CERTFin

14 Maggio 2024

Sicurezza e Frodi in Banca Report 2024

Mario Trinchera

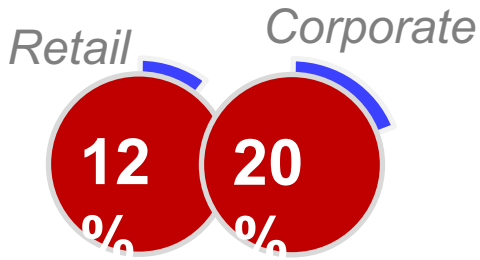
Technical Coordinator

TLP:GREEN

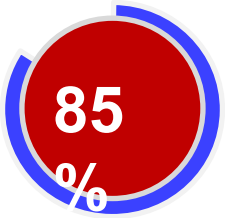
Key Results

CERTFin

In entrambi i segmenti cresce l'efficacia degli attacchi

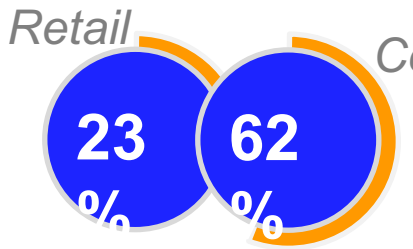


Si intensifica ulteriormente l'abuso dei canali telefonici come vettore iniziale

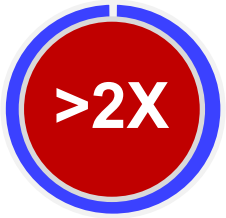


98 frodi su 100 sono completate assolvendo la SCA

Il bonifico istantaneo rafforza la sua posizione tra gli strumenti preferiti dai criminali nei loro tentativi di frode



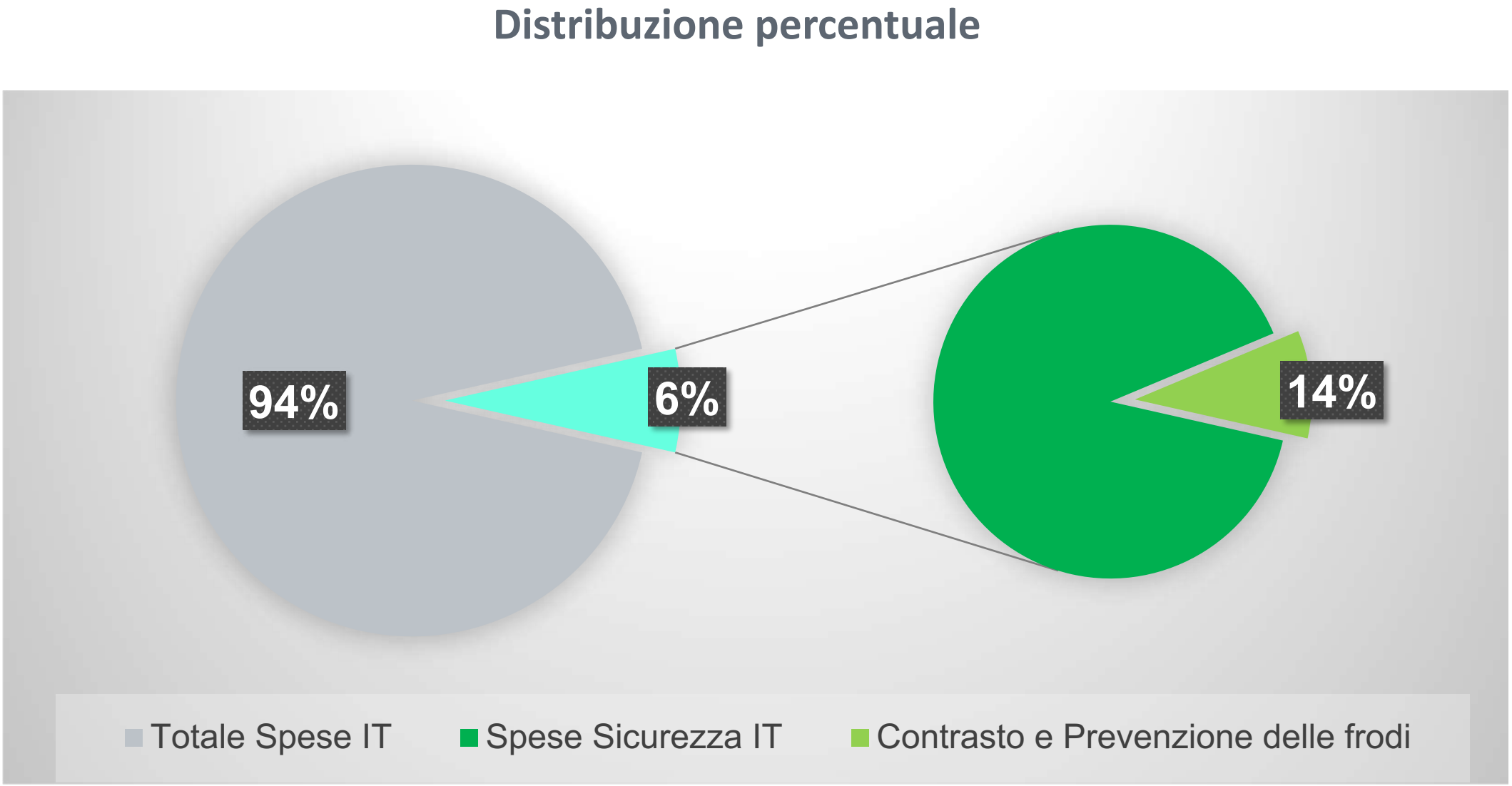
La rilevazione fa registrare un controvalore delle frodi effettive più che raddoppiato



Cresce progressivamente l'importo delle frodi «recuperate»

Budget dedicato alla Sicurezza

CERTFin



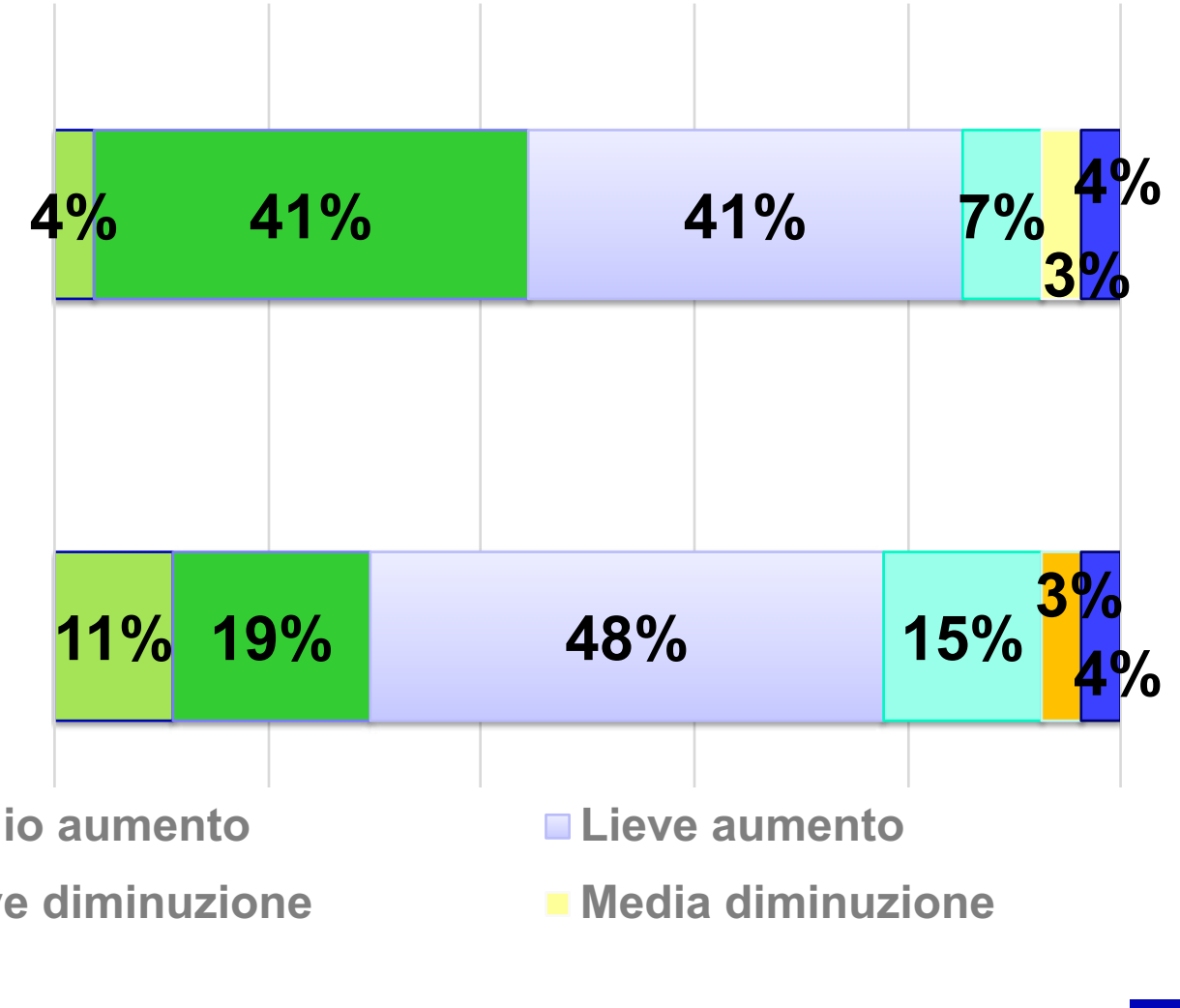
Budget dedicato alla Sicurezza

CERTFin

Evoluzione del livello di spesa dedicata alla sicurezza

Evoluzione della spesa per interventi lato organizzazione
(sistemi di monitoraggio, sw/hw di protezione, alerts, …)

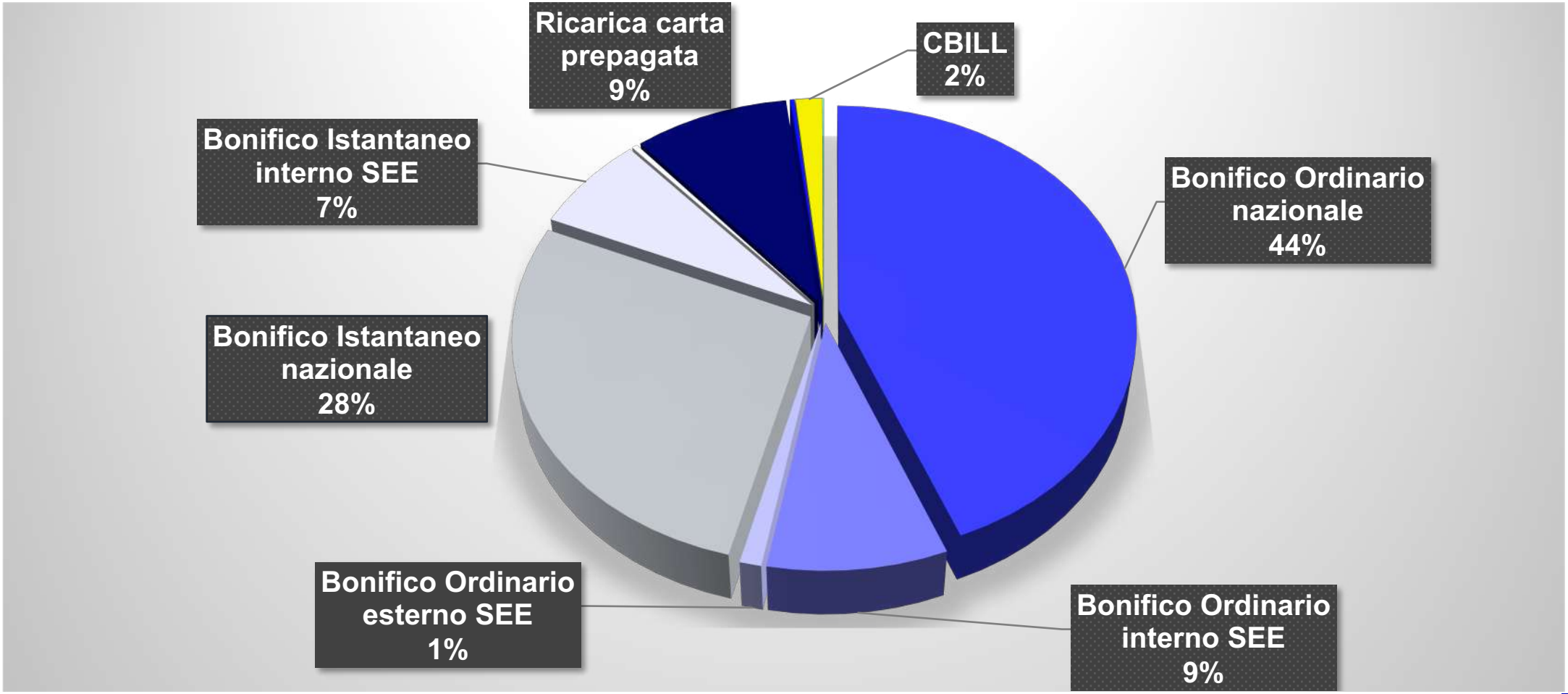
Evoluzione della spesa per progetti e iniziative a beneficio del cliente
(Sicurezza dell'identità, tecnologie MFA, Awareness, etc.)



Transazioni Fraudolente Effettive

CERTFin

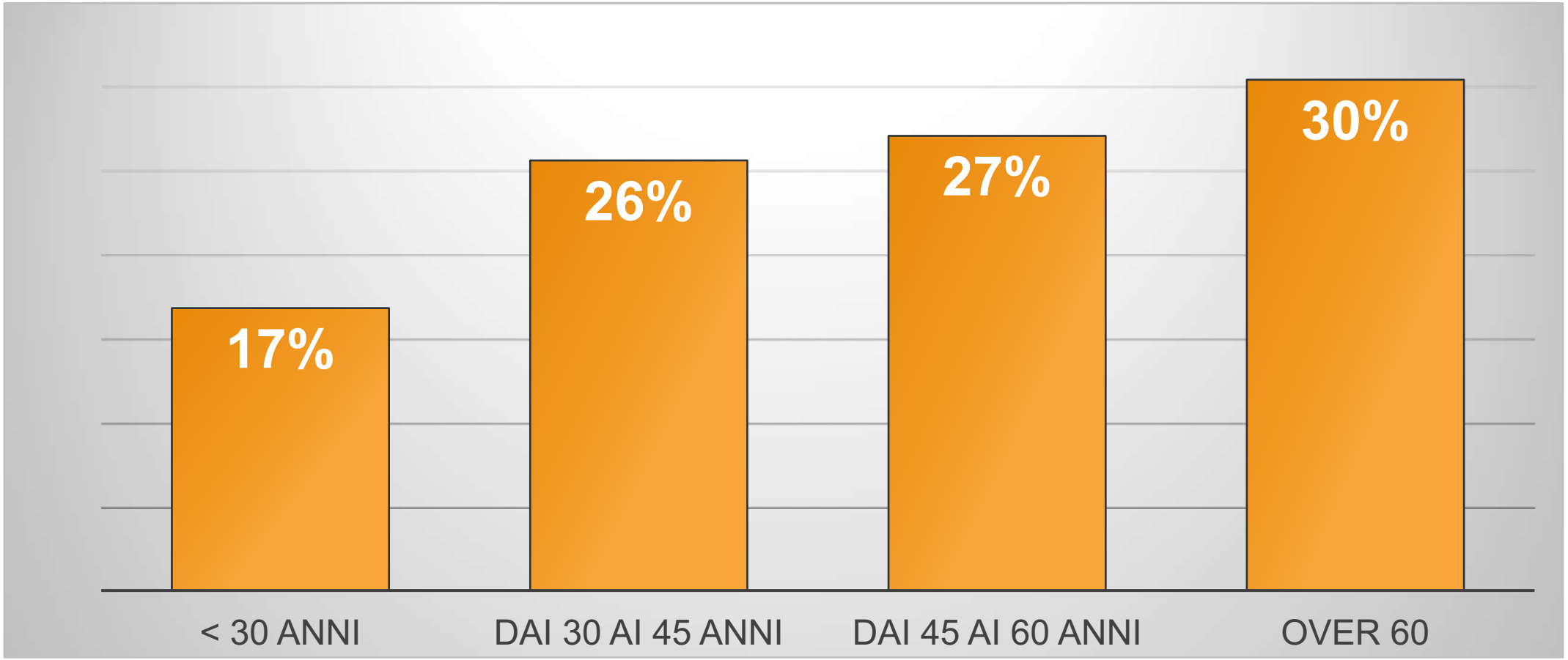
Ripartizione percentuale per tipologia – analisi sugli importi (segmento Retail)



Età delle vittime

CERTFin

Ripartizione percentuale per fascia d'età delle vittime di transazioni anomale (segmento Retail)

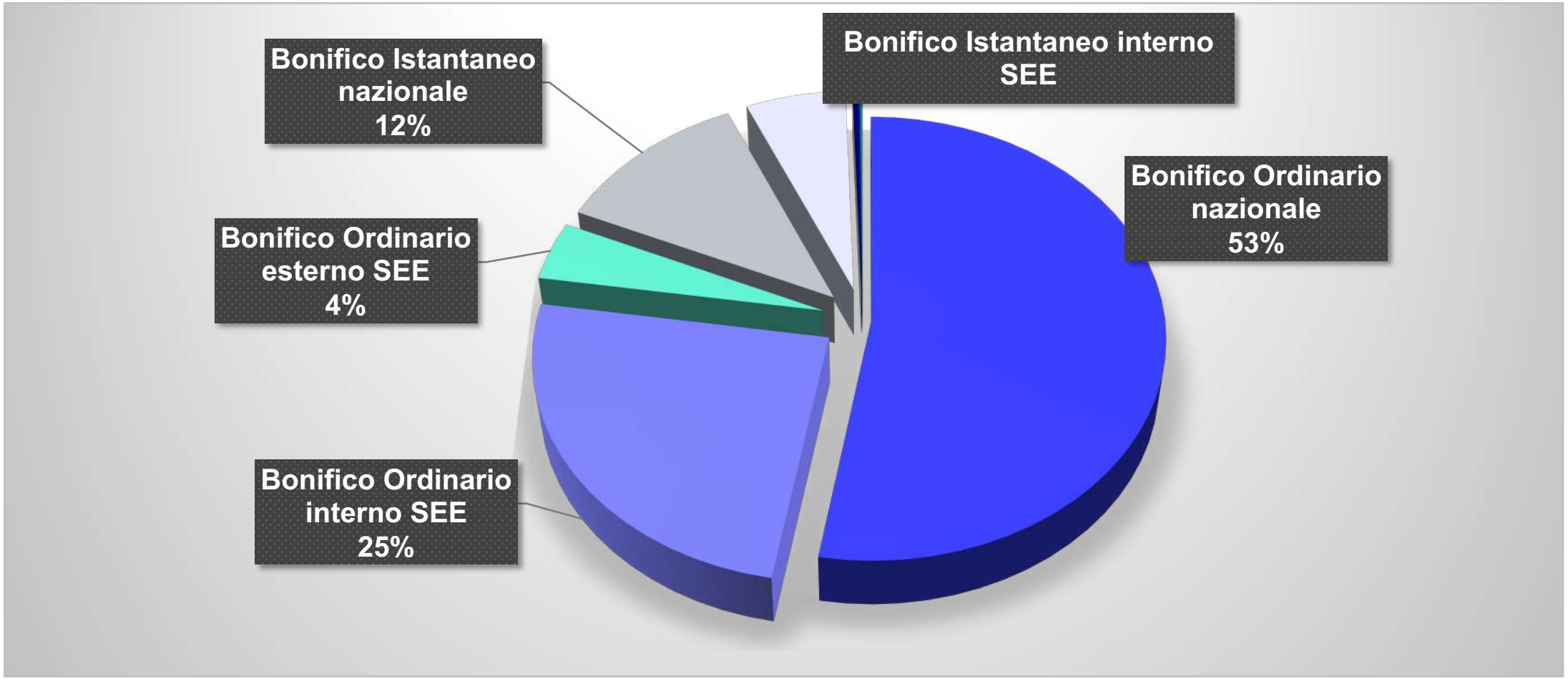


Transazioni Fraudolente Effettive

CERTFin

Ripartizione percentuale per tipologia – analisi sugli importi

(segmento Corporate)

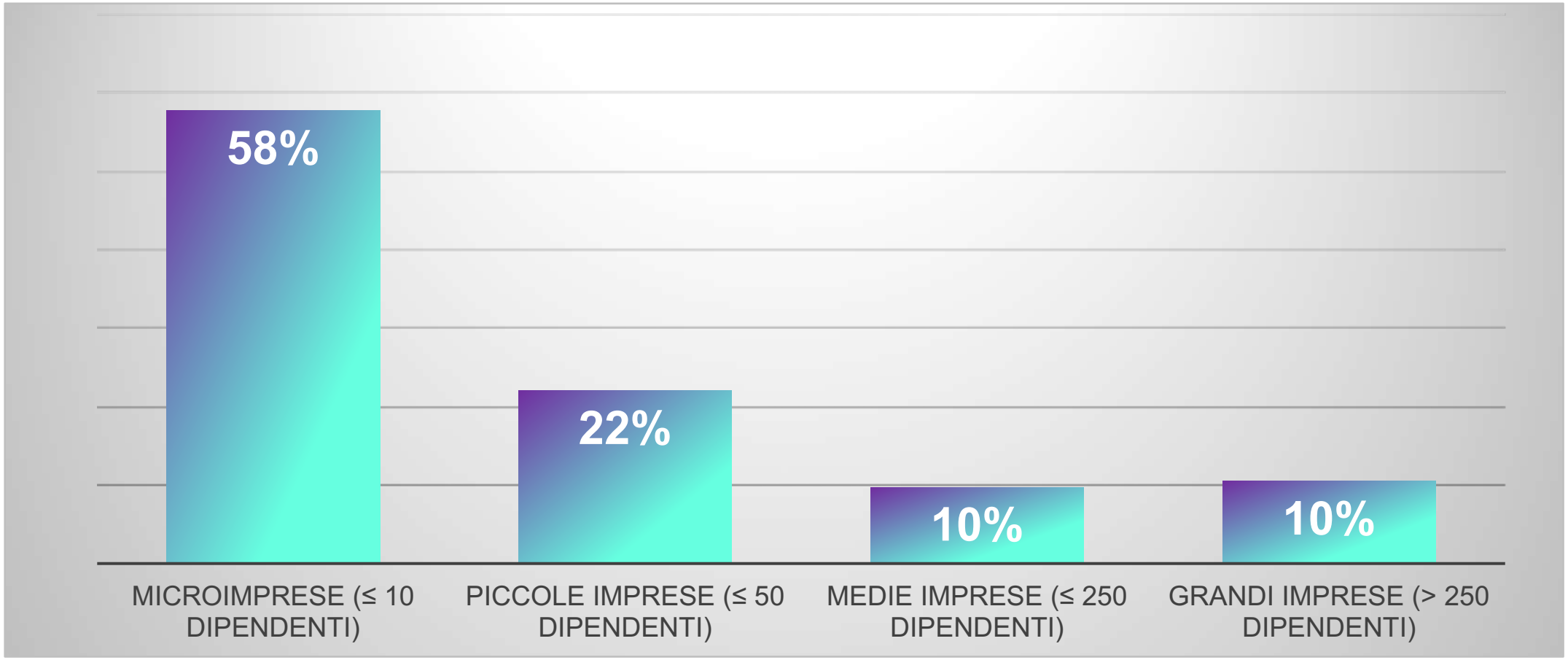


Dimensioni delle aziende vittime

CERTFin

Ripartizione percentuale per fascia dimensionale delle vittime

(segmento Corporate)

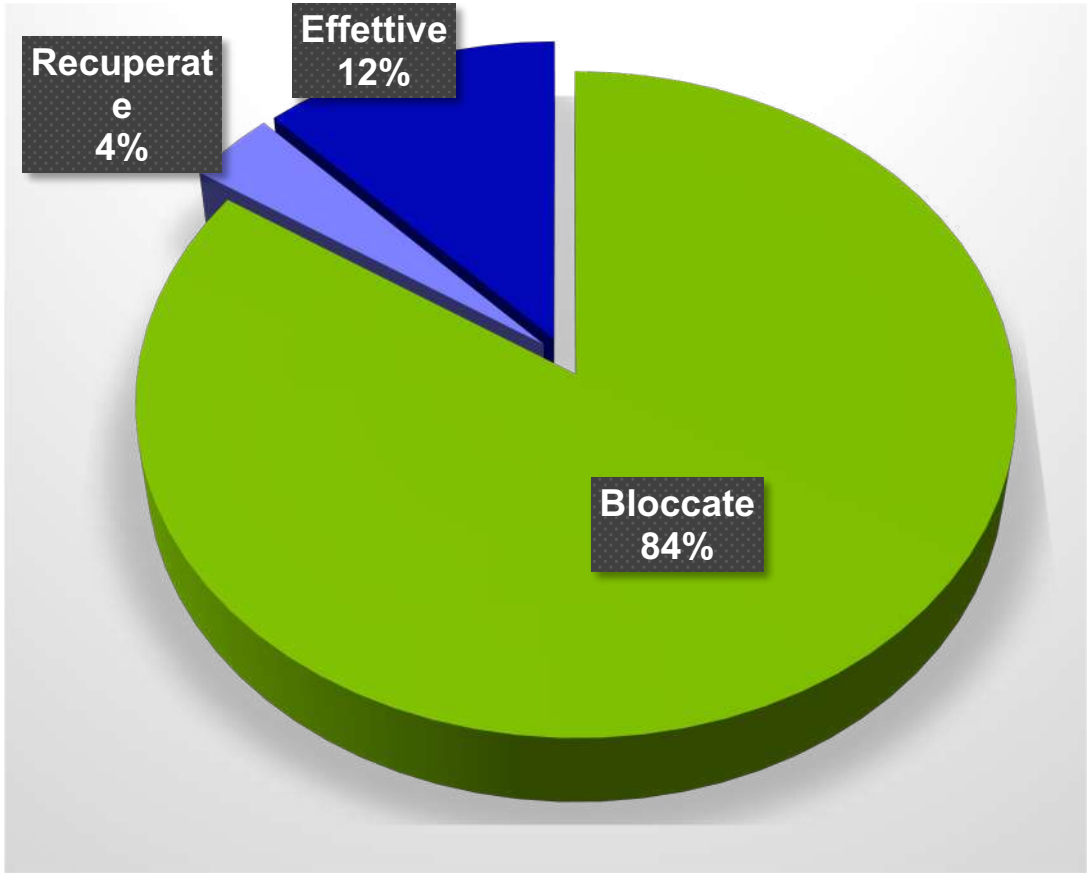


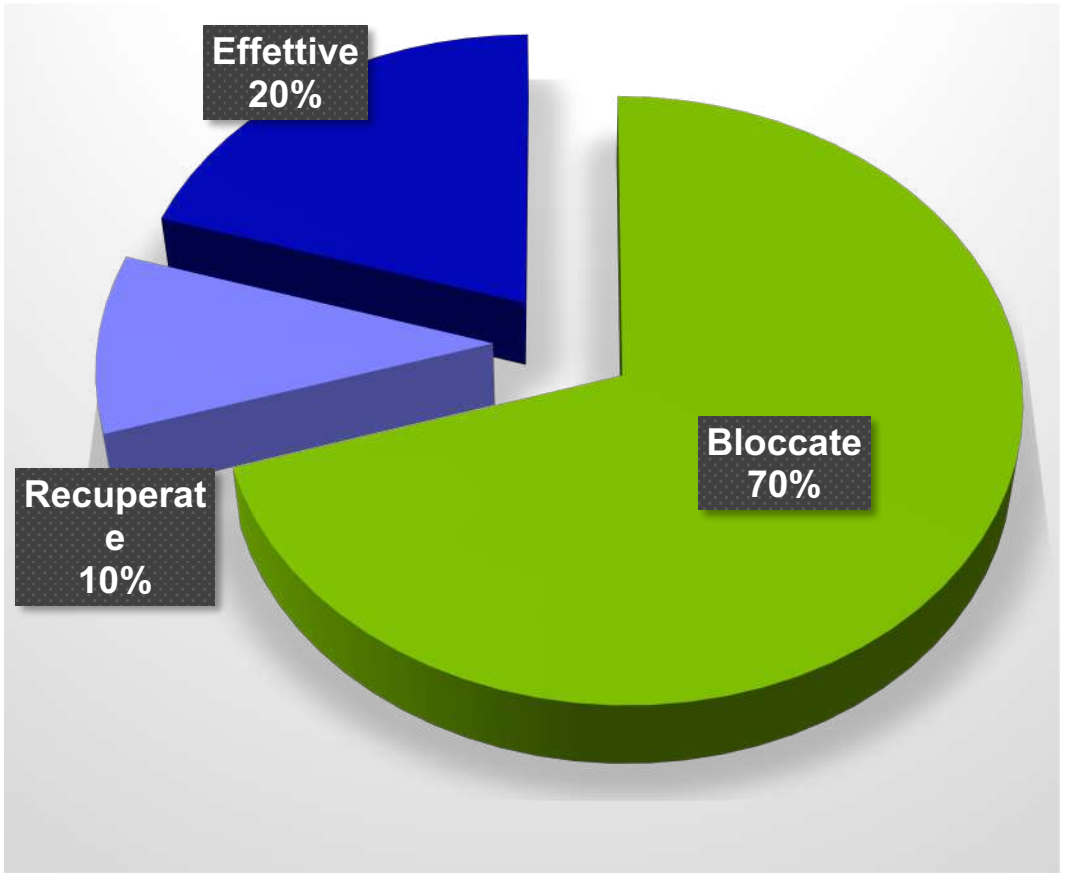
Transazioni Anomale

CERTFin

Ripartizione percentuale – analisi sul controvalore in euro

(Retail e Corporate)



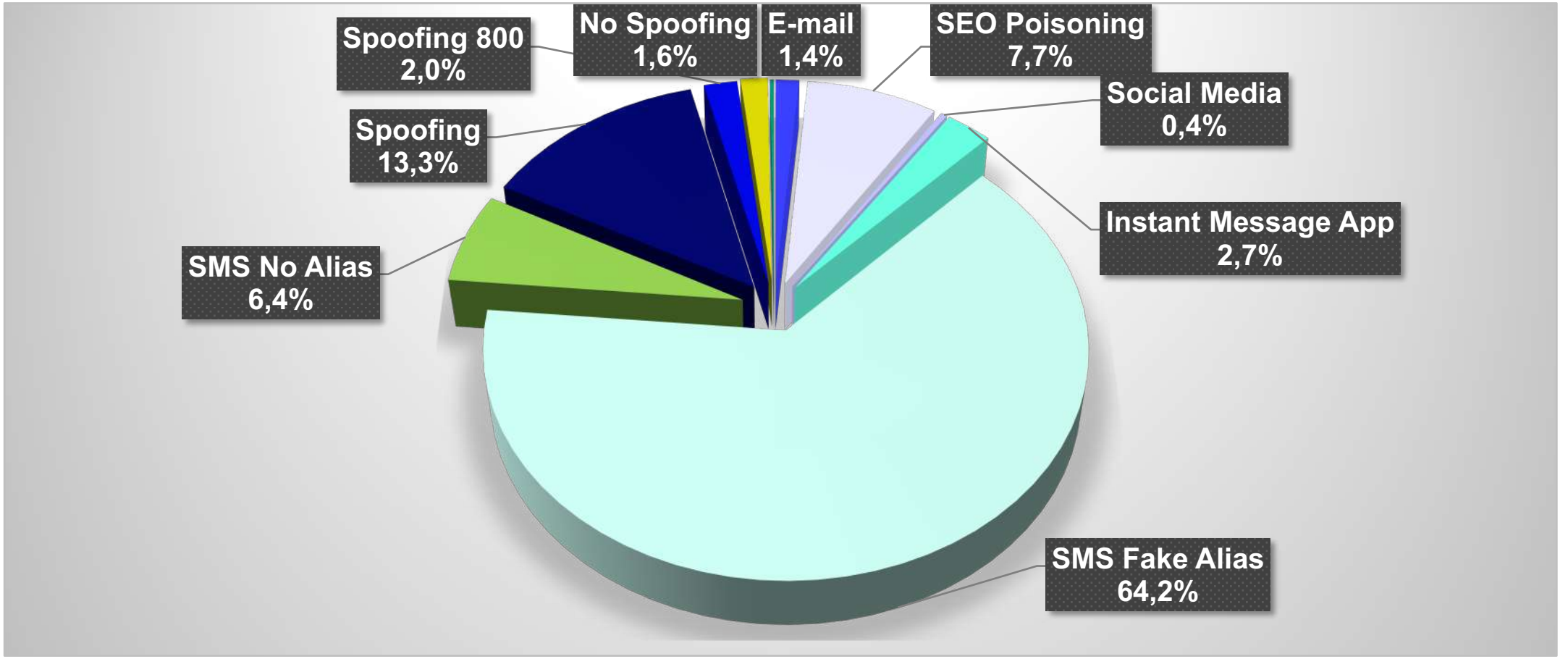


Fraud Chain

CERTFin

Punto di primo contatto/vettore iniziale della frode

(segmento Retail)

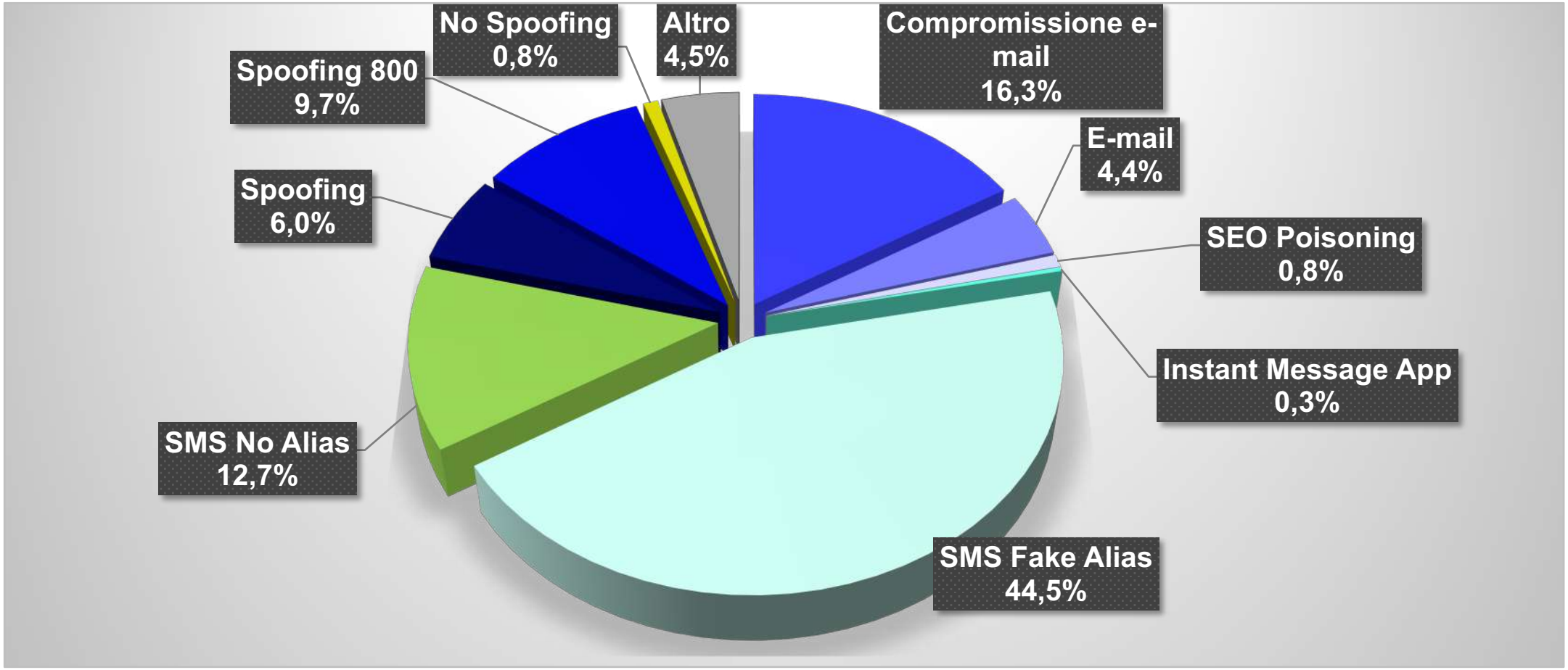


Fraud Chain

CERTFin

Punto di primo contatto/vettore iniziale della frode

(segmento Corporate)

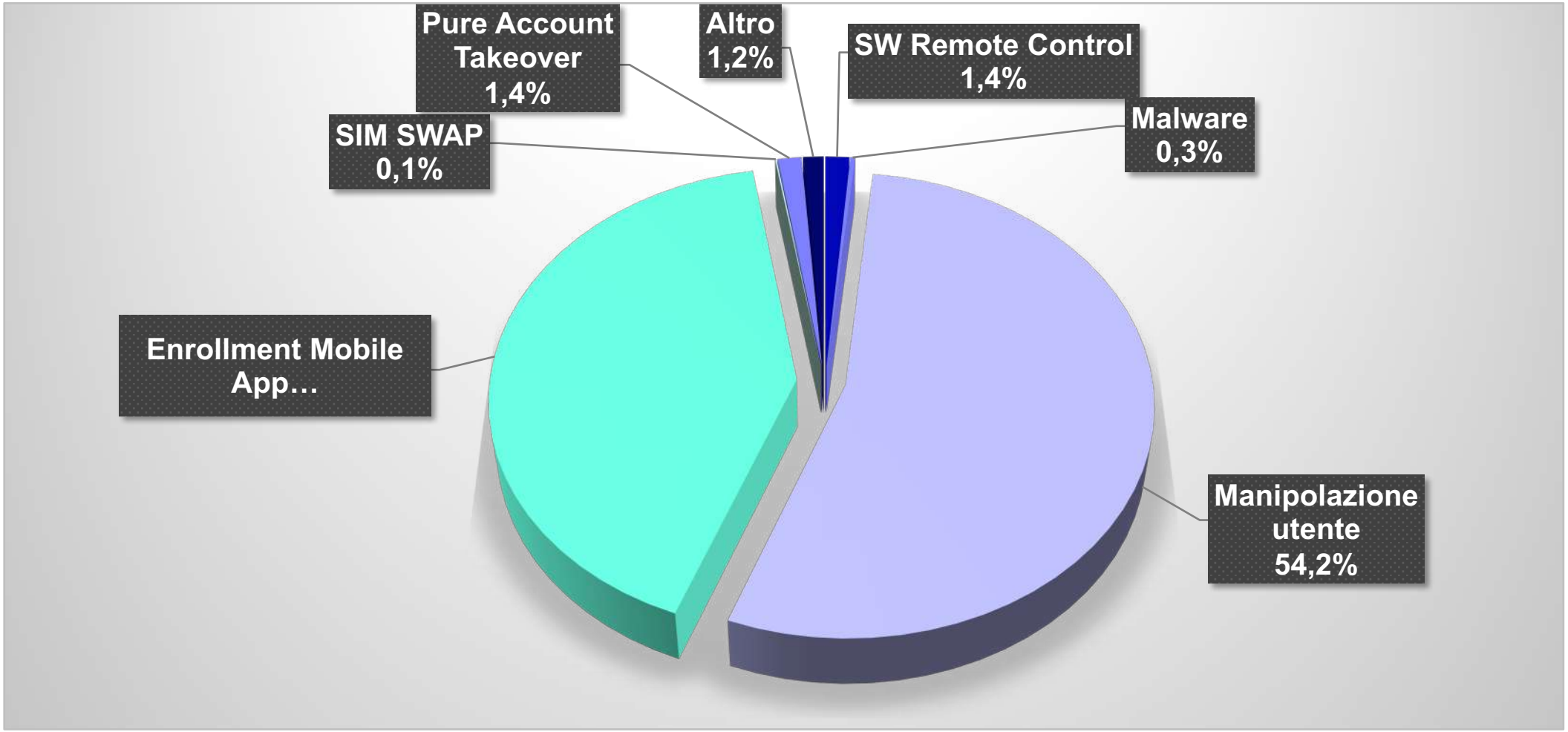


Fraud Chain

CERTFin

Tecnica utilizzata per finalizzare la frode

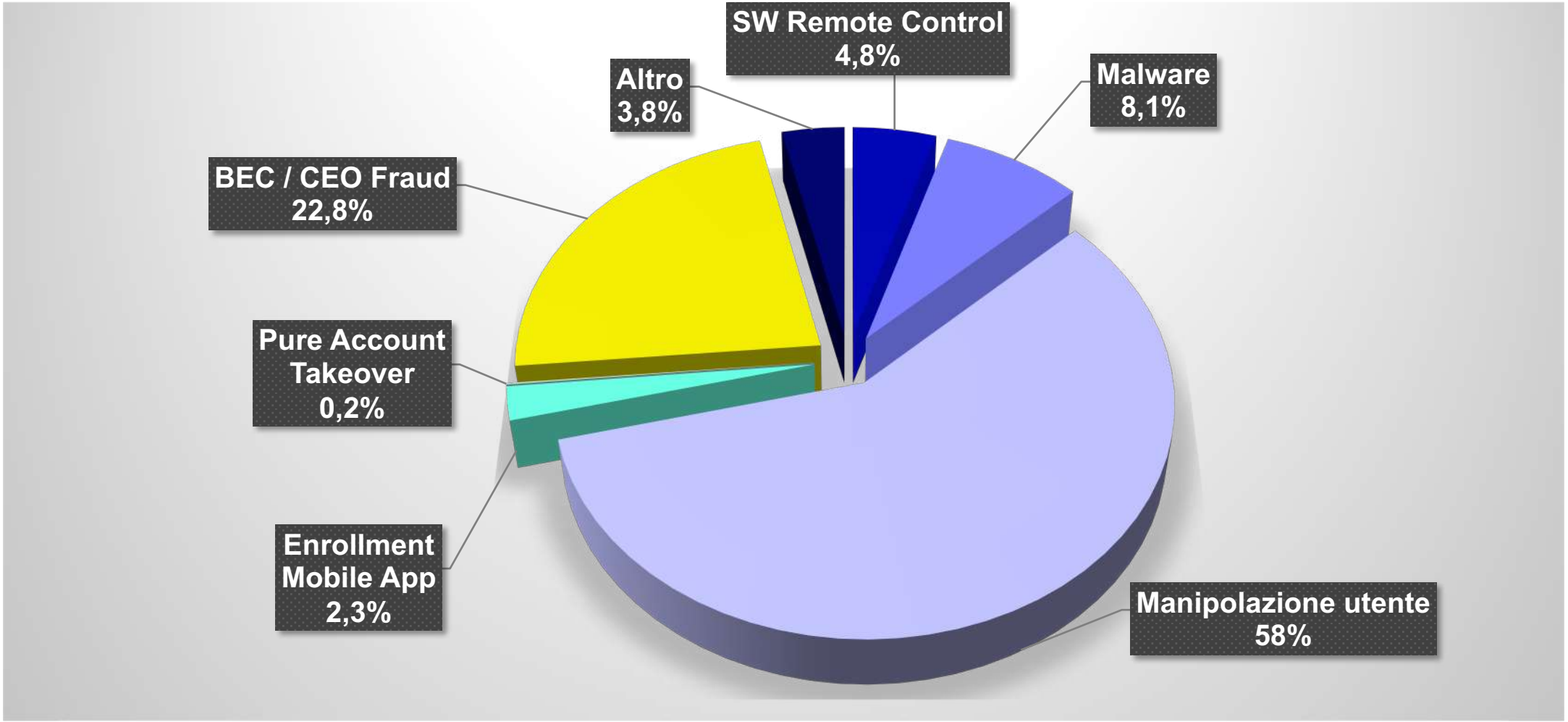
(segmento Retail)



Fraud Chain

CERTFin

Tecnica utilizzata per finalizzare la frode
(segmento Corporate)

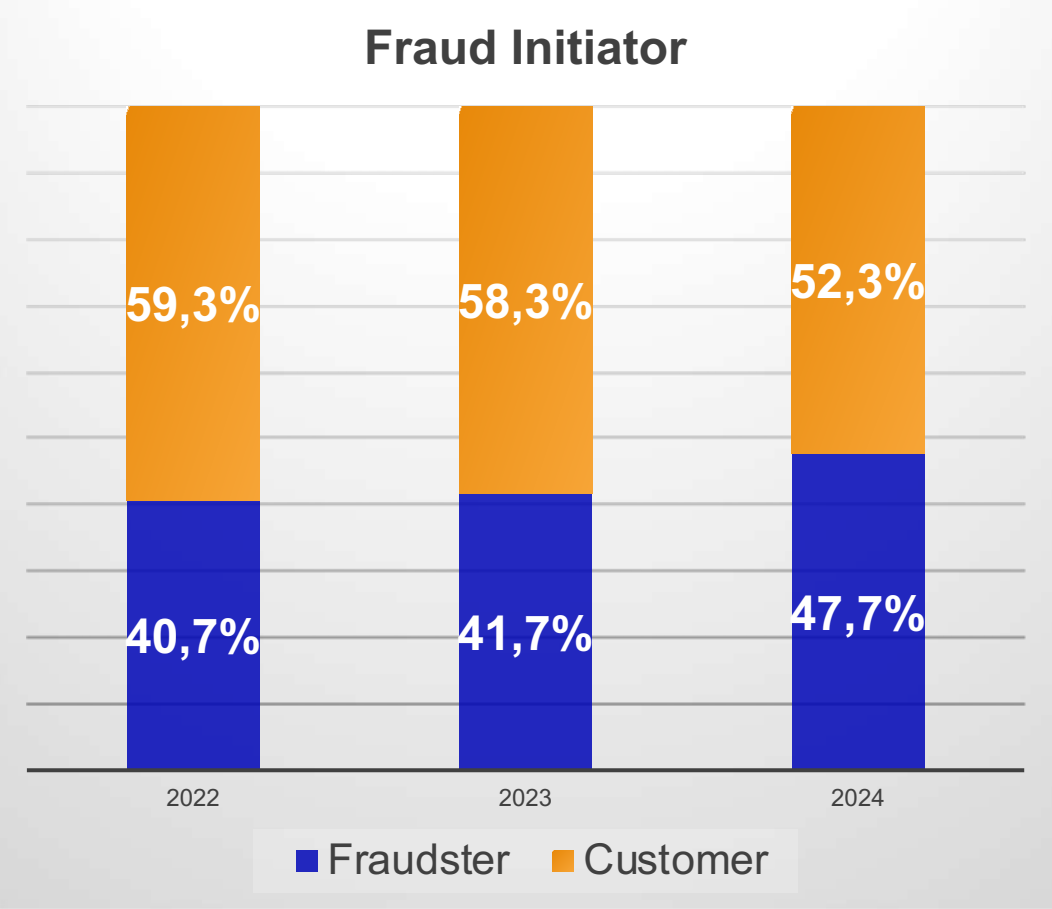


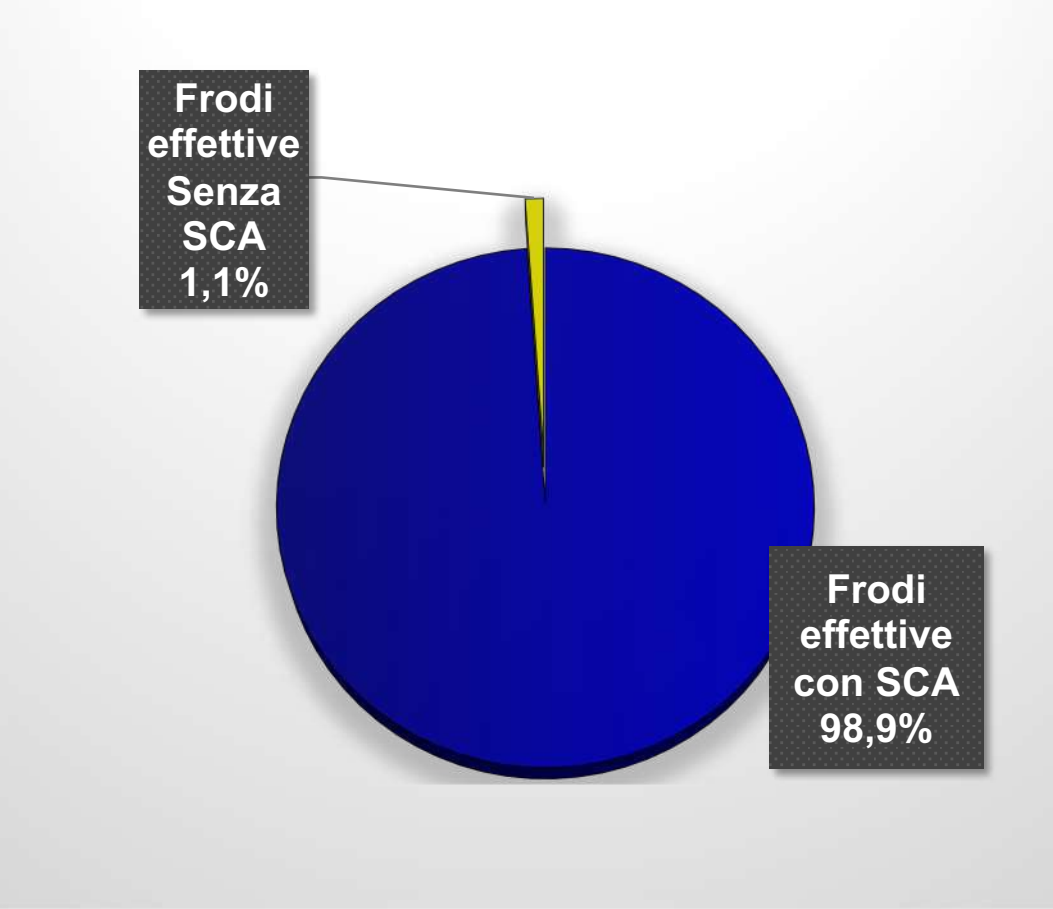
Fraud Chain

CERTFin

Dinamica sulla finalizzazione della frode

(Retail + Corporate)



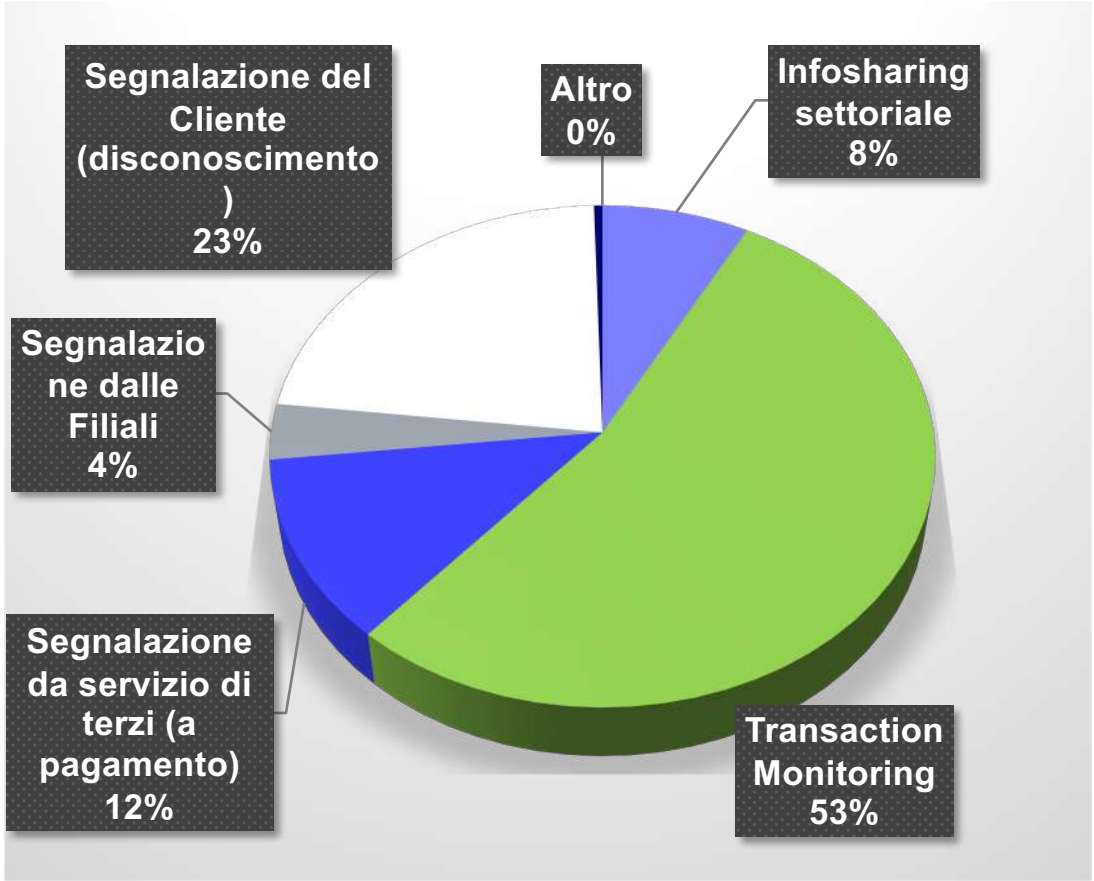


Fraud Detection

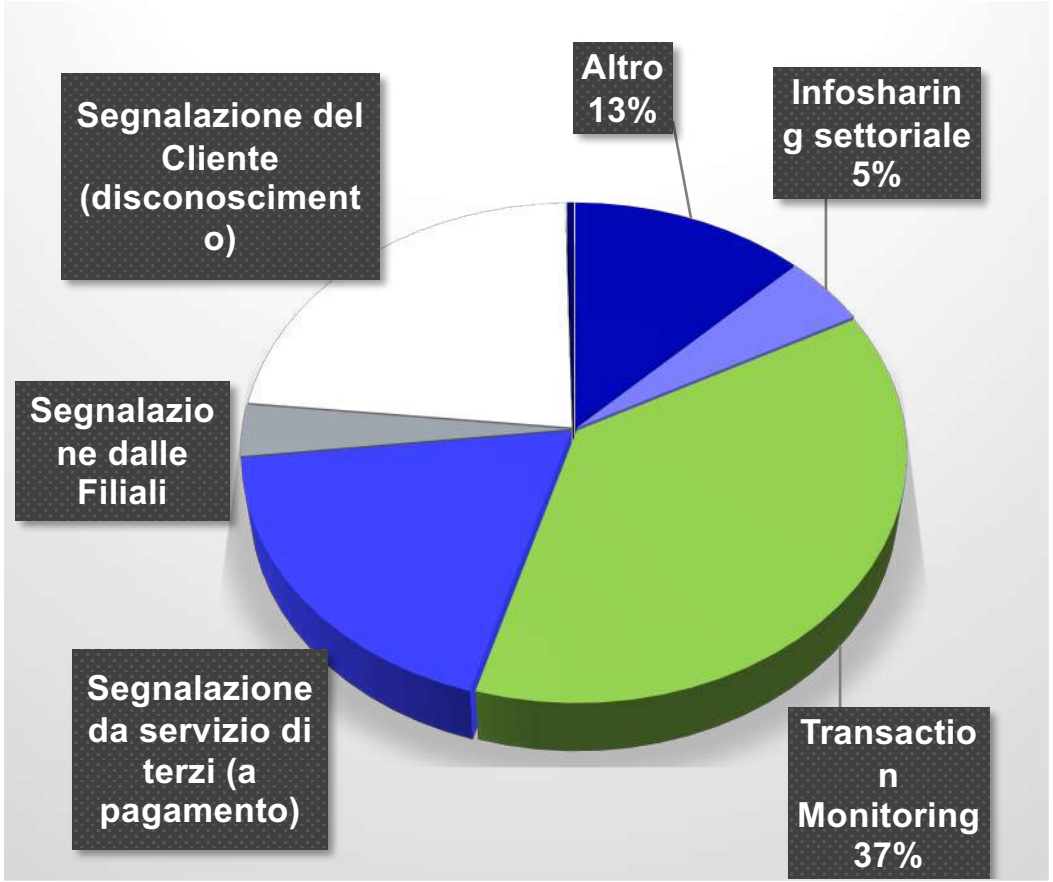
CERTFin

Fonti di segnalazione

Retail



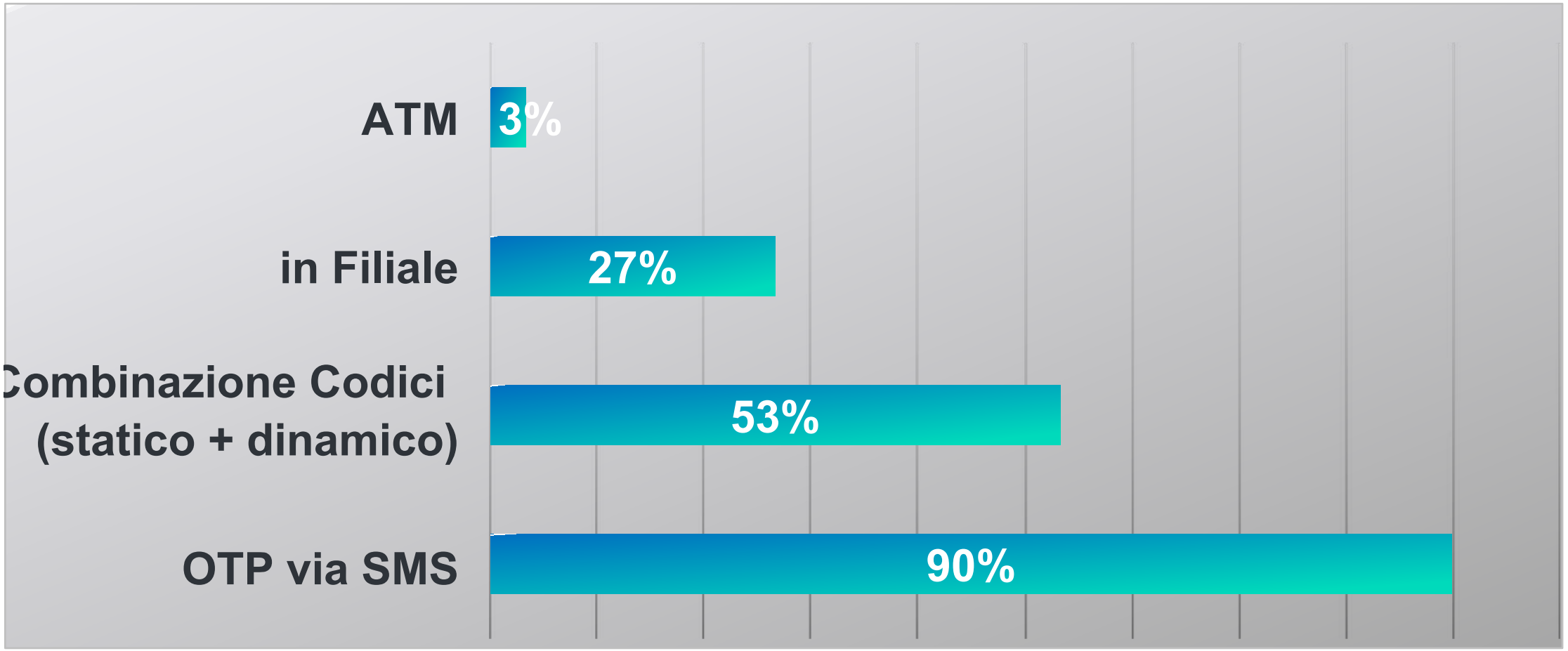
Corporate



Processo di Enrollment

CERTFin

Procedura di associazione dello strumento di pagamento in app (enrollment)



Attacchi basati sulla scarsa consapevolezza

CERTFin

#1

Comuni cittadini vengono agganciati attraverso banner o attraverso normali telefonate nelle quali vengono proposti dei **buoni amazon** in cambio di alcune «attività di test».

#4

I frodatori, con spesa limitata, si creano così una **rete di conti di appoggio** sui quali far transitare fondi sottratti ad altre vittime di frode.
Conti però intestati a **cittadini ignari**.

#2

Lo scopo del test è verificare quanto sia facile e veloce aprire un conto bancario in modalità totalmente online.
All'interessato viene indicato un sito (genuino) presso il quale iscriversi e avviare il processo di *onboarding*.

#3

I frodatori si raccomandano di non riferire ad eventuali altri operatori che si sta effettuando un test.
Una volta completato il processo, i frodatori consegnano il buono amazon in cambio del «feedback» del cliente e delle **credenziali del conto**, in quanto sarà loro cura registrare il parere e chiudere il conto.

***Durata Totale**: alcune ore*

I criminali riescono a irretire e convincere cittadini scarsamente consapevoli a mettere a loro disposizione una rete di conti. Dietro ricompensa di importo anche contenuto, i cittadini finiscono per fungere da money mule a loro insaputa.

Attacchi basati su tecniche miste

CERTFin

#0

I frodatori, dopo un attento studio dei processi di enrollment in uso nelle varie banche, predispongono attacchi mirati sulla clientela.

#1

Il cliente viene contattato telefonicamente, nella maggior parte dei casi giustificando la chiamata come necessaria ad indagare un potenziale problema sul suo conto o sul suo device.

#2

Utilizzando una certa varietà di storie, il frodatore convince il cliente a disinstallare l'app della banca e contestualmente la installa su un altro device in suo possesso.

#3

A questo punto sono possibili alcune varianti:

1. Con il solo **Social Engineering** il frodatore riesce a farsi riferire dal cliente il contenuto degli SMS OTP utili a completare l'enrollment sul device in suo possesso
2. Il frodatore convince la vittima ad installare un **malware** (spacciandolo da antivirus) che inoltra sul suo device gli SMS ricevuti dal cliente legittimo
3. Il frodatore chiama la banca con il numero del cliente (**spoofing**) e convince l'operatore a rimuovere il token sul device in possesso della vittima ed avere così via libera per avviare un nuovo enrollment su altro device.

***Durata Totale**: 1 ora*

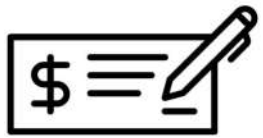
#4

I frodatori, con le informazioni estorte alla vittima, una volta completato l'enrollment **possono procedere in autonomia** a trasferire fondi verso conti da loro stessi controllati

A fronte di una conoscenza dettagliata del processo e attraverso la collaborazione inconsapevole del cliente, i criminali riescono a realizzare le condizioni necessarie ad operare in sua vece.

Attacchi basati sulla creatività

CERTFin



#1

Il frodatore si reca in banca per incassare un assegno circolare. **L'assegno risulta emesso da una (finta) banca sconosciuta all'operatore di sportello.**

#3

L'operatore chiama il numero presente sul sito per avviare le verifiche sull'autenticità dell'assegno.
Tuttavia, **a quel numero rispondono i frodatori che ovviamente ne confermano l'autenticità**, consentendo al complice di incassare l'importo.

#2

I frodatori, attraverso tecniche di SEO Poisoning (*), riescono a portare il sito della finta banca, creato ad hoc, in cima ai risultati dei principali motori di ricerca. Quando l'operatore di sportello prova a fare delle ricerche sulla banca a lui sconosciuta, **trova facilmente il sito e vi entra**.

Durata Totale: *20 minuti*

(*) Il SEO (search engine optimization) Poisoning è un insieme di tecniche progettate per sfruttare gli algoritmi dei motori di ricerca per promuovere pagine web dannose. Se un attaccante riesce a progettare la propria pagina web in modo che si posizioni in alto su Google o Bing, gli utenti sono più propensi a fidarsi e a visitare il sito web.

Attraverso un'abile combinazione di social engineering e capacità tecnica, i frodatori riescono a portare a termine numerose frodi immediatamente monetizzate a danno della banca.

Attacchi con una componente tecnica significativa

CERTFin

#1

I frodatori posizionano uno **shimmer** in un ATM compromesso (ATM#1) e aspettano che un cliente (vittima) inserisca una carta autentica nel terminale.

Lo shimmer viene applicato all'interno del vano carta, ha lo spessore di una sim, è smussato sul lato frontale in modo da non intralciare l'inserimento della carta della vittima e non è visibile dall'esterno.

#2

Quando viene inserita la carta genuina nell'ATM compromesso (ATM#1), lo shimmer ritarda l'operazione di prelievo legittima, copia il blocco dati della carta e **lo inoltra via bluetooth ai frodatori** che già hanno predisposto ad operare un secondo ATM (ATM#2).

#3

Attraverso una precisa combinazione di impulsi elettrici, di indurre l'ATM#2 a credere che la carta è predisposta **esclusivamente per il check-offline** (la verifica sulla correttezza del PIN inserito avviene completamente in locale).

#4

I frodatori sostituiscono il risultato della funzione di hash del PIN digitato con quello carpito dallo shimmer (ATM#1). Questa tecnica permette ai criminali di completare transazioni **anche senza conoscere il PIN della carta**.
In rapida successione vengono effettuati due prelievi di massimo importo.

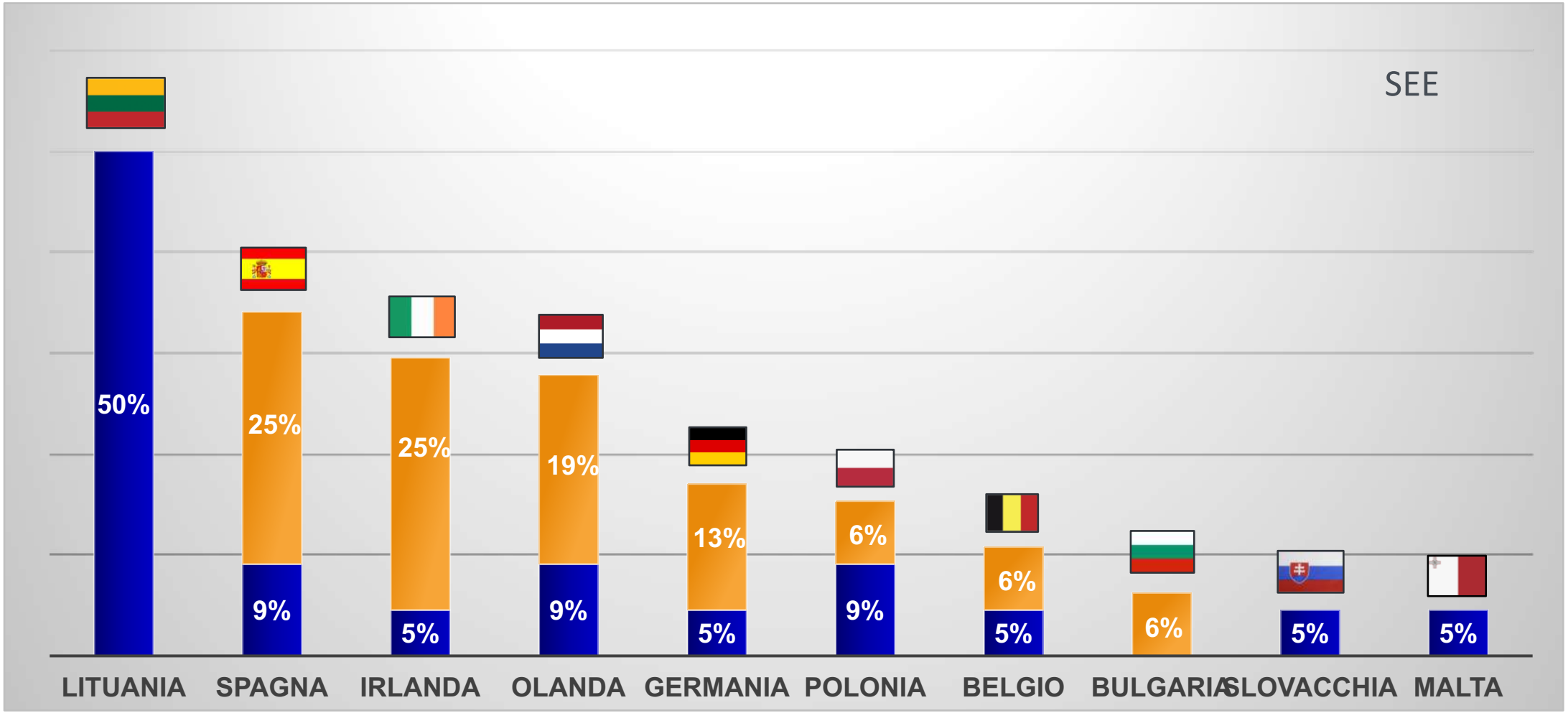
***Durata Totale**: pochi minuti*

Lo schema è molto complesso ed ha una componente tecnica significativa, tuttavia per essere portato a termine è necessario che gli attaccanti presidino due ATM contemporaneamente. Da fonti internazionali a cui il CERTFin ha accesso, risulta che lo schema è già stato osservato in Messico, Canada, Austria, Belgio, Olanda e Spagna.

Distribuzione Geografica

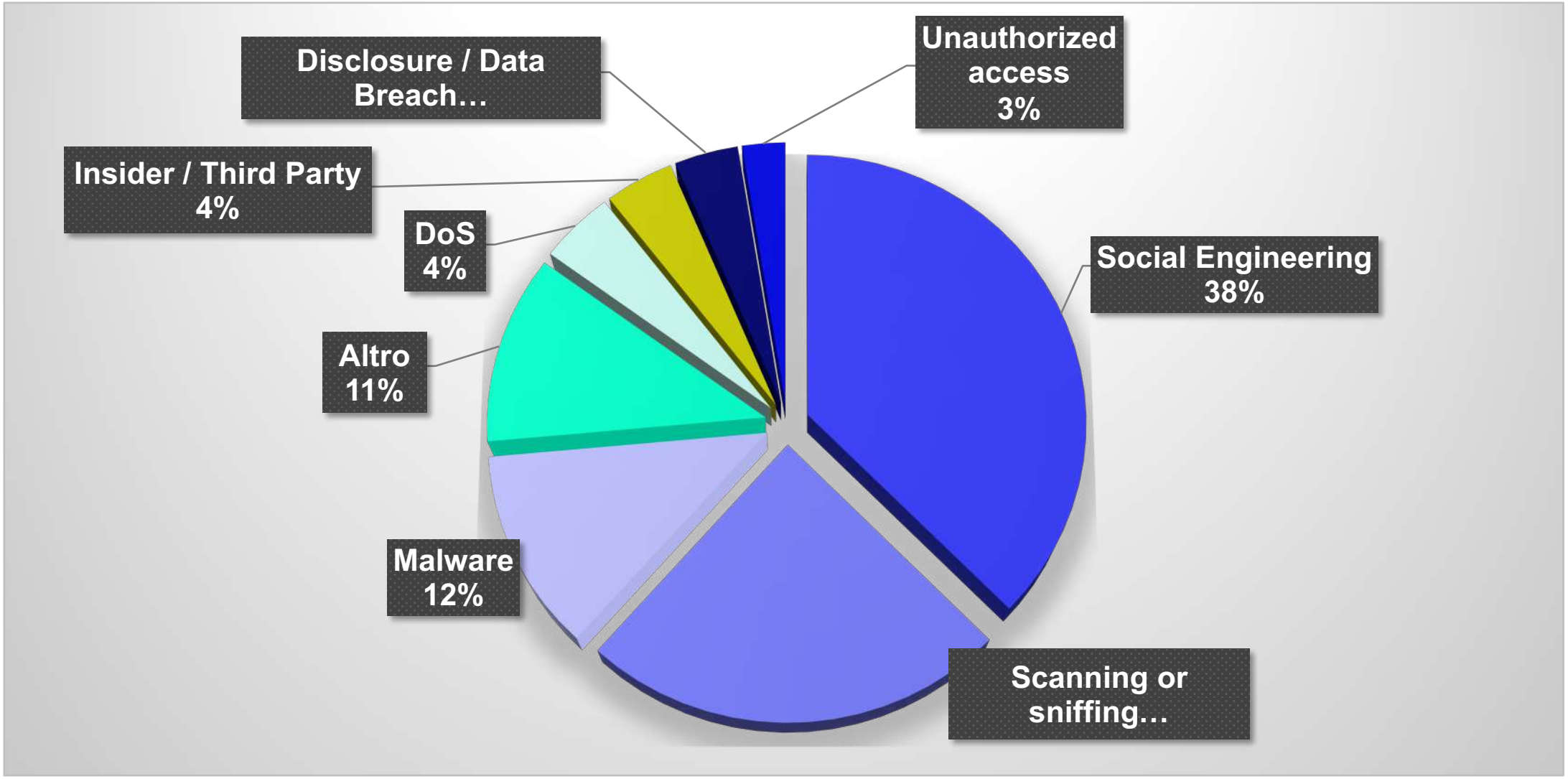
CERTFin

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



Distribuzione percentuale degli attacchi rilevati

CERTFin



Attacchi DDoS Rilevati

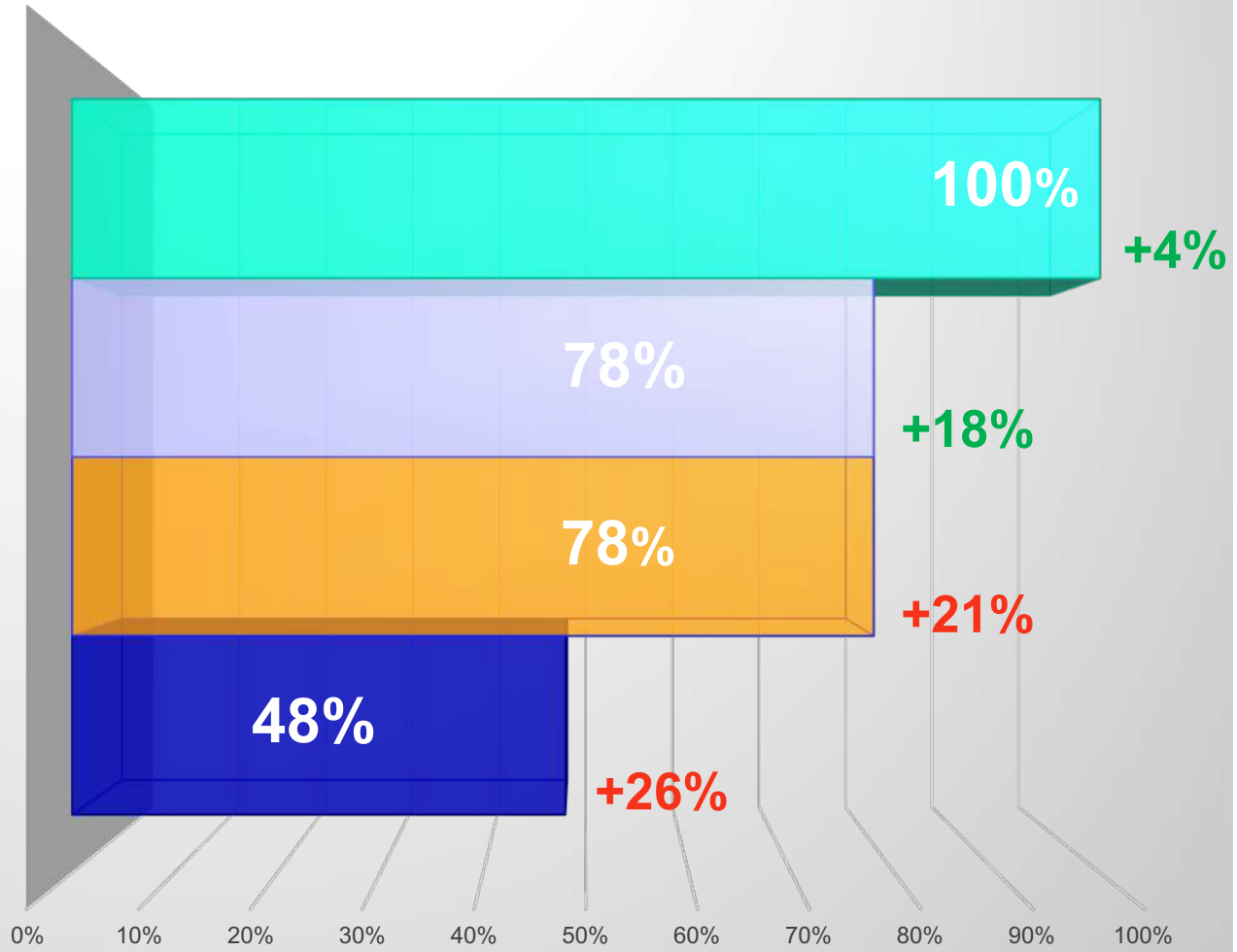
CERTFin

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

istituti che nel corso del 2023 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 filorussi



CERTFin

Grazie!