



**CERTFin**

# **Sicurezza e Frodi in Banca Report 2023**

16 maggio 2023



**Mario Trinchera**  
*Technical Coordinator*

**TLP: GREEN**

Nel retail aumenta il controvalore delle frodi tentate



*Rispetto allo scorso anno*

Si riduce la quota di Frodi Effettive sul totale transazioni anomale



...e, significativamente, anche il loro controvalore



*Rispetto allo scorso anno*

La transazioni fraudolente effettive sono spesso avviate dal cliente

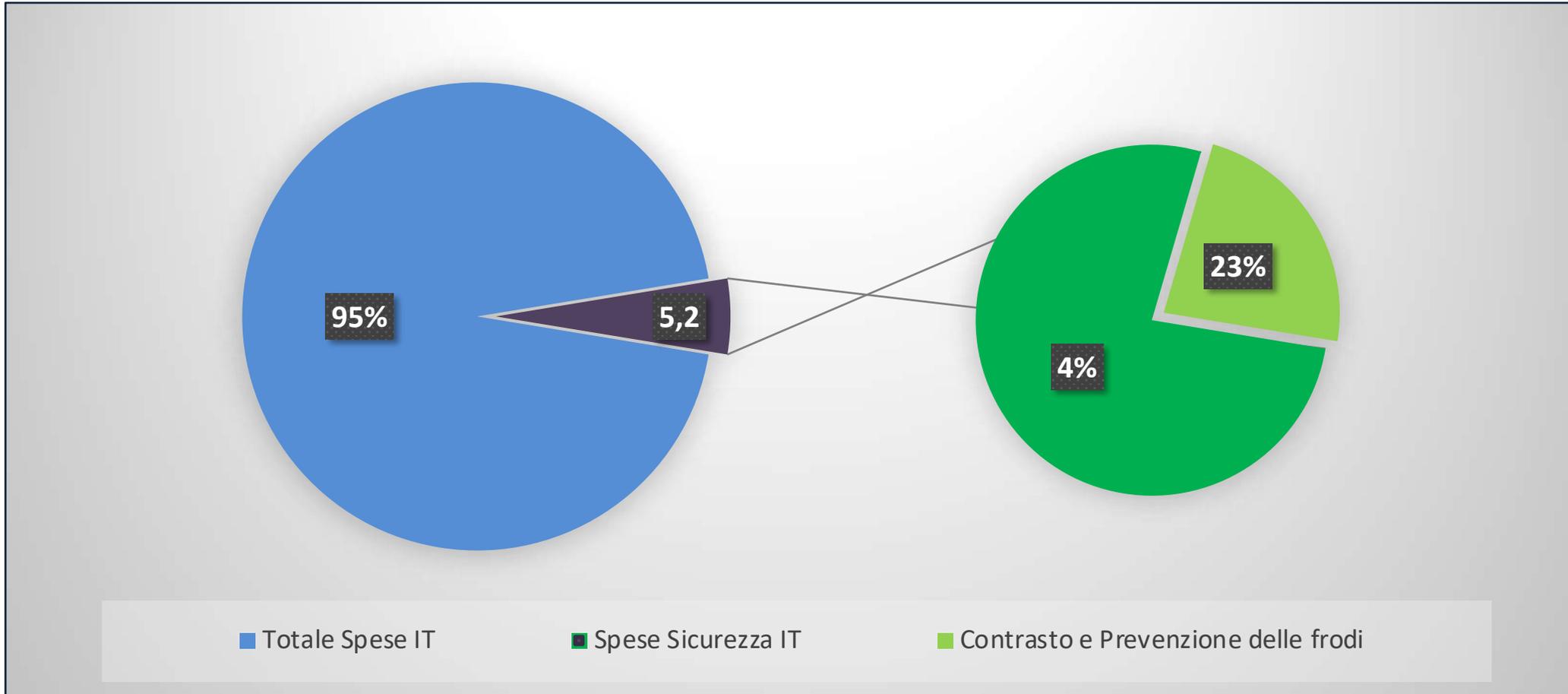


Ancora molto elevato l'importo delle frodi «recuperate»

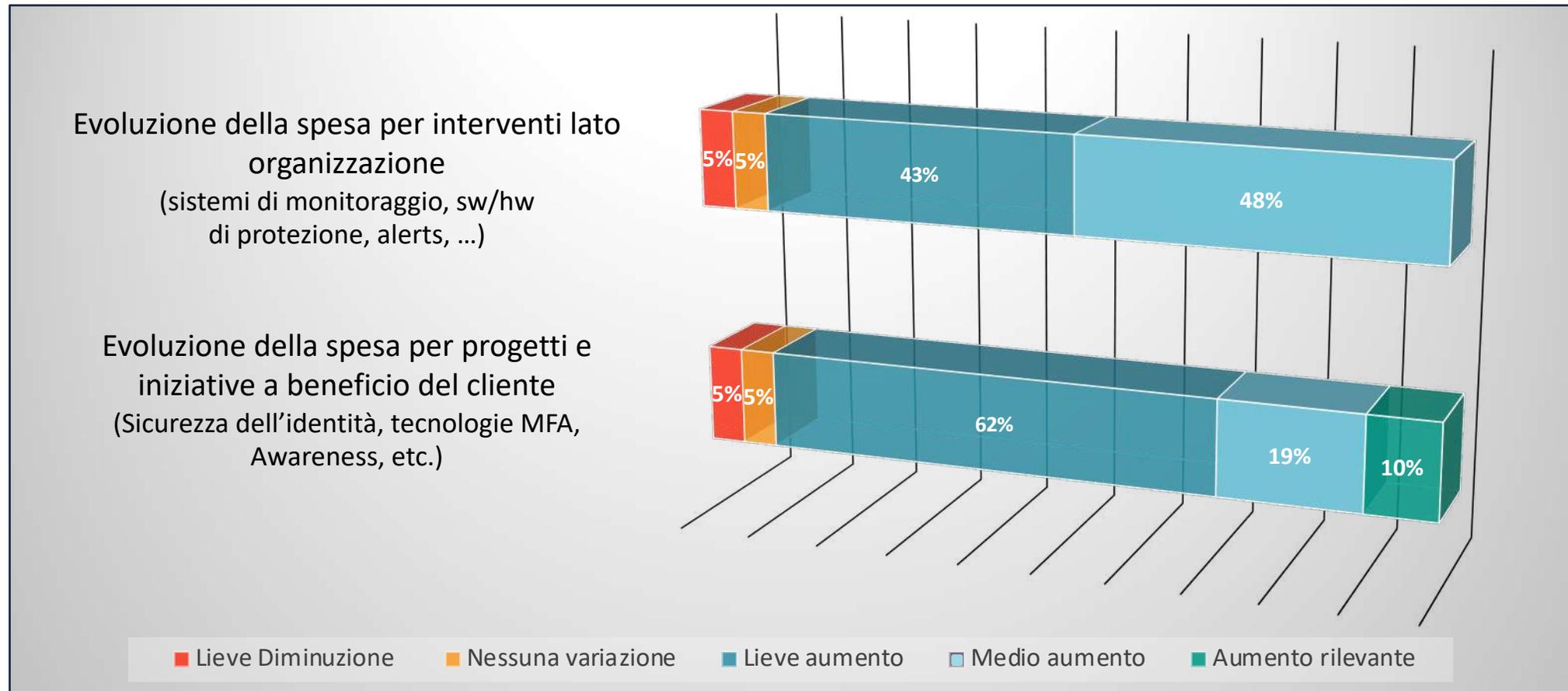


*Milioni di euro*

## Distribuzione percentuale

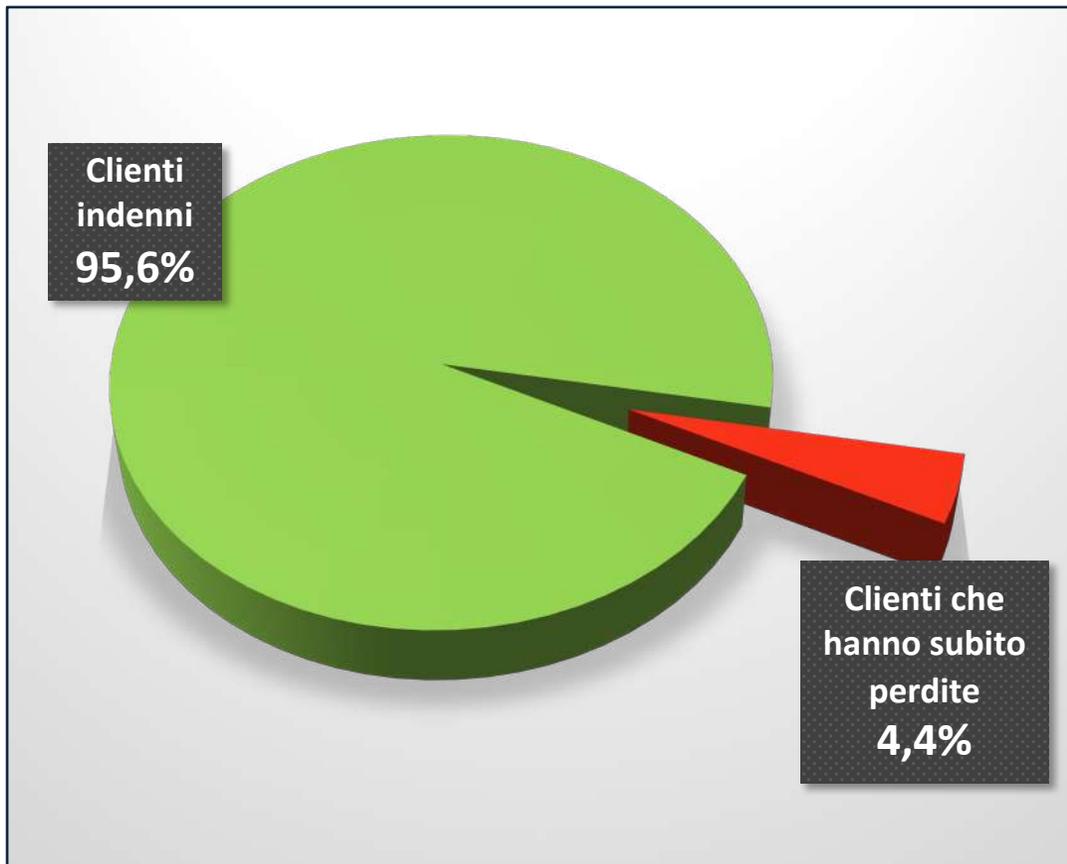


## Evoluzione del livello di spesa dedicata alla sicurezza

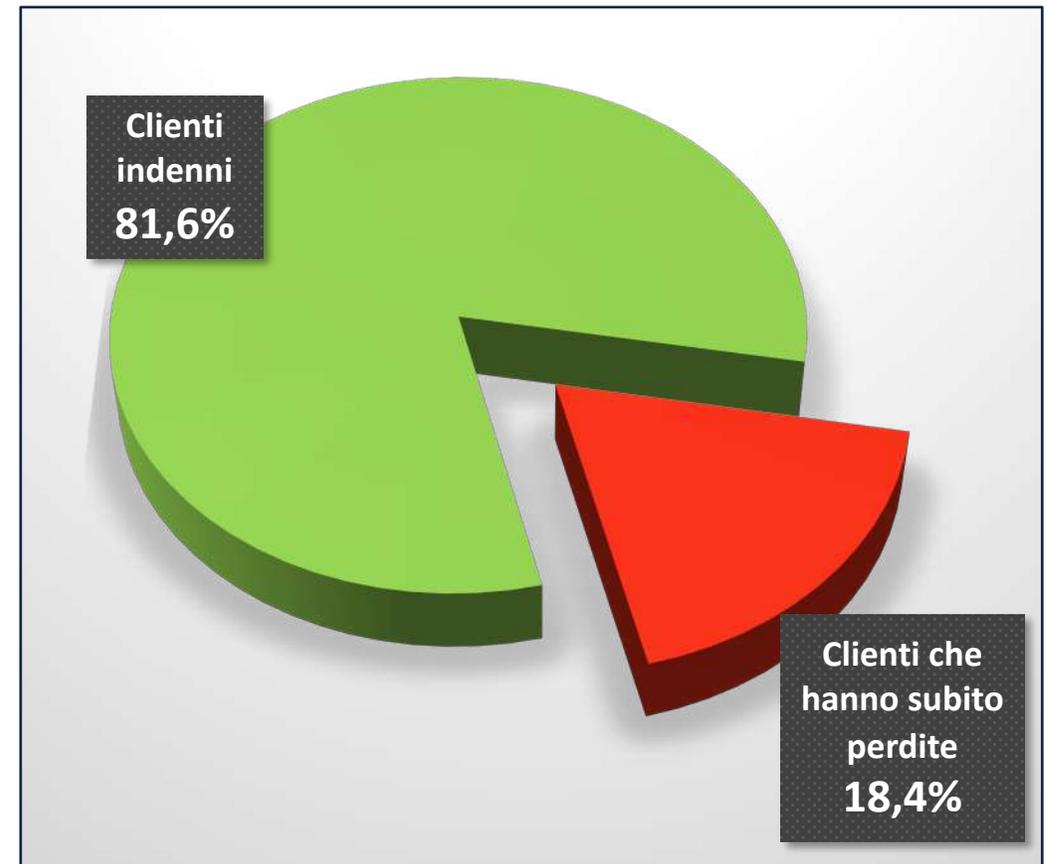


## Clienti vittime di furto di credenziali

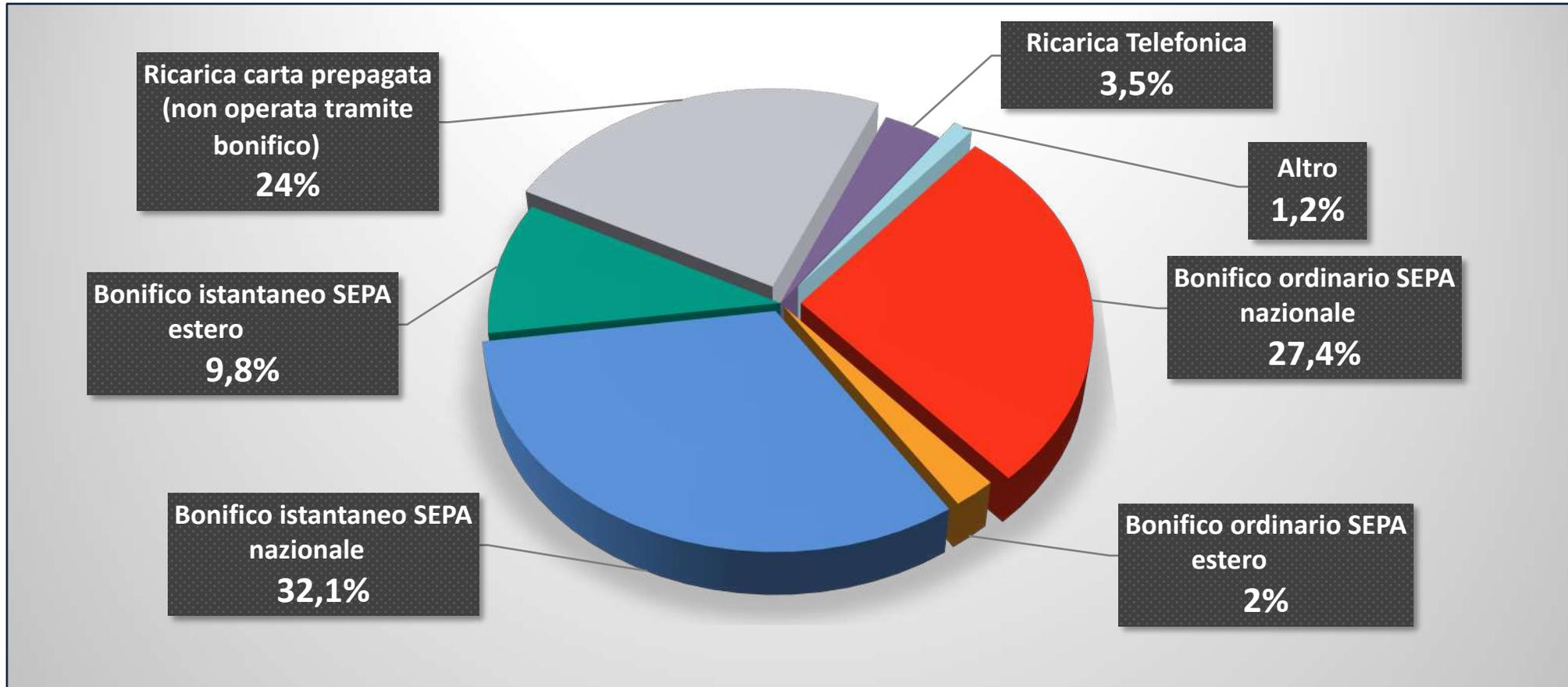
### Retail



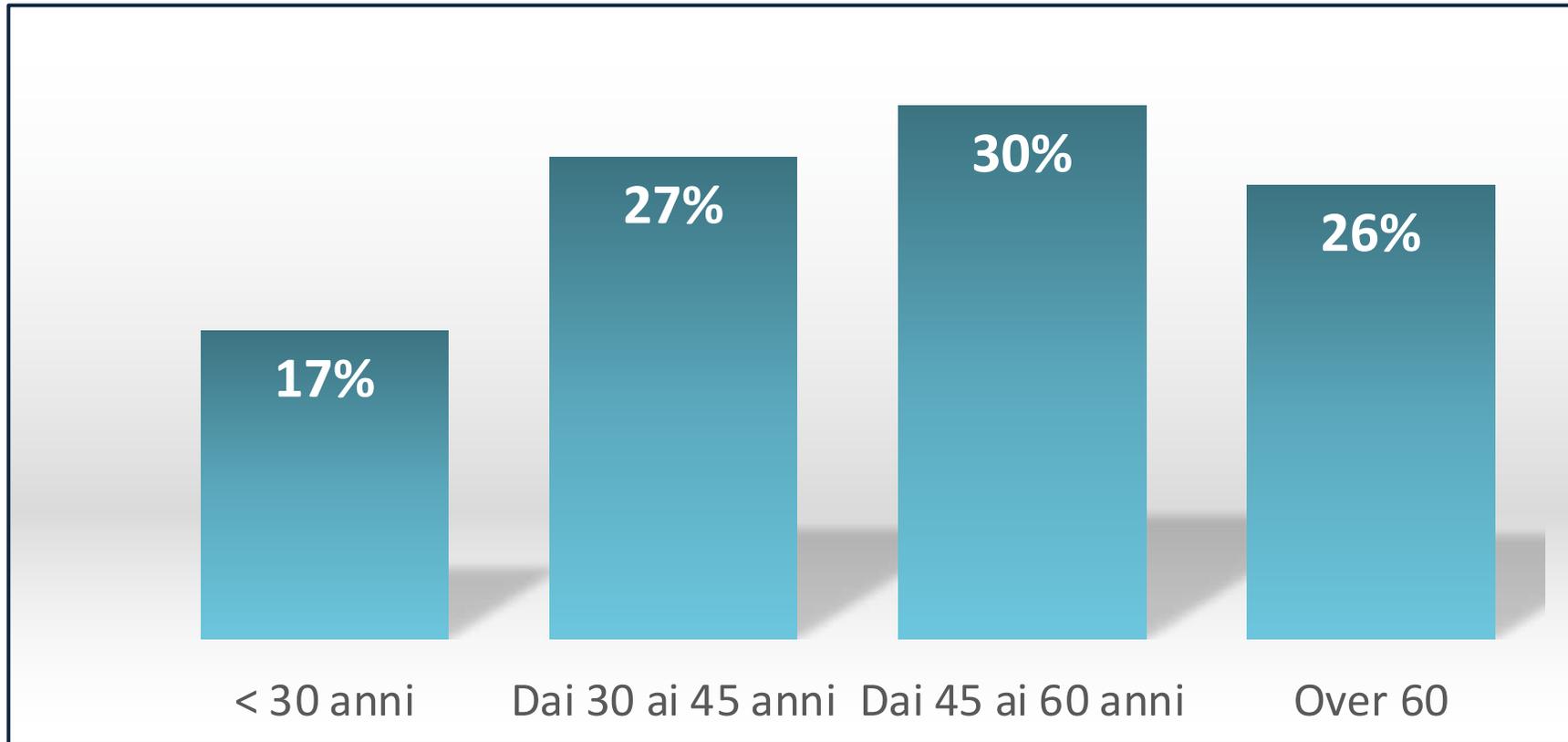
### Corporate



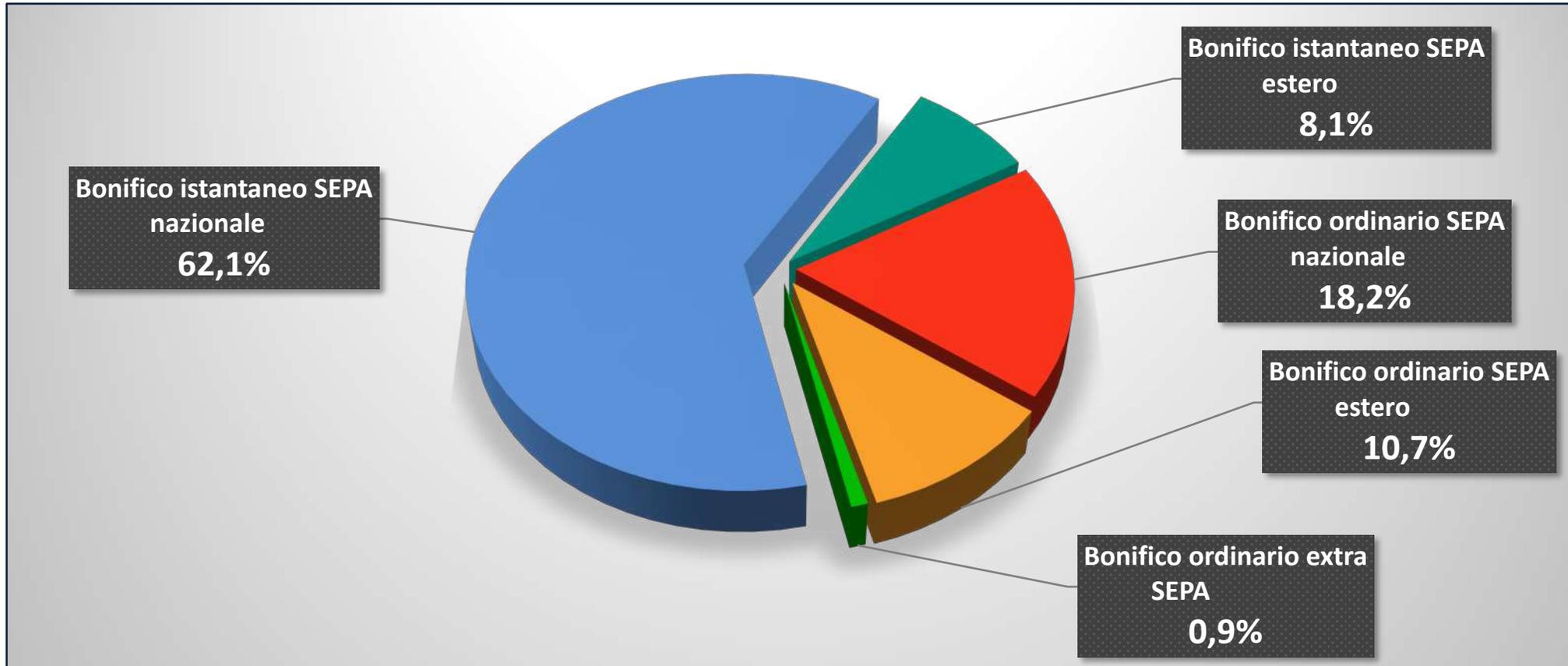
## Ripartizione percentuale per tipologia – analisi sul numero di accadimenti (segmento Retail)



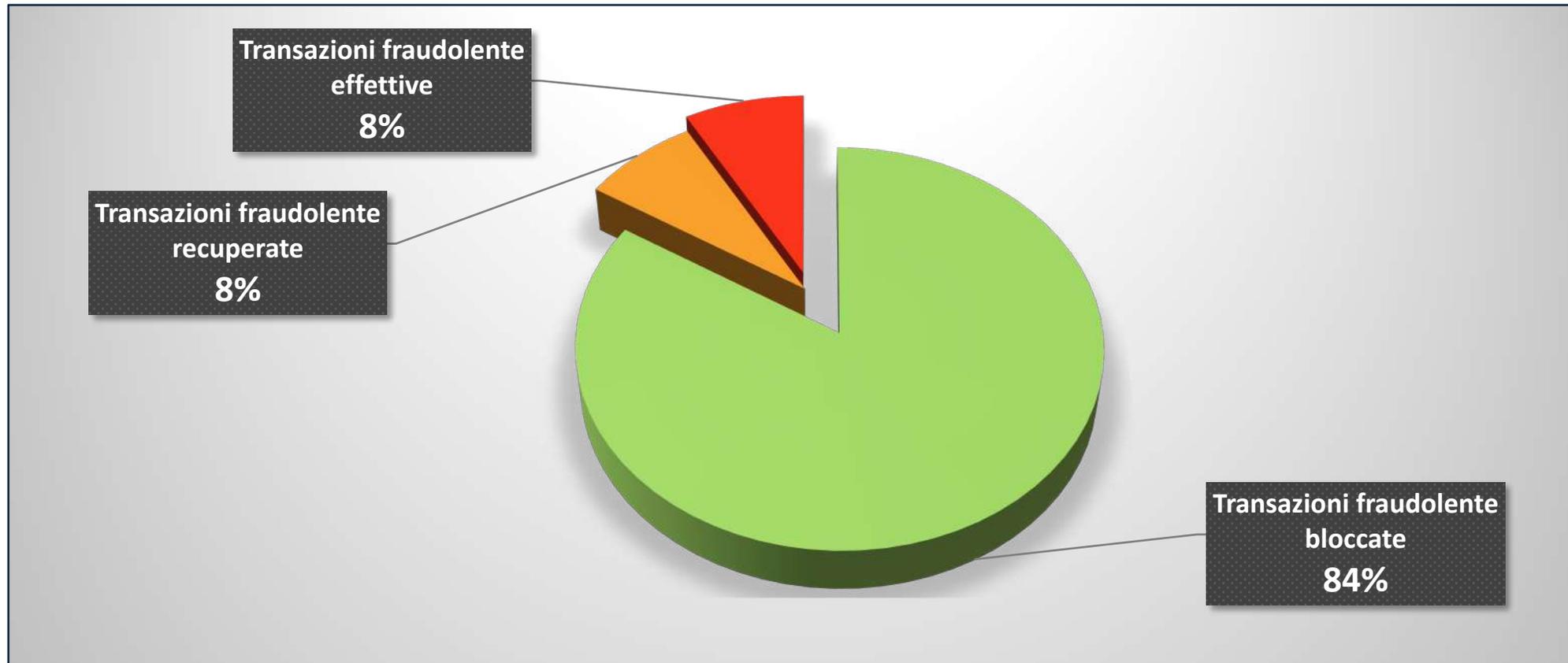
## Ripartizione percentuale per fascia d'età – analisi sul numero di accadimenti (segmento Retail)



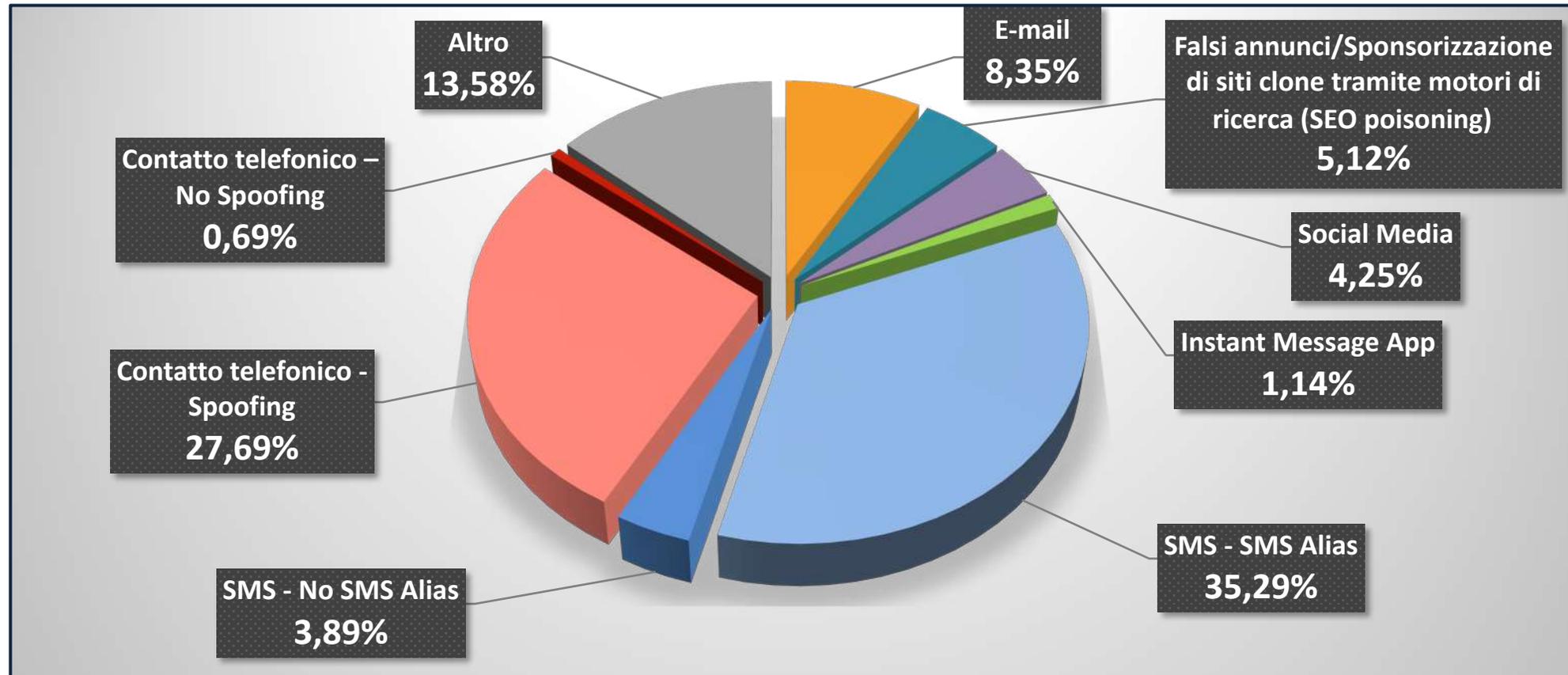
## Ripartizione percentuale per tipologia – analisi sul numero di accadimenti (segmento Corporate)



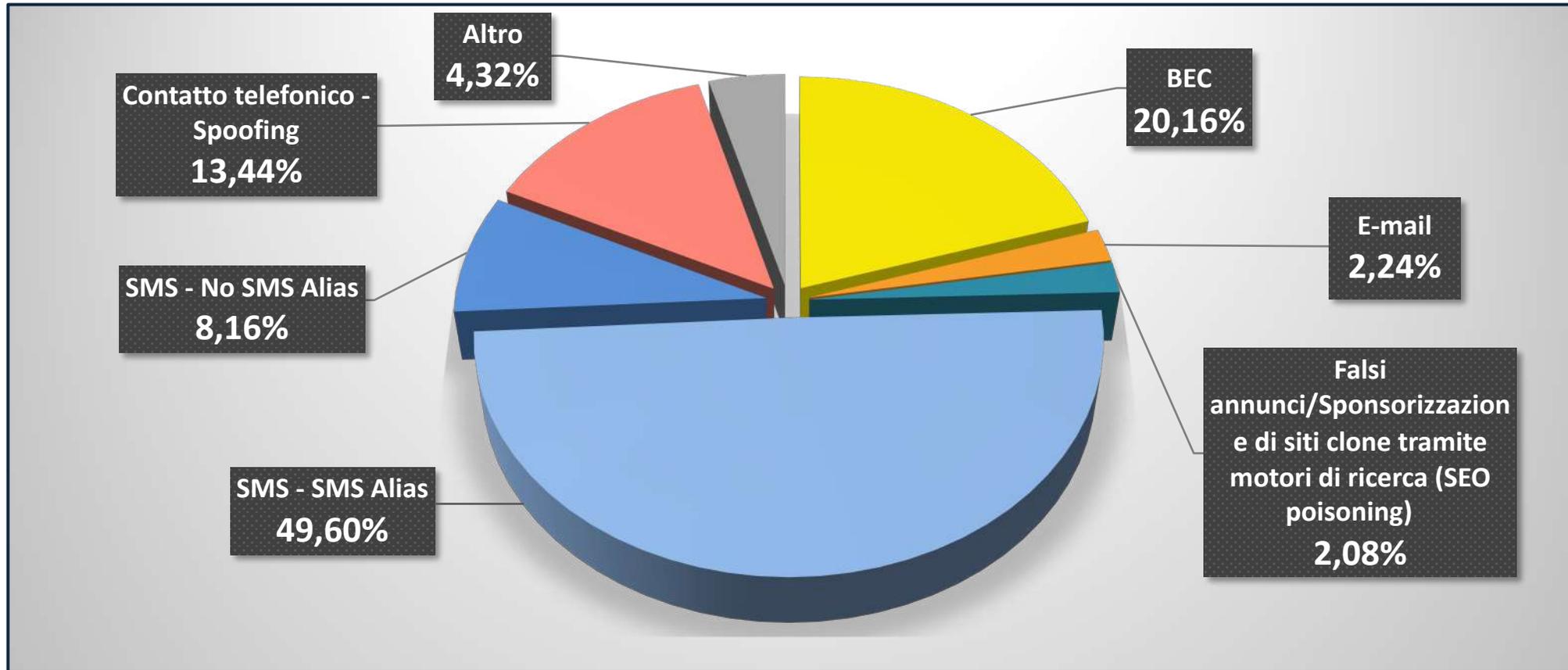
## Ripartizione percentuale – analisi sul controvalore in euro (complessivo Retail e Corporate)



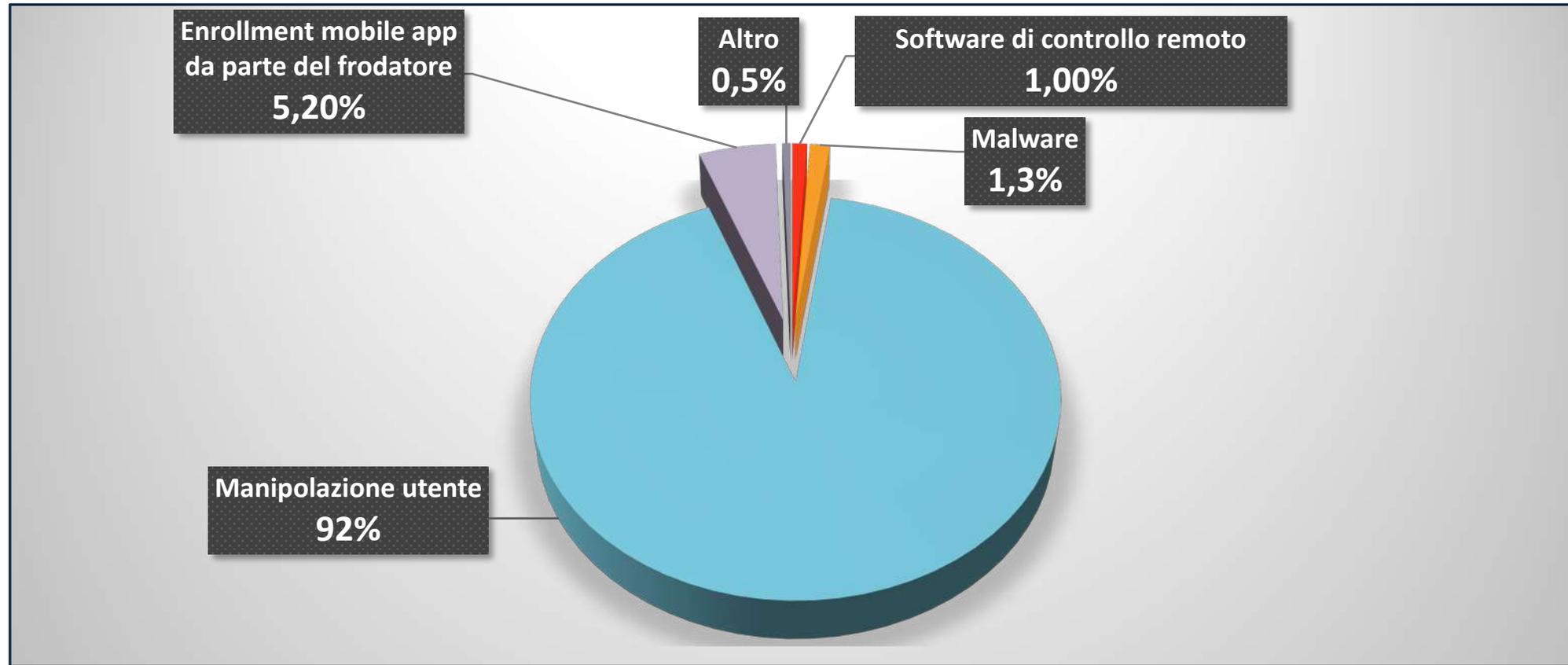
## Punto di primo contatto/vettore iniziale della frode (segmento Retail)



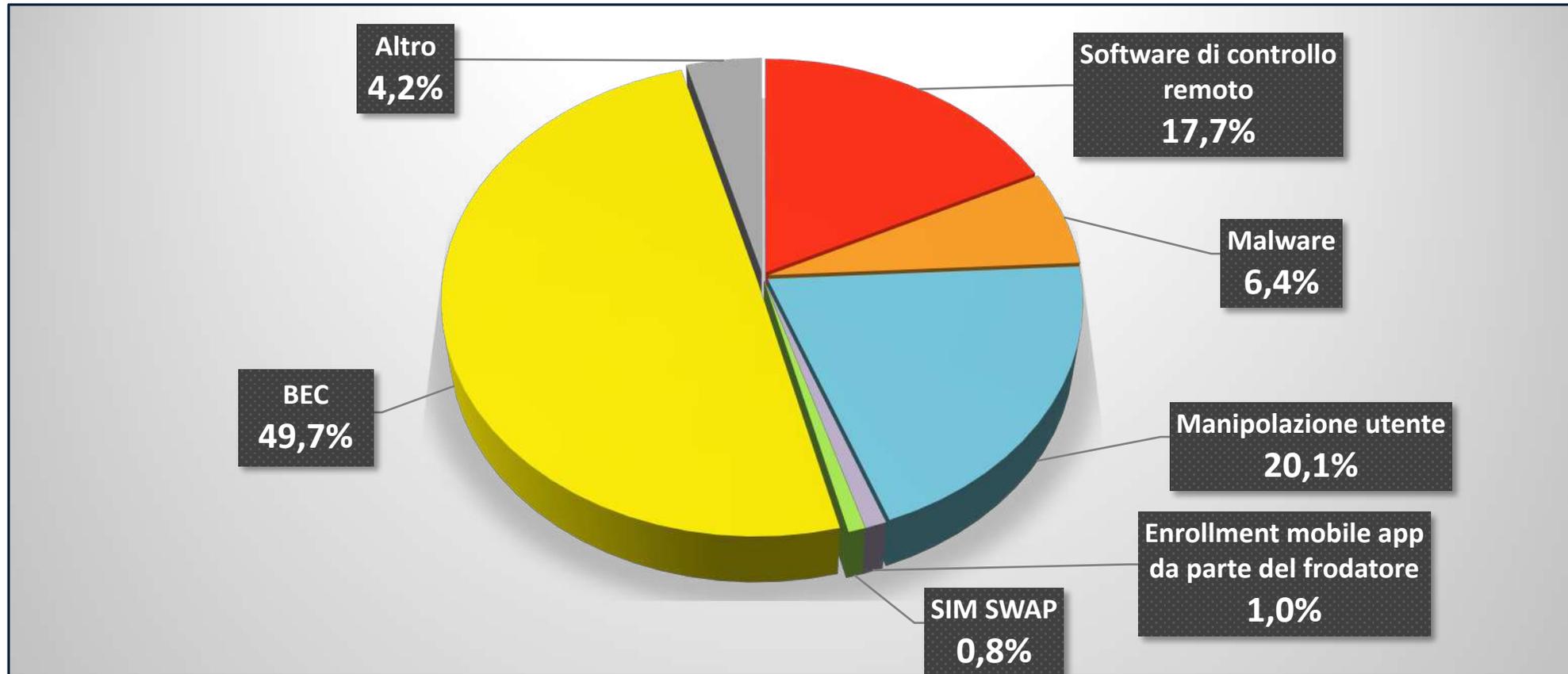
## Punto di primo contatto/vettore iniziale della frode (segmento Corporate)



## Tecnica utilizzata per finalizzare la frode (segmento Retail)

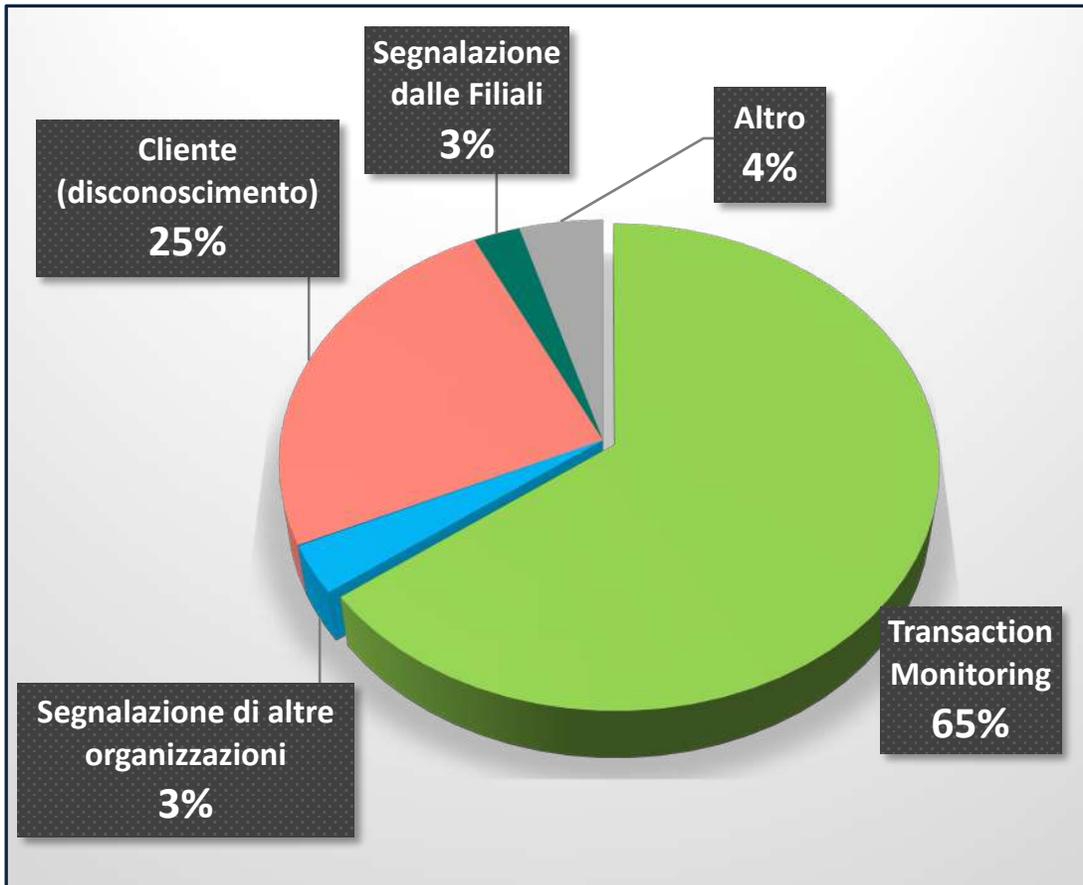


## Tecnica utilizzata per finalizzare la frode (segmento Corporate)

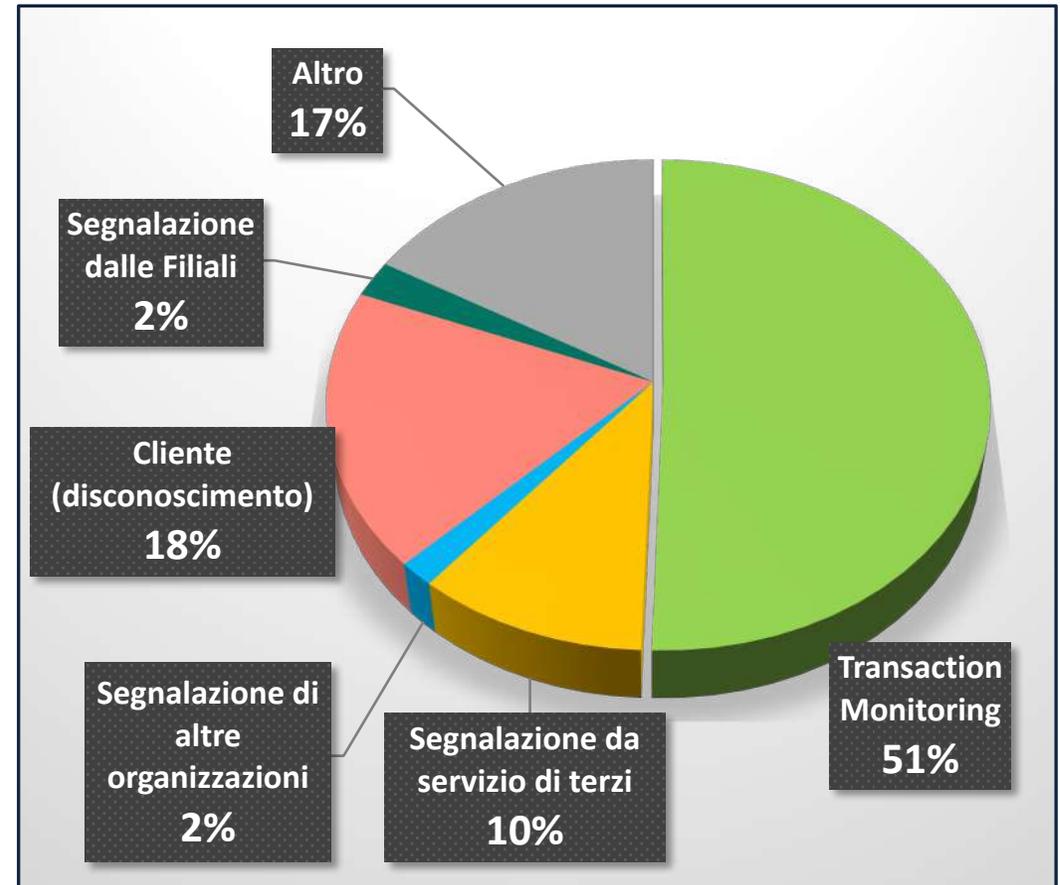


## Fonti di segnalazione

### Retail

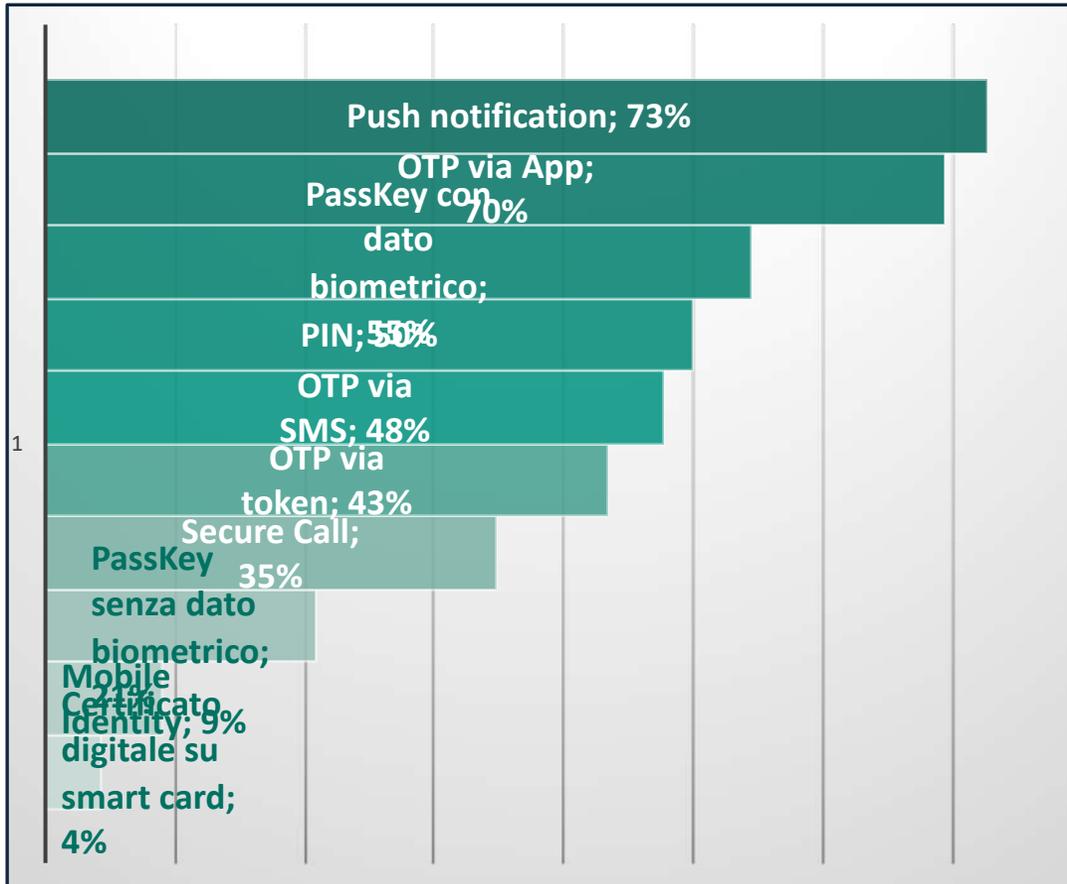


### Corporate

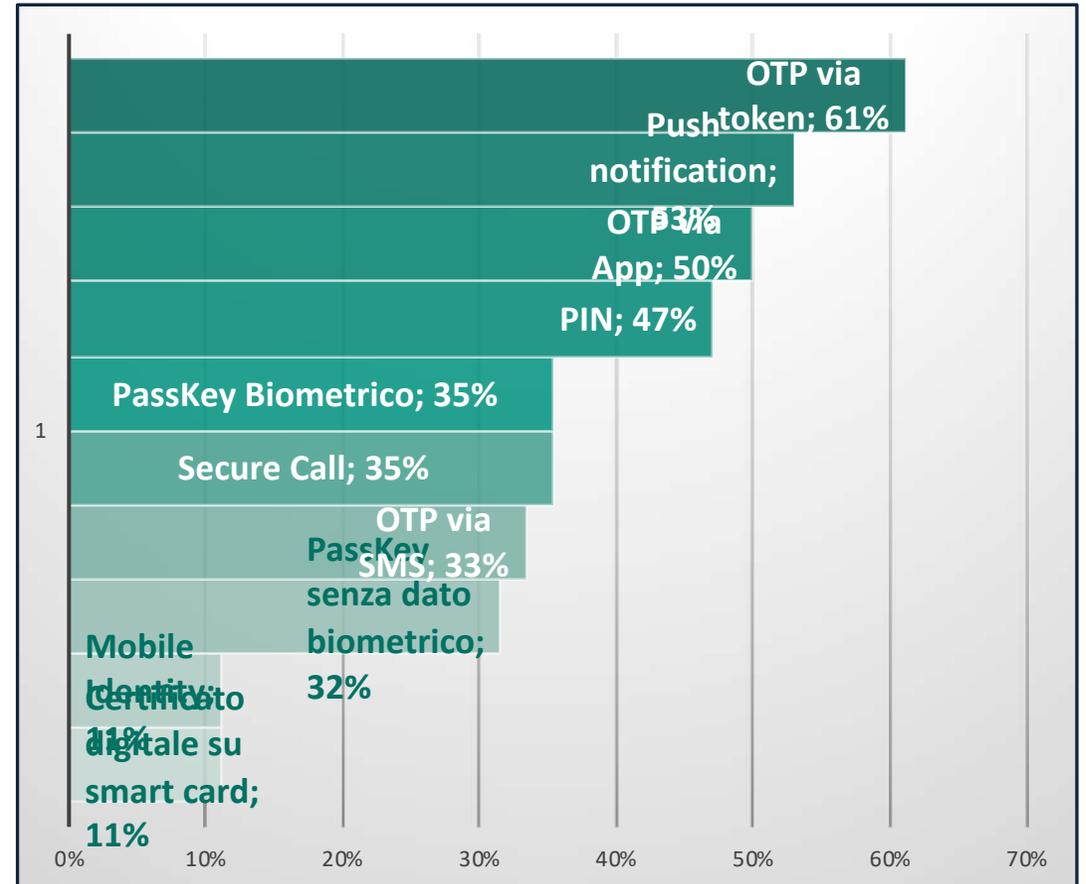


## Livello di diffusione

### Retail



### Corporate





## #1

La vittima riceve una telefonata apparentemente proveniente dalla sua banca durante la quale un sedicente responsabile di sicurezza lo 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.**



## #2

La vittima, colta dal panico, si affretta a seguire le indicazioni fornite dal falso operatore di banca, tra cui vi è anche l'IBAN sul quale versare «temporaneamente» i soldi che saranno così messi «al sicuro».

## #3

L'agitazione della vittima richiama però l'attenzione della moglie la quale si fa spiegare cosa sta accadendo e si unisce all'angoscia del marito. Il fraudatore a quel punto **chiede se anche la signora ha un c/c presso la stessa banca**, in modo da poter effettuare una verifica anche sul suo conto.

***Durata Totale: 70 minuti circa***

## #4

Alla risposta affermativa, la dinamica viene replicata: **il fraudatore riferisce che purtroppo anche sul conto della signora risultano accessi non autorizzati** e che «per sicurezza» è meglio trasferire temporaneamente anche i suoi soldi sul conto di appoggio.

Il fraudatore insinua ansia nella vittime, legittimato da una comunicazione apparentemente proveniente dalle banca. Lascia sgomenti la «fortuna» dei criminali nel trovare, con una sola chiamata, due vittime che si «gettano» tra le loro braccia senza esitazione.



## #1

Il cliente viene agganciato attraverso banner o attraverso normali telefonate nelle quali vengono proposti investimenti in crypto-valute. **Attratto dai rendimenti apparentemente molto appetibili**, la vittima decide di aprire un account e di fare un primo versamento.



## #4

I **frodatori ricattano la vittima** e, dietro la promessa di restituirgli parte dei suoi stessi soldi, **lo costringono a mettere a disposizione il suo c/c ed operare come «mulo»** oppure a prestare la sua identità per altre attività illecite.



## #2

La vittima ottiene l'accesso ad una piattaforma di trading ed **inizia a versare con regolarità fondi** che, seguendo le indicazioni dei frodatori, sembrano portargli alti rendimenti.

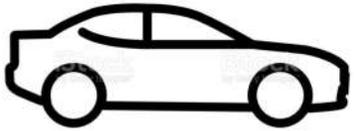
## #3

Dopo un certo tempo, ad esempio quando prova a trasferire i presunti grandi guadagni sul suo c/c, **la vittima comprende di essere stata truffata e subentra la disperazione.**



***Durata Totale: variabile***

I criminali sfruttano due volte l'ingenuità delle vittime: prima inducendole a investire denaro in attività senza nessuna possibilità di ritorni e poi costringendole a mettersi a disposizione della stessa organizzazione criminale che li ha colpiti.



## #1

Le vittime si trovano a dover parcheggiare in grandi centri urbani in cui non è facile trovare abbondanza di posti auto. Invariabilmente, **l'auto viene parcheggiata male o in divieto di sosta.**



## #3

Le vittime procedono al pagamento seguendo le istruzioni a cui il QR code rimanda, il quale però **non è legato al conto corrente della polizia municipale bensì a quello dei criminali.**



## #2

Al momento di ritornare presso la propria autovettura, **le vittime ritrovano sul parabrezza una (falsa) multa per divieto di sosta.** Sul documento sono riportate anche le istruzioni per il pagamento, il quale, **se effettuato subito ed attraverso il QR code allegato,** sarà ridotto in una certa misura.

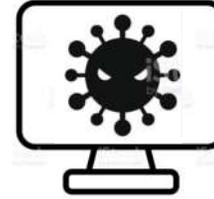
**Durata Totale: minuti**

Attacco tanto semplice quanto efficace, fa leva sulla sensazione della vittima di trovarsi in difetto e può contare su uno schema non ancora diffuso e dunque non facilmente riconoscibile dal cittadino comune.



## #2

Il software malevolo resta silente anche per settimane, limitandosi a raccogliere info del PC su cui si trova. Solo quando l'infetto viene valutato «idoneo» a diventare vittima, il sw invia le info al suo C&C e scarica una nuova componente software che **combinata con la precedente diventa concretamente dannosa**.



## #4

il malware, **al fine di ritardare la detection e utilizzando specifici webinject, maschera la compromissione** sia alterando i dati mostrati a video sia alterando eventuali pdf richiesti dall'utente relativi all'estratto del conto corrente aziendale.

## #1

L'azienda riceve una **PEC** apparentemente attendibile ma il cui allegato è malevolo. Spinto dal falso senso di sicurezza il destinatario apre l'allegato infettando il PC.



## #3

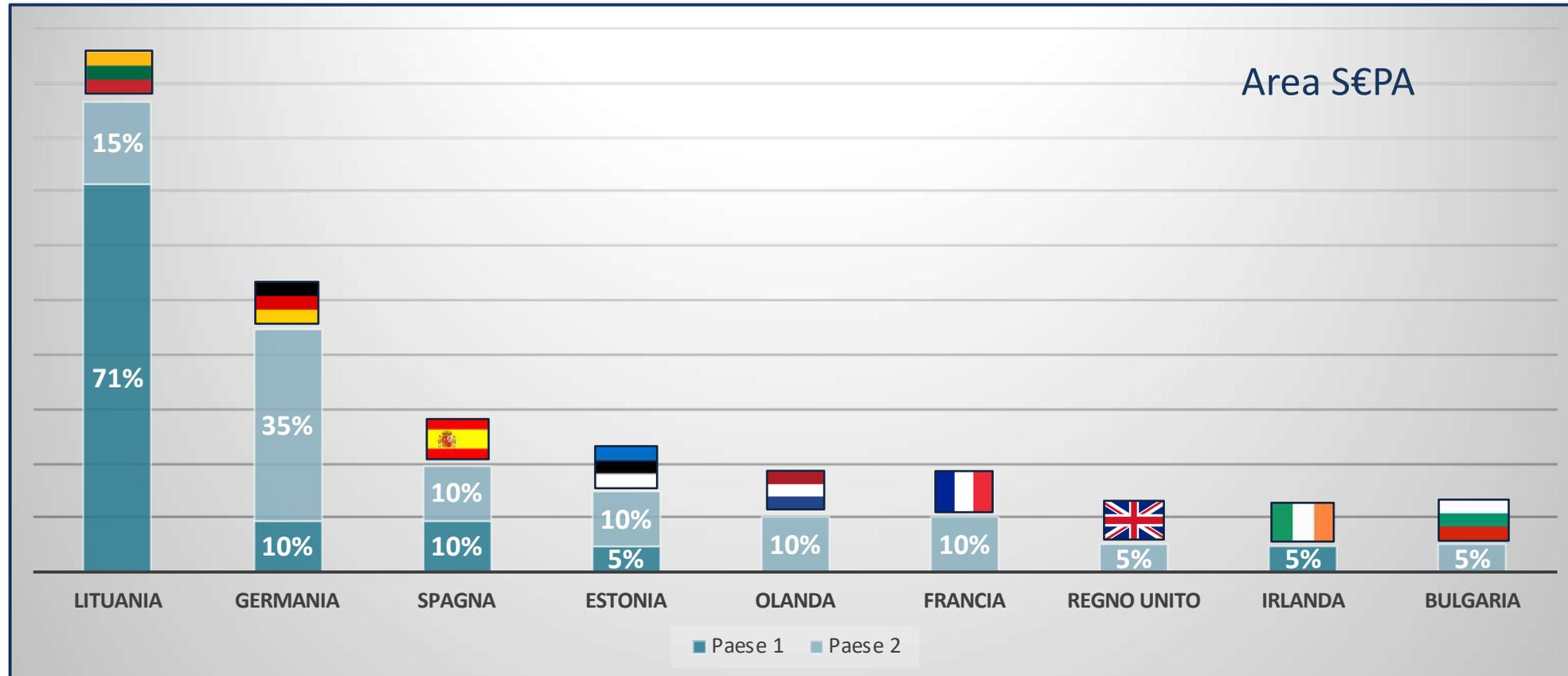
All'atto della sottomissione di una nuova transazione da parte dell'utente, **il malware interviene sostituendo l'iban del destinatario legittimo con un altro** ed alterando i dati riepilogativi mostrati al termine dell'operazione.



***Durata Totale: Diverse Settimane***

Attacco molto sofisticato le cui vittime sono scelte con cura. La frode viene condotta sfruttando il falso senso di sicurezza indotto dalla PEC e mettendo in campo una componente tecnica decisamente superiore alla media.

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

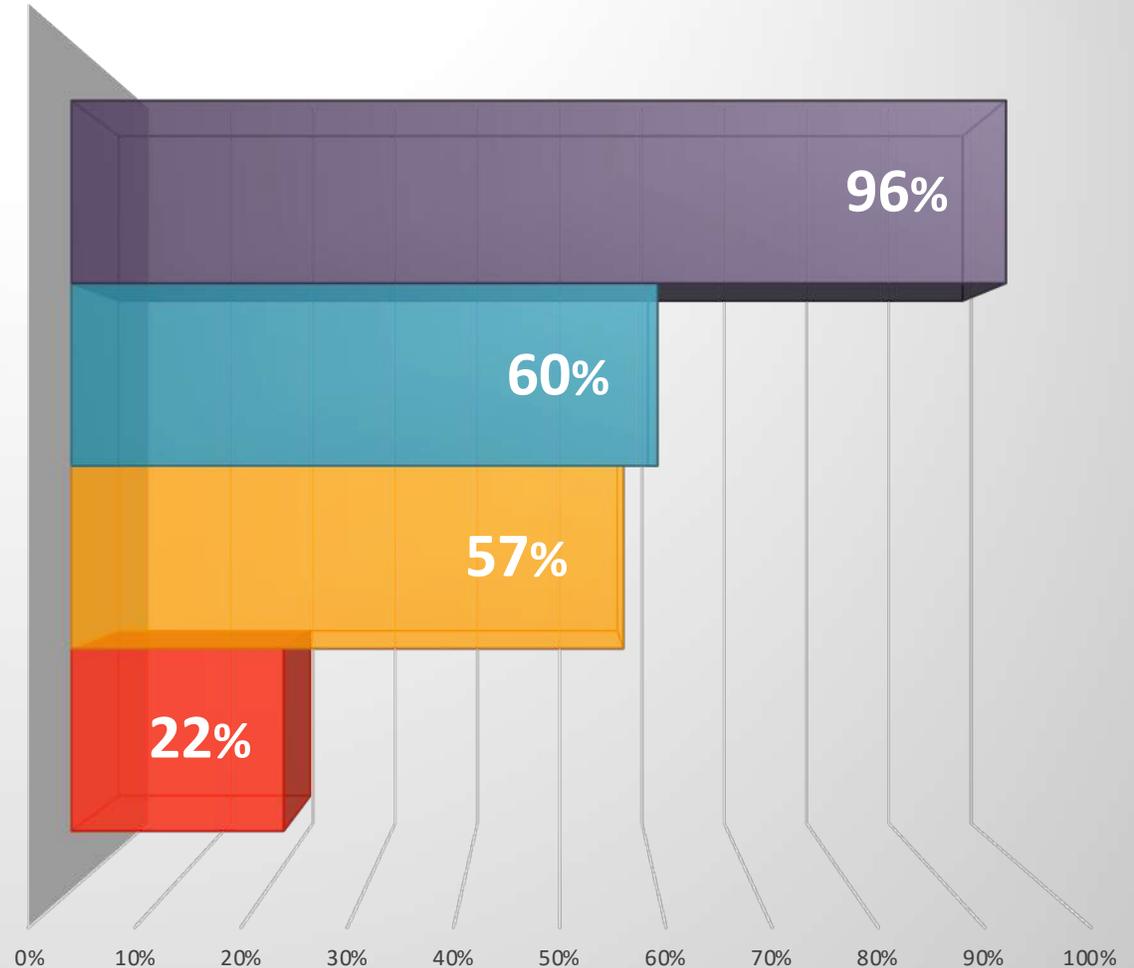


istituti che nel corso del 2022 disponevano di contromisure tecnologiche (i.e., soluzioni interne e/o servizi esterni) volte a mitigare attacchi DDoS

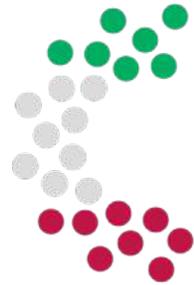
istituti che nel corso del 2022 hanno rafforzato le contromisure tecnologiche volte a mitigare attacchi DDoS

istituti che hanno rilevato un attacco DDoS

istituti che hanno rilevato un attacco DDoS rivendicato da gruppi filorusi



**Thank You!**



**CERTFin**

**Defend. Inform. Evolve.**

*For more info visit [www.certfin.it](http://www.certfin.it) or write to [ricerca@certfin.it](mailto:ricerca@certfin.it)*