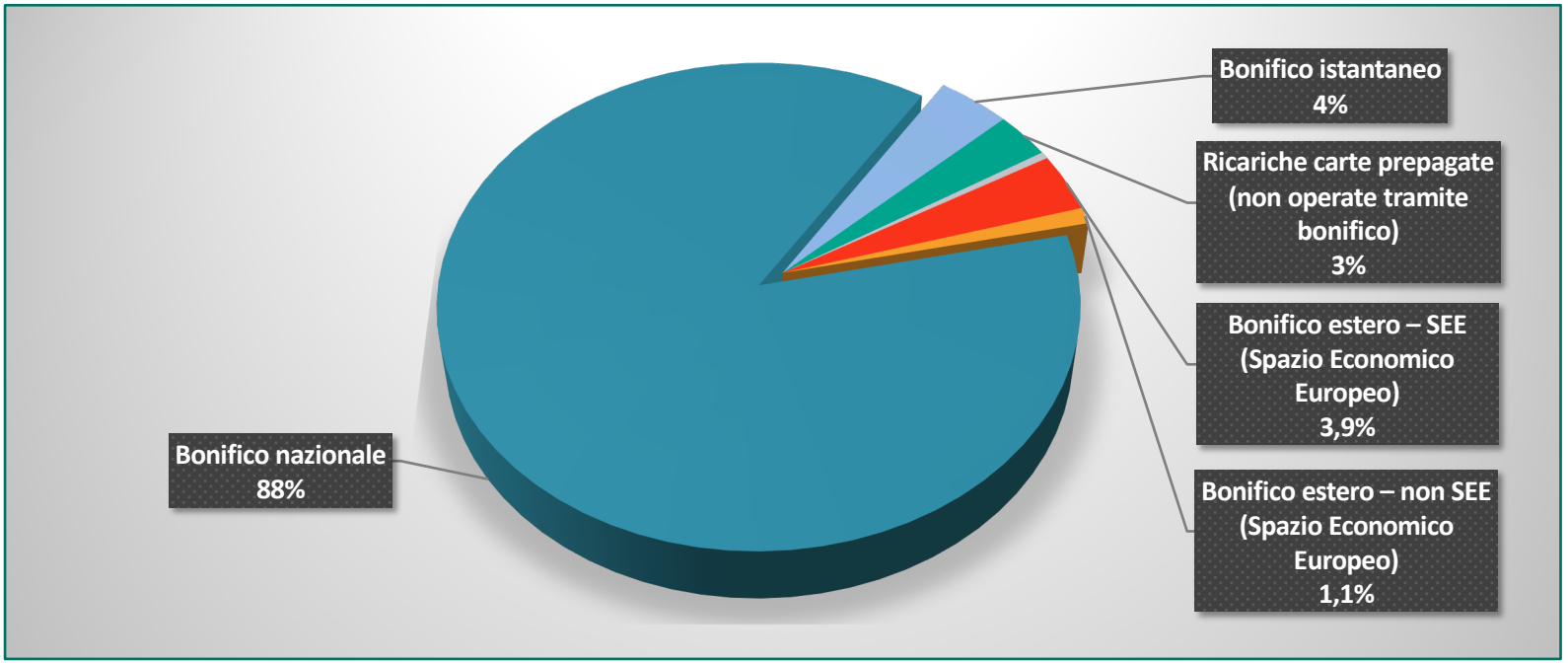
Ripartizione percentuale – analisi sul controvalore in euro

(segmento Retail)



Transazioni Fraudolente Effettive

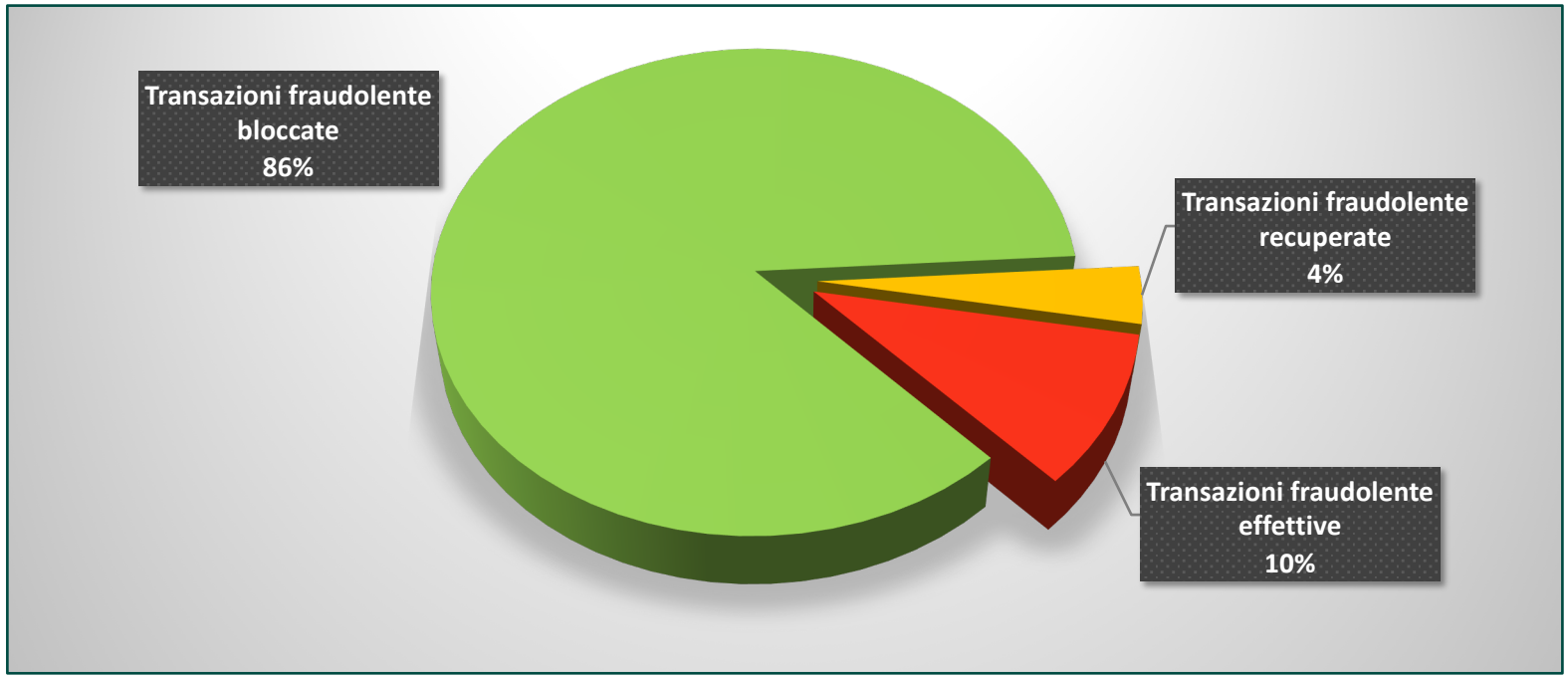
Ripartizione percentuale per tipologia – analisi sul numero di accadimenti
(segmento Corporate)



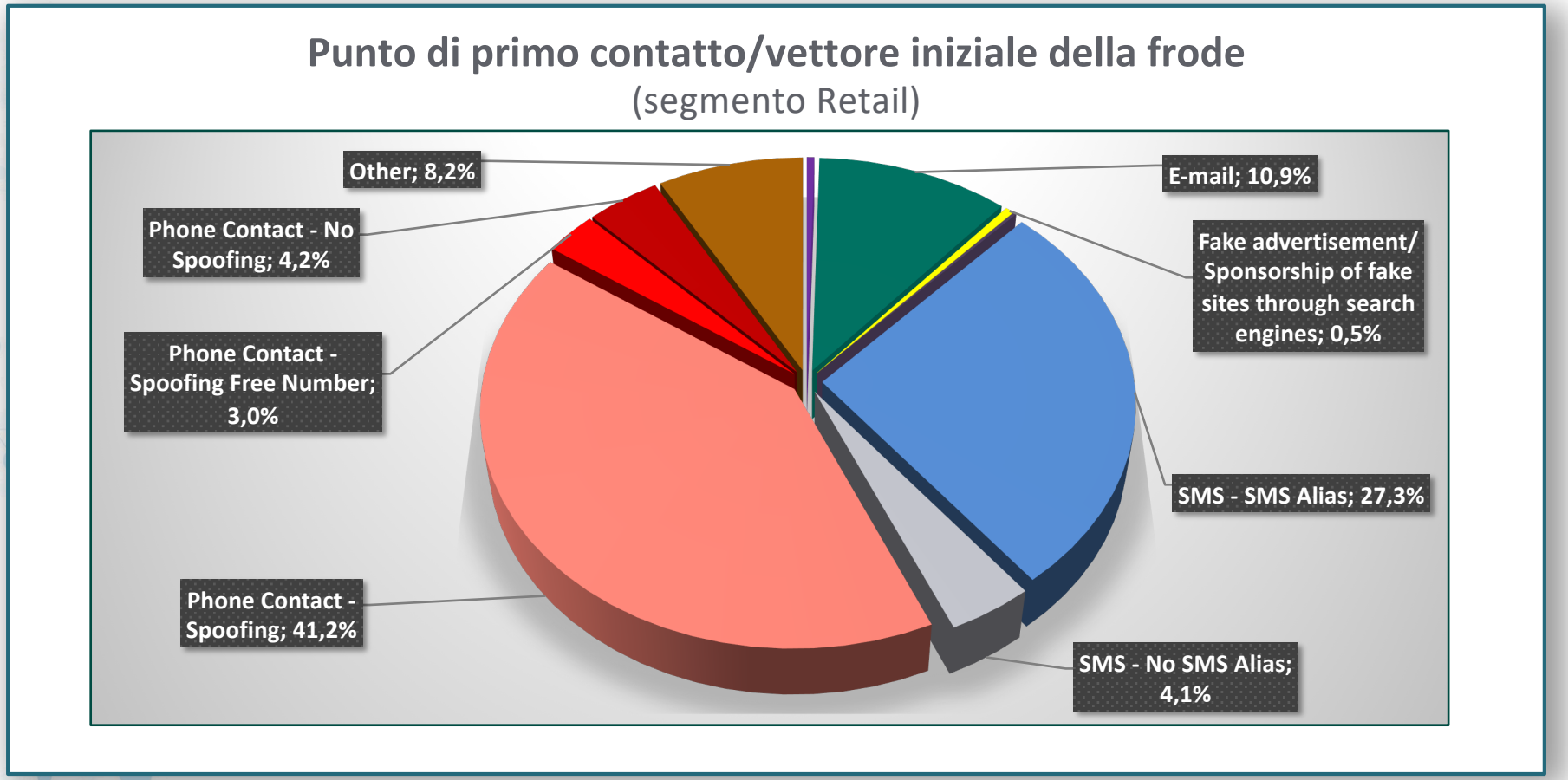
Transazioni Anomale

Ripartizione percentuale – analisi sul controvalore in euro

(segmento Corporate)

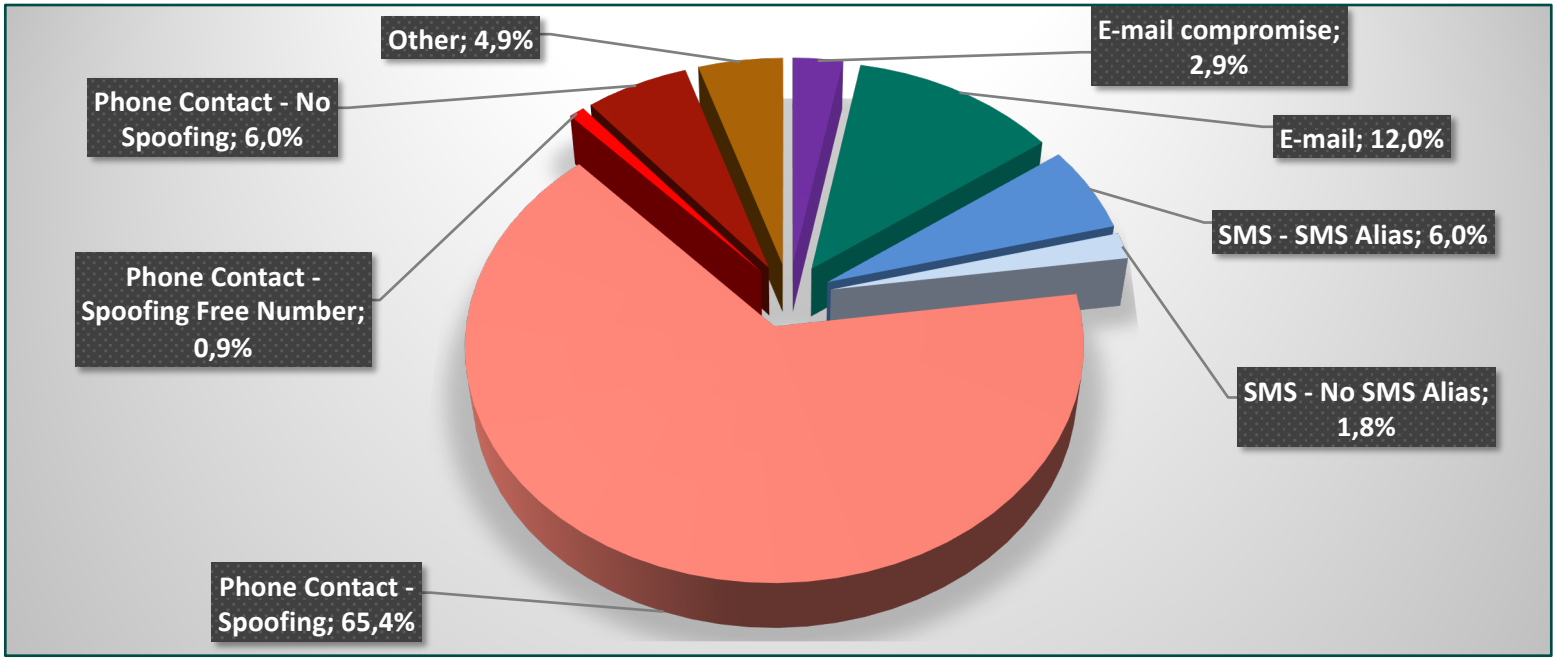


Fraud Chain


Punto di primo contatto/vettore iniziale della frode
(segmento Retail)
Other; 8,2%
E-mail; 10,9%
Phone Contact - No Spoofing; 4,2%
Fake advertisement/ Sponsorship of fake sites through search engines; 0,5%
Phone Contact - Spoofing Free Number; 3,0%
SMS - SMS Alias; 27,3%
Phone Contact - Spoofing; 41,2%
SMS - No SMS Alias; 4,1%

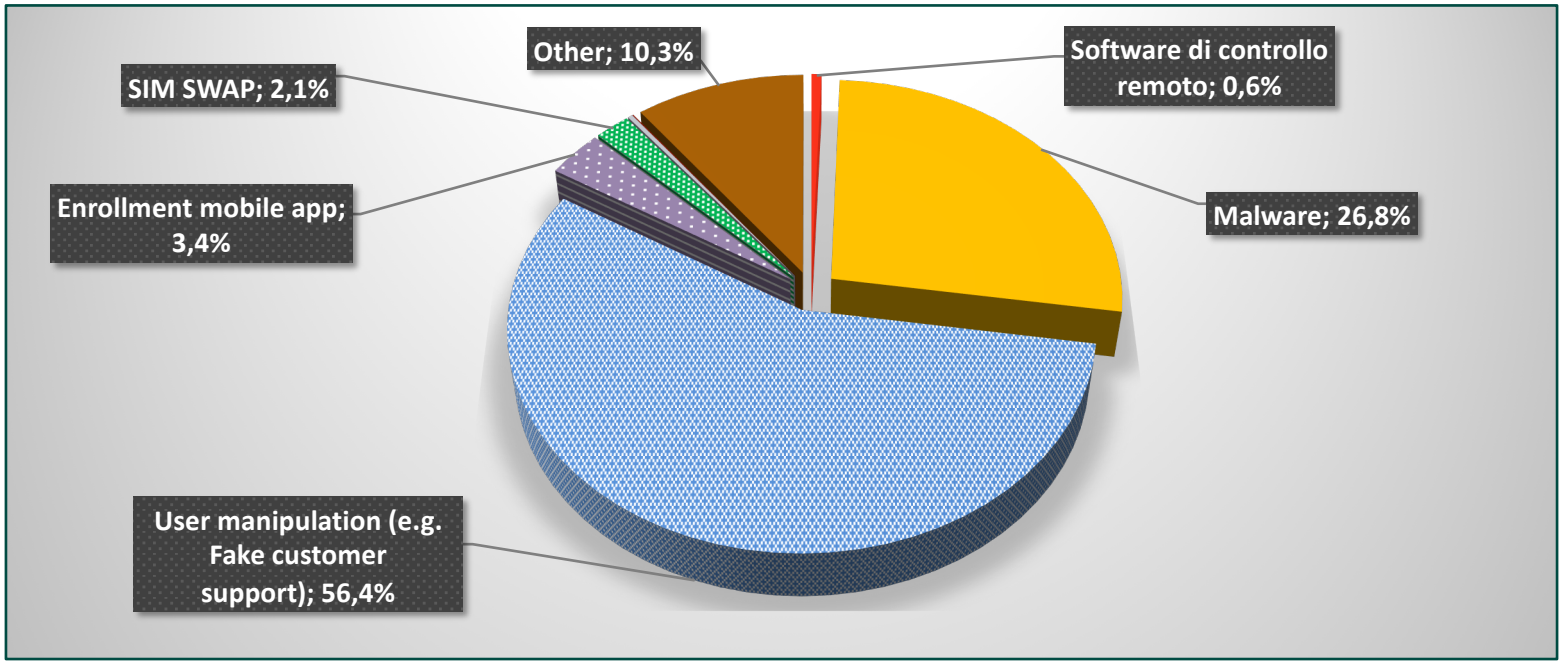
Fraud Chain

Punto di primo contatto/vettore iniziale della frode
(segmento Corporate)



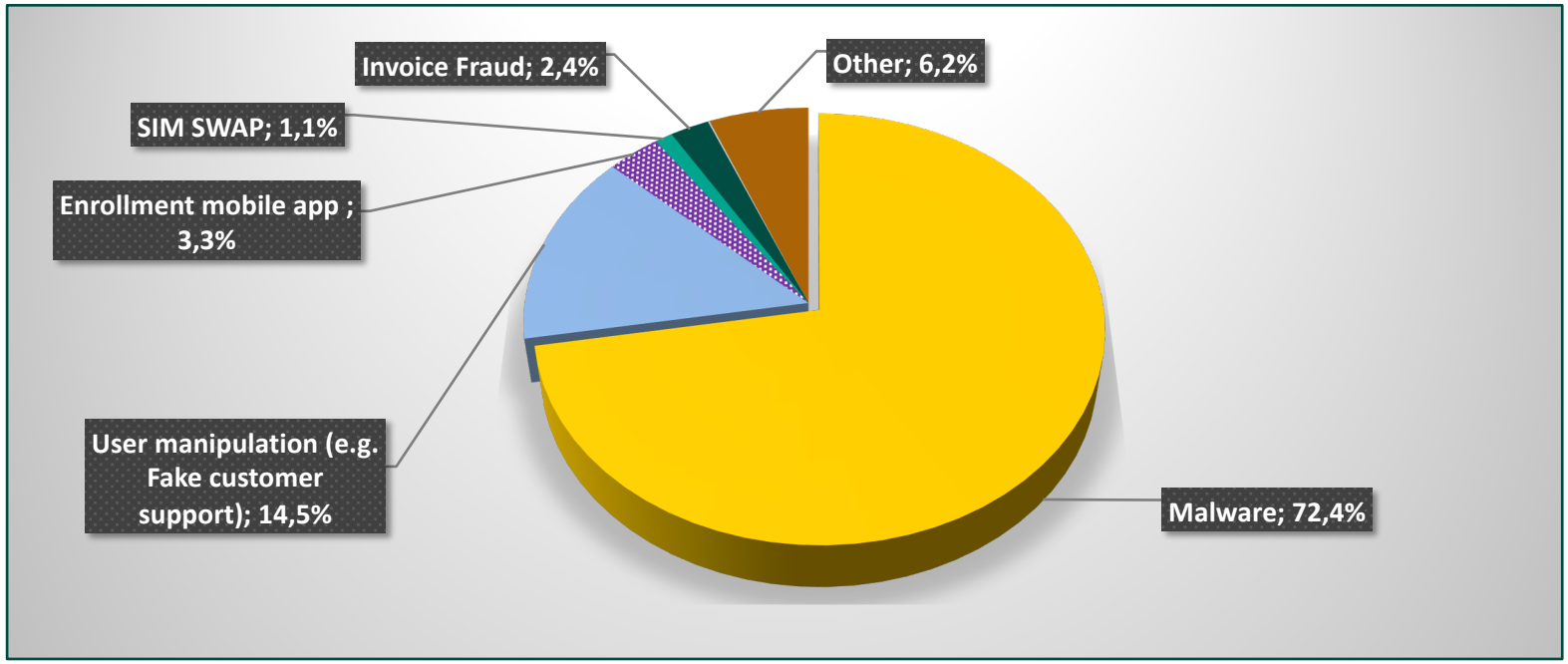
Fraud Chain

Tecnica utilizzata per finalizzare la frode
(segmento Retail)



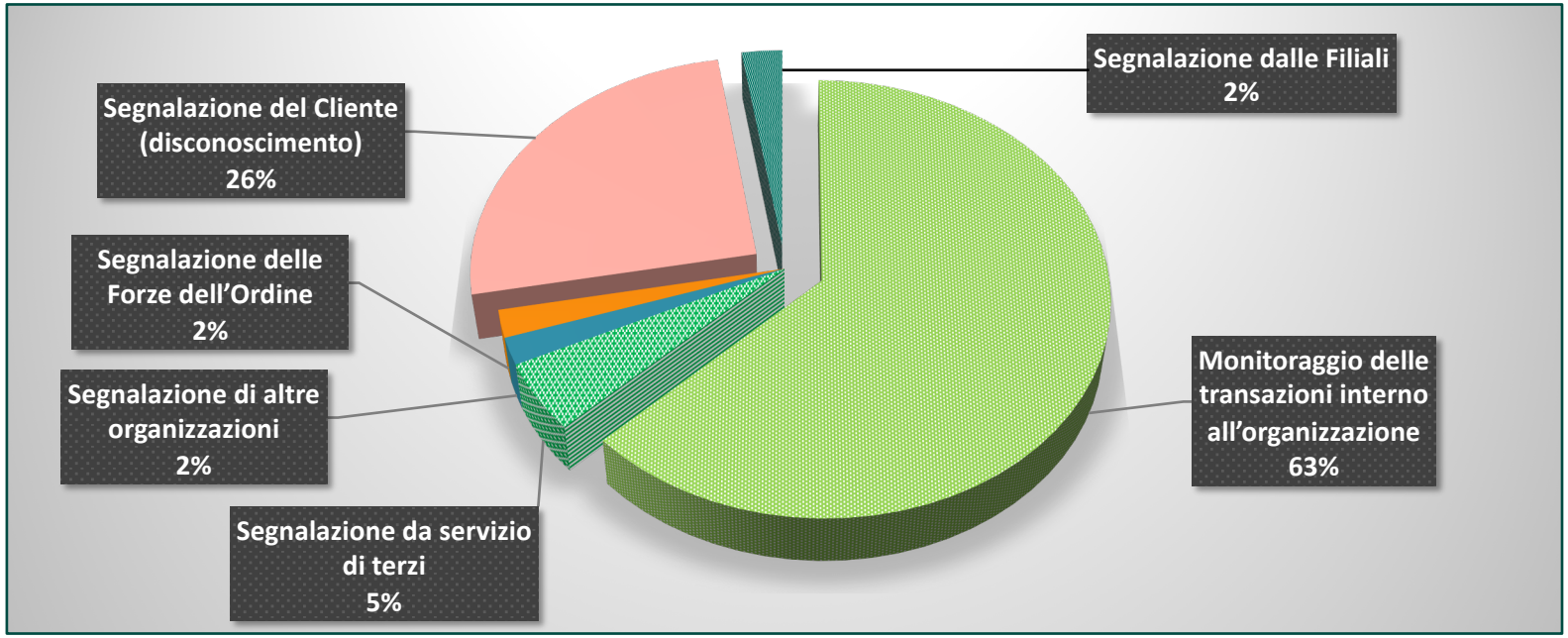
Fraud Chain

Tecnica utilizzata per finalizzare la frode
(segmento Corporate)



Fraud Detection

Fonti di segnalazione
(segmento Retail)



Caso 1:
Spoofing + Social Engineering + Malware

#0
Premessa: i frodatori sono già in possesso di alcuni dati della vittima: nome, numero di cellulare, a volte anche delle credenziali di accesso al conto.

10:37

#1
La vittima riceve una telefonata, **apparentemente proveniente dal 113**, in cui un falso agente lo avvisa che il suo conto è stato compromesso, che sono già in corso indagini e che la banca lo chiamerà a breve per riportare in sicurezza il suo conto corrente.

10:40

#2
Poco dopo, la vittima riceve una chiamata da un (falso) operatore del reparto antifrode che lo induce a disinstallare l'app della banca e ad installare un malware mascherato da tool di sicurezza.

11:02

#3
il malware inoltra tutti gli OTP ricevuti sul device della vittima ad un numero in mano ai frodatori, che in questo modo possono finalizzare un certo numero di transazioni.

***Totale**: meno di 30 minuti*

Il frodatore insinua ansia nella vittima, legittimata attraverso una comunicazione apparentemente proveniente dalle forze dell'ordine. Alla successiva chiamata, già annunciata, la vittima si «getta» nelle mani dei frodatori ed esegue senza esitare quanto gli viene detto di fare.

Caso 2:
Furto fisico + Social Engineering

#1

I frodatori sottraggono la corrispondenza contenente carte in via di rinnovo durante le varie fasi di consegna.

I criminali si ritrovano con le carte ma **non conoscono né i codici di sicurezza né i numeri di telefono delle potenziali vittime.**

#2

I frodatori, conoscendo l'indirizzo dei clienti, si recano presso le loro abitazioni ed appongono sulle cassette delle lettere **falsi adesivi DHL** che annunciano una mancata consegna ed invitano i clienti a concordarne una nuova chiamando il numero di cellulare ivi riportato.

#3

Quando il cliente chiama i frodatori memorizzano il suo cellulare e successivamente lo richiamano **inducendolo abilmente a riferire il proprio PIN**.

A quel punto i criminali procedono ad utilizzare la carta senza difficoltà.

***Totale**: variabile*

Qui i criminali mescolano reati tradizionali con reati informatici, facendo leva sulle loro abilità di social engineering per ottenere le informazioni necessarie ad operare in maniera non autorizzata.

Caso 3:
Social Engineering

#1

La vittima riceve una telefonata da un sedicente responsabile di sicurezza della propria banca. L'interlocutore la informa che il suo conto è in mano a degli hacker, che i suoi soldi sono in pericolo e che vanno **immediatamente spostati su un conto di appoggio.**

16:22

#2

Dopo alcune (false) verifiche, il frodatore comunica alla vittima che il suo device è infetto e che l'operazione di trasferimento non può essere effettuata dal device ma che **deve recarsi quanto prima allo sportello della sua filiale** per finalizzare il trasferimento verso l'IBAN «sicuro» comunicatogli nella stessa chiamata.

16:29

#3

Una volta allo sportello, l**a vittima, di suo pugno, procede a trasferire i soldi sul conto del frodatore, bypassando eventuali controlli del sistema antifrode** in quanto la disposizione avviene in presenza del cliente legittimo.

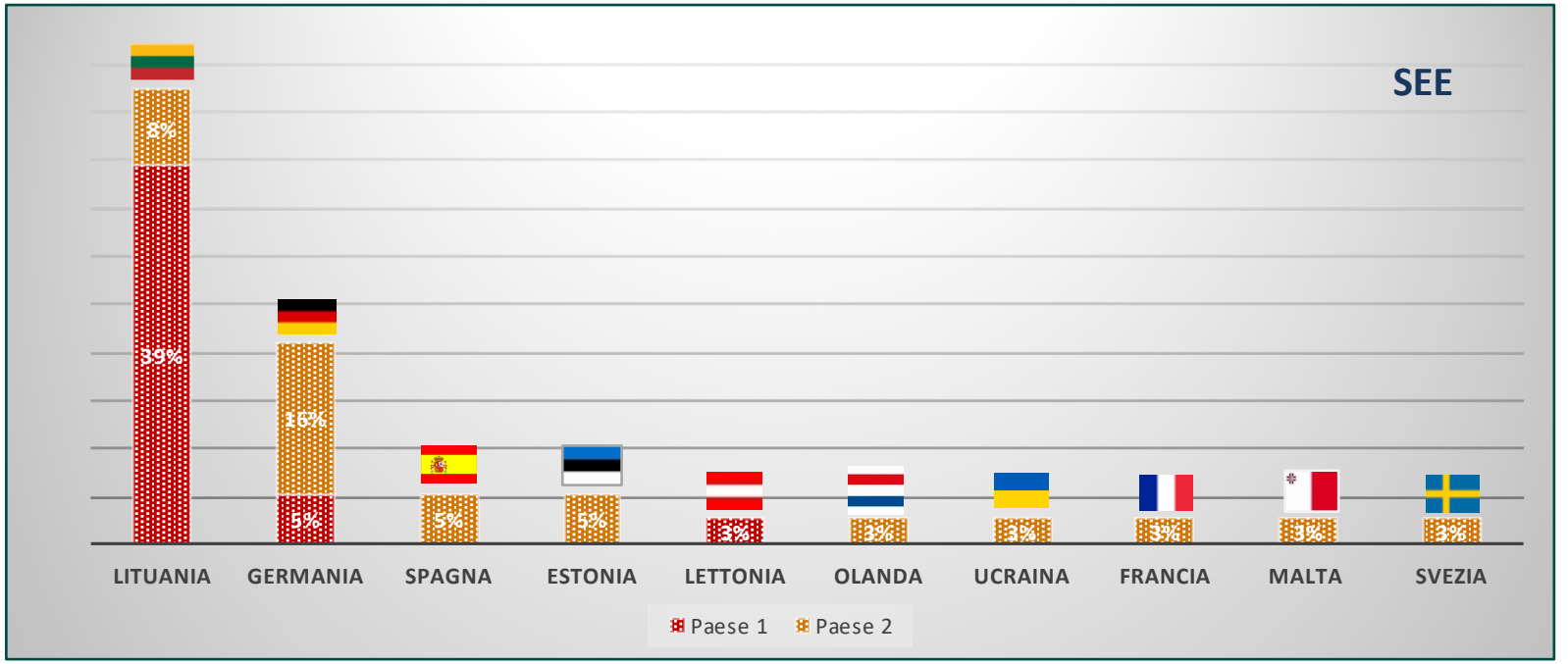
17:06

***Totale**: circa 45 minuti*

Diversamente dal passato, la tecnica di social engineering è assai aggressiva. Nei casi in cui l'operatore di sportello, o anche il Direttore di filiale, suggeriscono cautela al cliente, il frodatore si fa passare al telefono il personale di banca e non si risparmia in minacce ed intimidazioni verso di loro.

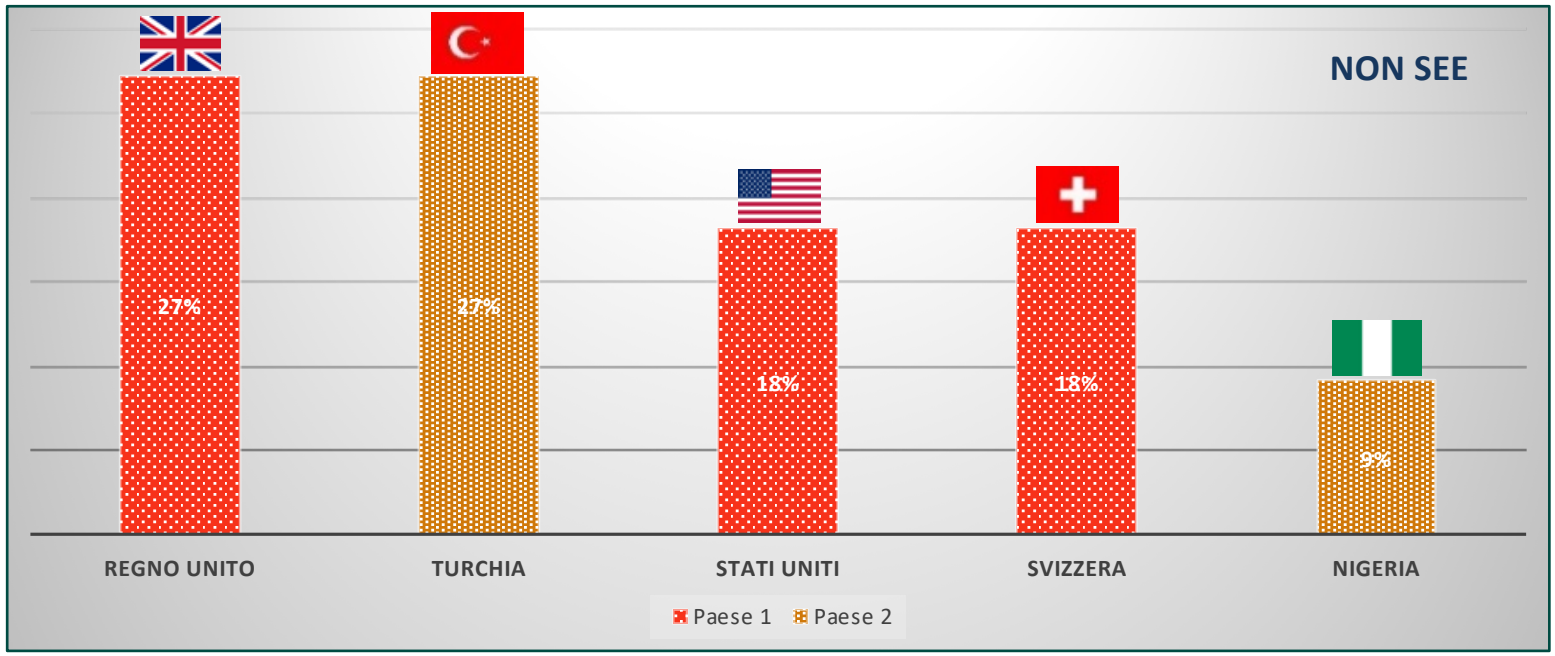
Distribuzione Geografica

Elenco, in ordine percentuale, dei Paesi destinatari di bonifici fraudolenti



Distribuzione Geografica

Elenco, in ordine percentuale, dei Paesi destinatari di bonifici fraudolenti



Thank You!

CERTFin

Defend. Inform. Evolve.

For more info visit www.certfin.it or write to ricerca@certfin.it