Euro Retail Payments Board (ERPB) Working Group on Fraud

INTERIM FINDINGS

ERPB PLENARY MEETING, 20 NOVEMBER 2023

Agenda

- 1. Introduction
- 2. Highlights of conclusions from Phase 1
  - Part A: Conclusions after fact-finding on fraud in all its forms
  - Part B: Conclusions after deepdive on impersonation scam & investment scam
- 3. Recommended next steps Phase 2

1. Introduction: **Context**

- Evolutions in payments and in fraud
  - Challenges arising from **disintermediation** (the absence of intermediaries, which heightens the risk of fraud, particularly due to lacks of verification)
  - **Regulatory developments**
    - Instant payments, no thorough verification of transactions
    - PSD3 and PSR
  - Developments of Artificial Intelligence and of new technologies, which enable **new fraud techniques**
- The Working Group will also take into account the acquis of **different workstreams** currently focused on fraud
  - EPC Payment Schemes Fraud Prevention Working Group (PSFPWG) and Payment Security Support Group (PSSG)1 ; and lessons learned at SEPA community level.

1. Introduction: **Structure** and **timeline** of the WG

- **Mandate**: ''The working group is expected to deliver a **mapping of possible actions** concerning the **prevention, mitigation and investigation of fraud** by **different types of stakeholders**, in compliance with data protection requirements and based on an analysis of the current state of fraud for retail payment instruments with a focus on new/emerging fraud modus operandi and techniques.''

The work is **organized in two phases**:

- Phase 1: August – November 2023
  - Subgroup 1: Scope and terminology, number & value
  - Subgroup 2: Fraud manifestations and patterns
    - Two fraud cases: impersonation scam and investment scam
  - Three WG meetings during which the findings of both subgroups have been discussed

- Phase 2: November 2023 – June 2024
  - agreeing on a common set of recommendations
  - November – December: internal reflection of each member organization
  - In-person 17 January meeting: formal launch of discussions for phase 2

1. Introduction: **Participants** and **chairmanship**

Co-chairs
- EACB — Sanne van der Neut
- OCU on behalf of BEUC — Miryam Vivar Goméz

Secretariat
- EACB

Members/alternates
- AGE Platform Europe
- BEUC
- EuroCommerce
- Ecommerce Europe
- EACT
- SMEunited
- Nat. public admin.
- EPC
- EACB
- ESBG
- EBF
- EPIF
- EMA
- ETPPA
- EDPIA

Active participants
- ECB
- Banque de France
- Banca d'Italia
- Banco de Portugal
- Deutsche Bundesbank

Observers
- EC
- EBA
- Europol
- EDPB

1. Introduction: Non-ERPB Members invited to join the Working Group

- **DigitalEurope**
  - 'trade association representing digitally transforming industries in Europe'
  - Corporate members (i.e.: Airbus, Amazon, Bosch, Google…), national trade associations (Ametic, Digital Poland…)
- **DOT Europe**
  - 'the voice of the leading internet companies in Europe'
  - i.e.: Airbnb, Apple, Ebay, Google, TikTok…
- **European Internet Services Providers' Association (EuroISPA)**
  - 'the voice of Internet Services Providers'
  - Council Members (i.e.: Associazione Italiana Internet Providers…); Industry Forum Members (i.e.: Amazon, Facebook, Google, Verizon…)
- **European Telecommunications Network operators' association**
  - 'the voice of Europe's telecommunication network operators since 1992 and has become the principal policy group for European electronic communications network operators'
  - Members (i.e.: Elisa, KPN,…), Observers (i.e.: Nokia)

2. Highlights of conclusions from phase 1

Overview slide of conclusions

Part A: Conclusions after fact-finding on fraud in all its forms

1. Fraud comes in **many different forms** and is described in **many different ways**
2. **Credit transfer fraud is rising** with **higher losses** and the new trend in **social engineering** can **bypass SCA.** Card fraud is in decline due to effective interventions (i.e. SCA & risk-based approach)
3. Fraud results in **financial losses** to consumers, companies, payment providers and authorities. It also results in **lower (digital) self-reliance** and **perceived safety and trust** in society and the digital world.
4. The scale of **fraud cases and loss is likely to grow** over the coming years due to professionalised crime, the modernisation of fraud techniques (i.e. use of AI), continued digitization of society and rise of instant payments.

Part B: Conclusions after deepdive on impersonation scam & investment scam

1. Criminals use **psychological biases** and tactics for impersonation scam and investment scam by creating an **overwhelming sense of urgency** and **coaching** the victims through the payment process, successfully bypassing SCA
2. Various **authorities and institutions** are **impersonated** via evolving attack vectors
3. Europol recognizes **three phases** of impersonation scam: Preparation phase, Execution phase, Completion phase
4. Per phase **different types of tools** are used and different actions take place
5. Per phase **different stakeholders** are involved
6. Criminals **adjust modus operandi continuously** as the examples of investment scam and impersonation bank employee scam show.

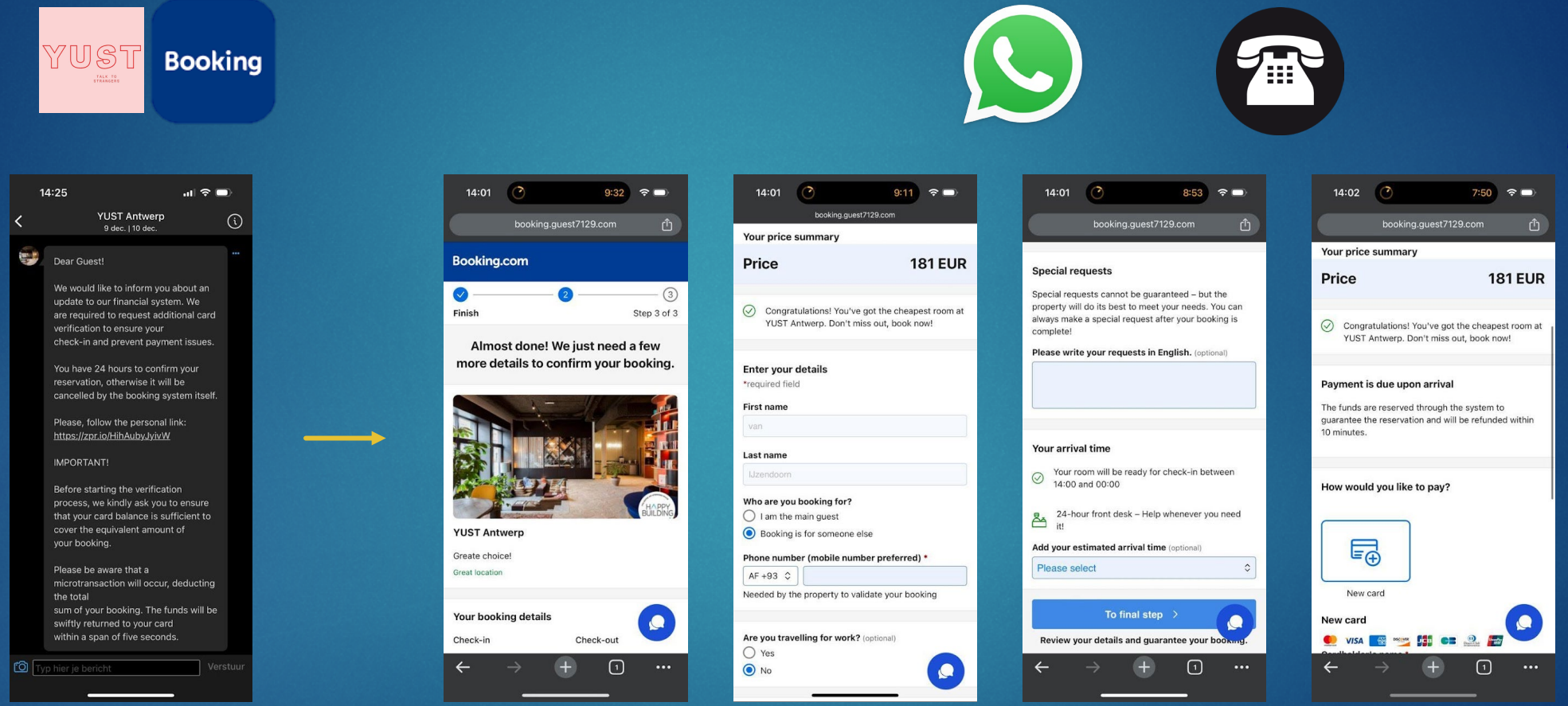
WG Observations and disclaimer on data quality

- European consolidated **reporting is available only delayed** which makes it **difficult to show a current view** on fraud as fraud patterns are changing fast
- Current reports are based on payment methods, **not on fraud modus operandi**, which makes it difficult to make informed conclusions on trend in Europe and local trends in terms of fraud patterns used.
- Quality of reporting varies a lot between countries. The WG welcomes the way forward of the European Commission and the ECB to improve fraud reporting and would welcome more detailed and timely data on fraud patterns included therein.

2. Highlights of conclusions from phase 1

Part A: Conclusions after fact-finding on fraud in all its forms

Visual introduction:
Fraud example from experience of Co-chair



Vectors: Email platform, Booking platform, Hotel, social media & telco, Bank
Enablers: Phishing, lacking 2 factor authentication at booking, AI website builder, authorized CC payment

1.1 Fraud comes in **many different forms** and is described in **many different ways**

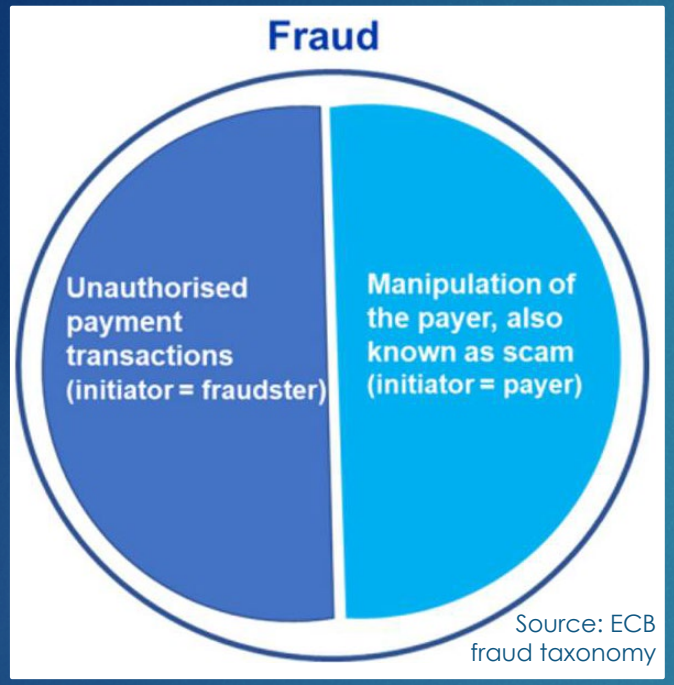
Fraud = *Wrongful or criminal deception intended to result in financial or personal gain* (Oxford Dictionary)

Payment fraud = *Loss of money in a payment process to a fraudulent third party* (Euro Banking Association, 2023)

- Includes related fraud types
  - Identity theft
  - Theft of security credentials
  - Fakeshops & fake investment platforms
  - Impersonation of authorities or trusted individuals
  - Invoice manipulation
- Excludes other fraud types
  - High costs for goods/services (e.g., doorstep selling, unsafe products, poor quality goods on e-commerce platforms.

*

1.2 Fraud comes in **many different forms** and is described in **many different ways**

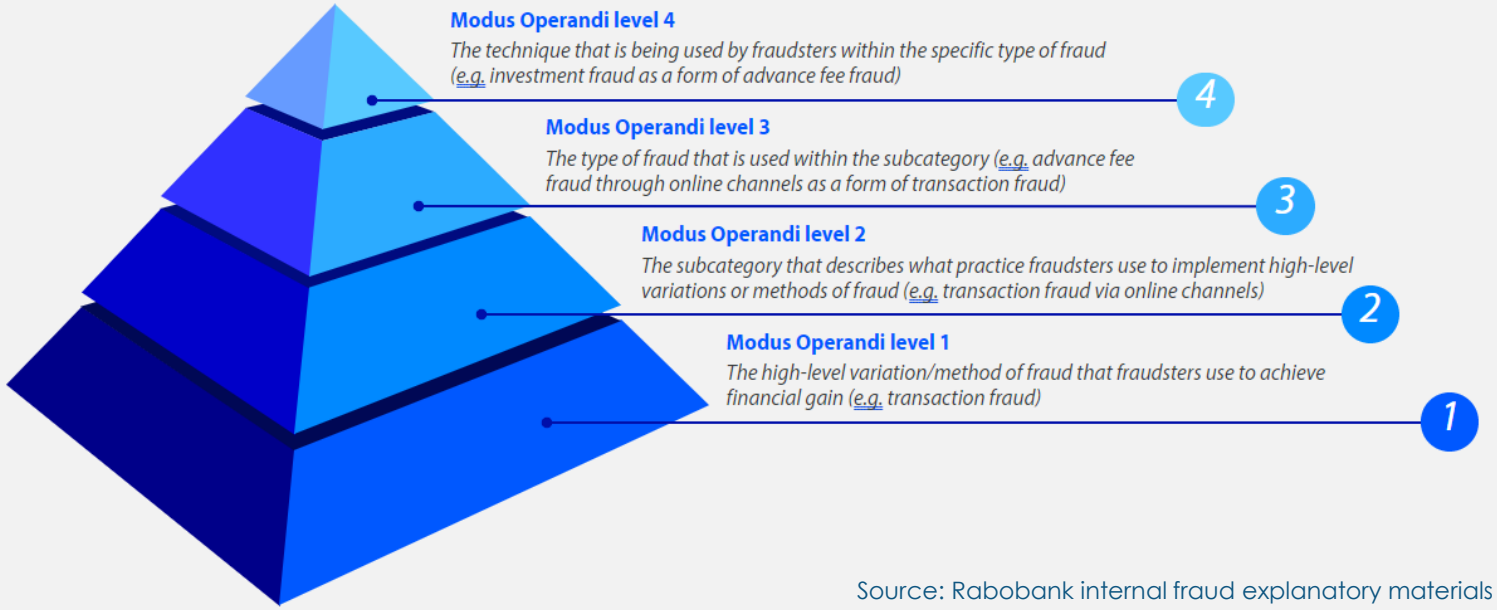


Source: ECB fraud taxonomy

< In some fraud Modus Operandi, the ultimate fraudulent payment transaction is **initiated by the fraudster** (i.e. possible when Strong Customer Authentication is lacking or card hardware can be easily copied). In others the **payer is initiating** a payment they think is valid but turns out to have been deceitful. This second type makes it more **difficult to detect**.

Modus operandi can be described at **multiple levels**, and existing terminologies look at fraud from **multiple perspective** (Modus Operandi, Payment method used), adding to the complexity and challenge of coming to a **common understanding of fraud.** >

Overview of different Modus Operandi levels



Source: Rabobank internal fraud explanatory materials

2. **Credit transfer fraud is rising** with **higher losses** and the new trend in **social engineering** can **bypass SCA.**

Card fraud is in decline due to effective interventions (i.e. SCA & risk-based approach)

Card payments: highest fraud rate but lower average fraud amounts (€73) Losses have steadily been in decline in recent years, mostly due to widespread introduction of Strong Customer Authentication (SCA) and a risk based-approach.

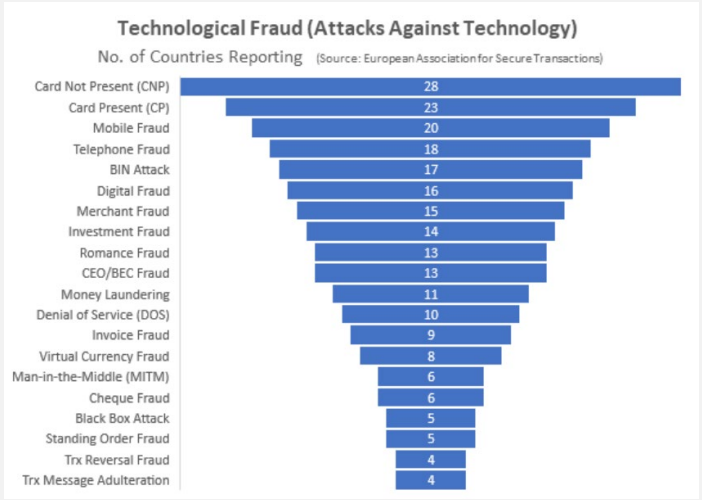
Credit transfers: lower fraud rates but much higher average fraud amounts (€4191) This payment method shows the strongest increase in payment fraud.

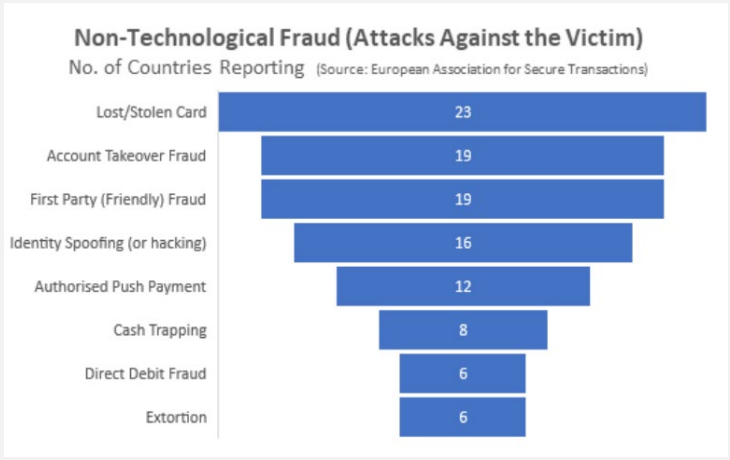
Cash withdrawals: much lower volumes, mostly due to lost and stolen card payments but significant losses (€459)

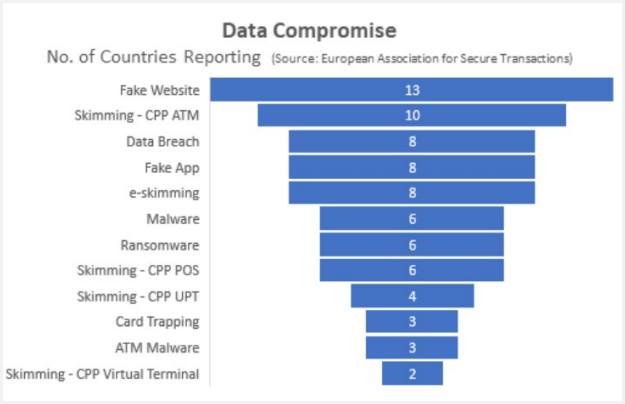
Since 2022 the focus of attacks has shifted towards **social engineering** (EPC, 2022), more often bypassing SCA.

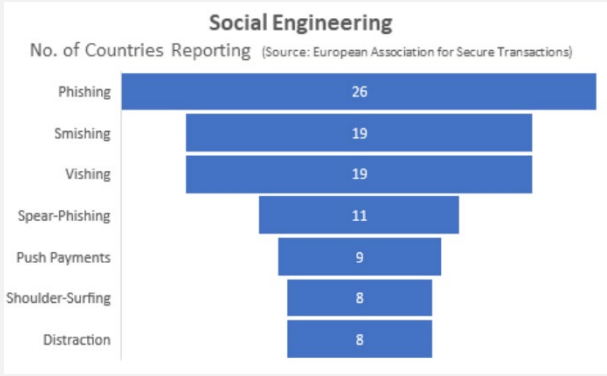
Source: European Banking Authority, Discussion Paper on the EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry, 2022. Numbers reported for H2 2020.
Source: ECB, Report on card fraud in 2020 and 2021, 2023

Overview of relevant payment and terminal crime situations (in 19 SEPA and 8 non SEPA countries









Source: European Association for Secure Transactions (EAST)

3. Fraud results in **financial losses** to consumers, companies, payment providers and authorities.

It also results in **lower (digital) self-reliance** and **perceived safety and trust** in society and the digital world.

National examples:

- Portugal: 14% of Portuguese consumers have already been victims of payment fraud, resulting in average losses of € 155.50 per person according to a study recently released by Adyen, a global financial technology platform.
- France: 15% of French consumers declare having been victim of a scam in 2022, 30% of which relating to payment fraud, 21% to non-delivery of goods and services according to a study by the French consumer organisation UFC Que Choisir
- Belgium: in 2022, an increase in phishing messages resulted in higher losses. A total of €39.8 million was stolen due to phishing, marking an increase from €25 million in 2021, according to Febelfin.

4. The scale of **fraud cases and loss is likely to grow** over the coming years

Due to professionalised crime, the modernisation of fraud techniques (i.e. use of AI), continued digitization of society and rise of instant payments.

Fraud is organized by professional criminal organizations and services:

- **Offenders are not lone actors**
  Offenders are part of a world-wide cybercrime industry supported by the darknet.
- **Offenders are able to adapt quickly** to new technologies and societal developments, while constantly enhancing cooperation and specialization of offenders,
- **Illicit service providers cater** to a large number of criminal actors by offering monitoring, delivery and obfuscation services. **Obfuscation is the technic** that makes impersonation crimes possible.

Modernization of society and fraud and payment techniques add to this growth in scale as well:

- Increased **digitization of society** makes growing (vulnerable) groups more susceptible to fraud
- **Rise of instant payments** reduces time to detect and act toward remediation of lost funds
- **Modernisation of fraud techniques** used by criminals (i.e. deepfakes & AI) make it increasingly difficult for all parties to distinguish real from fake and increase the scale of attacks

Sources: Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023
ERPB WG Fraud Mandate 2023

2. Highlights of conclusions from phase 1

Part B: Conclusions after deepdive on impersonation scam & investment scam

1. Criminals use **psychological biases** and tactics for impersonation scam and investment scam By creating an **overwhelming sense of urgency** and **coaching** the victims through the payment process

- **Fraudsters are opportunistic:** many attempts will fail but people outside their "emotional window of tolerance" i.e. being particularly stressed or tired are likely to fall into the trap
- **Technical elements help them to convince victims:** number spoofing, data leakage allows for precise knowledge on the bank account statement, professional imitation of websites & bank procedures
- **In combination with psychological biases:** fraudsters imitate trusted people or institutions and push victims to pay by creating a sense of urgency and fear to lose money and by coaching them through the payment process incl. bypassing of bank's warnings
- **Fraudsters are professional:** Consumers try to challenge the fraudster with questions but receive convincing answers diminishing their doubts

Source: Which? study – The psychology of scams. Understanding why consumers fall for APP scams

2. New trend is that **various authorities and institutions** are **impersonated** via **evolving attack vectors**

Who is impersonated

Friend / relative in need
Request for support with money transfer or cash/ payment of bail to avoid arrest/ robbery

Member of technical support team
Use of malicious software / remote access tools

Police/tax authority/government
Collection of payment card after phishing call for PIN/ request for money transfer to controlled accounts

Employee of a bank or call center
Request of money transfer to controlled accounts

Alleged Lawyer
Call from person who announces the winning of a prize against payment of an advance fee

Landlord/lady
Deposit and rent for flat/house

How: attack vectors

Phishing/ Vishing/ Smishing:

- Phone / SMS/ email/ letter/ social networks (fake) website
- QR code
- Invoice fraud

Voice or picture spoofing via AI

Stand alone or as part of other scams

3. Europol recognizes **three phases** of impersonation scam: Preparation phase, Execution phase, Completion phase

Preparation	Execution	Completion
Buy data or collect data viaphishing or databreaches	Communicate to victim Mass phoning, SMS, all concealed (VPN, ID caller, spoofed ID)	Cash out money via money mules, card trx, ATM, giftcards, crypto
Buy technical tooling & services	Gain trust & create urgent situation & offer support (via Remote Access Tool)	Block the victims phone or get rid of the phone
Recruit, educate & prepare content MO	Victim transfers money/ visit victim at home to collect card/ scripting	

See also annex: What do criminals do

4.1 Per phase **different types of tools** are used and different actions take place – **Preparation phase**

Gather Know How	• telegram/friends • darkweb
Financial Infrastructure	• money mules/ foreign bank accounts/ installment purchase/ create crypto wallet
Technical Infrastructure	• Account takeover: voicemail hack/ social engineering/ WA-hacking platform • Create new account • Record family member's voice
Information	• Use ongoing conversations • Buy data • Collect open source data
Concealment measures	• Block owner from account • Alternate phone numbers

4.2 Per phase **different types of tools** are used and different actions take place – **Execution phase**

Communicating	• The action starts • Communication with potential victim
Gaining trust	• Social conversation • Becoming a trusted 'identity' • Explain the new number/account
The sting	• Creating a crisis, with time pressure • The fraudster's 'inability to pay' • Personal appeal
Crisis continuation	• Ongoing requests for money • Followed with other types of fraud
Concealment	• The fraudster may use VPN • Rent a hotel room • The fraudster does not remain in one location

4.3 Per phase **different types of tools** are used and different actions take place – **Execution phase**

Cash out	• Cash withdrawal • Supplementary transactions • Setting up gift cards in cryptocurrency
Leave crime scene	• Blocking the victim • Go offline
Concealment	• Threatening the victim if they uncovered the deception • The fraudster remain unrecognizable in their plans • Get rid of telephones • Cash out from a different area

5. Per phase and per type of scam **different stakeholders** are involved

See below an example for **impersonation scam** and the **vectors per phase**

Preparation	Execution	Completion
• Telecom Providers • Search engines • Platforms (e.g. GAFA) • Dark web and internet Forums • Wallet Providers • Domain name providers • Payment service providers *Targets companies for impersonation such as government entities and other services to consumers.*	• Telecom Providers • Internet Service providers • Merchants (fake or genuine) • Remote Access Tool providers • Payment service providers • Schemes • Wallet Providers	• Consumers • Card schemes (e.g. virtual or prepaid cards) • Crypto companies • Cash • Schemes, • Payment service providers • Wallet Providers • Fraudulent merchants or merchant bust-outs

5. Per phase and per type of scam **different stakeholders** are involved

See below examples of the **different vectors** per **type of scam**

Stakeholders bank employee scam	Stakeholders romance scams	Stakeholders investment scam	Stakeholders CEO/BEC fraud	Stakeholders online sales fraud
• Social media platforms • Internet service providers • Telecom providers • Payment service providers • Remote access tool providers	• Consumer • GAFA • money transfers • social media platform	• Consumer • Banks • Payment Institutions • Social platforms • Crypto providers	• Companies • Banks • Payment Institutions • Technical providers (e.g. email security)	• Consumer • GAFA • Social media platforms • (online) Merchants • Payment providers • Online marketplaces

Source: Workgroup research (bank impersonation) & Europol (other four types)

See also annex: What do criminals do

6. Criminals **adjust modus operandi continuously**

See here an example of **Impersonation bank employee scam**

Impersonation bank employee scam

1. The spoofed name, logo and phone number of the bank appeared in the victims telephone screen
2. After the Telecom providers took technical measures to avoid spoofing criminals used look-alike numbers
3. Now all kind of telephone numbers are used and name of bank is mentioned
4. Remote Access tools used
5. Visit home to collect debit card
6. Ask victim to open new account with other bank
7. Script the victim phoning the real bank to deblock the account

6. Criminals **adjust modus operandi continuously**

See here an example of **Investment scam**

"get-rich-quick" investment scam

Part 1

1. Criminals set up
   - **bank accounts,**
   - **recruit money mule networks**
   - **or use previously captured bank accounts.**
2. Criminals ***open companies*** overseas, for example a Call Center.
3. Criminals set up fake ***investment domains*** promising lucrative proceeds.
4. Criminals purchase adverts from
   - **search engines and**
   - **social media platforms,**
   - **and pay for search engine optimisation and advert visibility on the platforms.**
5. Victim looks for investment opportunities with search engines or sees the criminal ads on their social media website.
6. Victim registers.

Part 2: ***APP Investment fraud, Customer does transaction***

7. Victim logs into the fake investment platform and is lured in making more and more investments based on the advertising and fictious profit promises.
8. The website promises apparently large profits, and encourages the victim to send more money.
9. The website may at some point implement limitations on how quickly the profits can be withdrawn from the platform, for example 3 months.
   - ***This happens at the latest on the moment when the victim sends in the first withdrawal request.***
   - ***Some websites may even allow little withdrawals in the beginning, in order to create trust to the victim. Later on withdrawals are not allowed again.***
10. The victim loses all the invested money.
11. Later on the criminal organization may approach the same victim impersonating a law firm who helps victims to get their money back.
    - ***This law firm is set up by the same criminals with the purpose to extract more money from the victim.***

3. Recommended next steps for phase 2

The workgroup is aligned in the observation that the complexity and length of the fraud manifestations and the threat of the expected fraud increase warrants **more cross-sector and public-private collaboration** in order to better prevent the current and expected fraud damage to society. This ERPB workgroup is already providing a welcome basis for this collaboration.

Moving forward, phase 2 aims to deliver:

- *"**…a mapping of possible actions concerning the prevention, mitigation, investigation of fraud by different types of stakeholders, and complaint to the authorities,** in compliance with data protection requirements and based on an analysis of the current state of fraud for retail payment instruments with a focus on new/emerging fraud modus operandi and techniques."*

Thank you for your attention!

Appendix

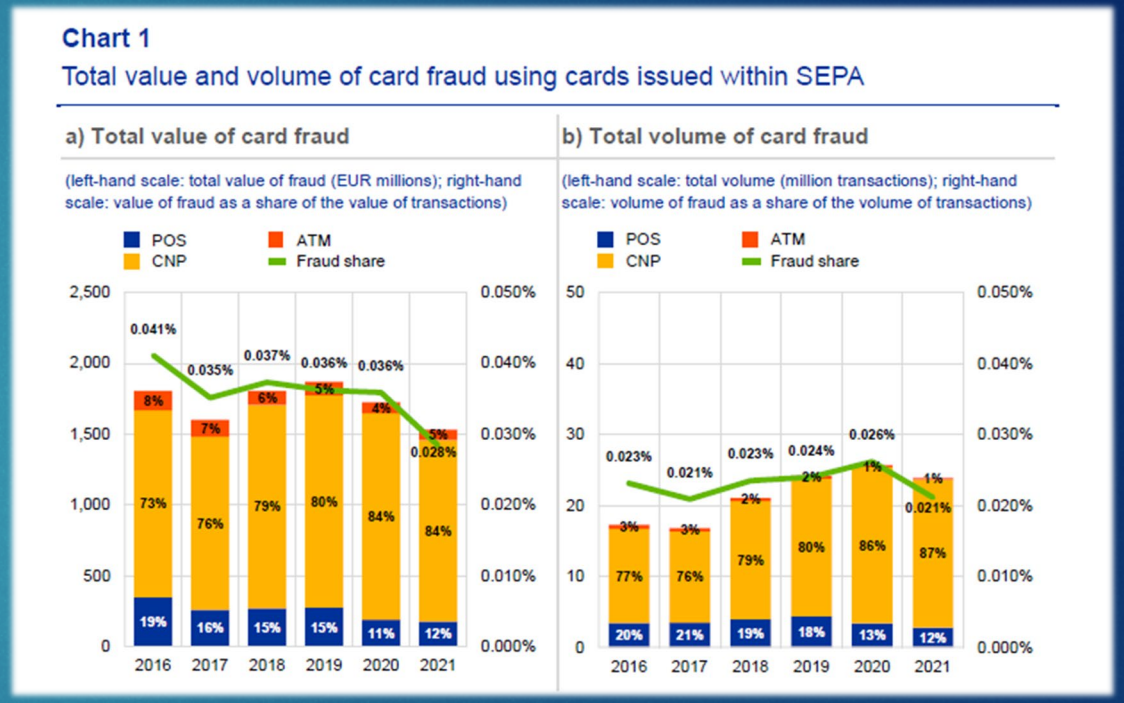
Please find slides on additional supporting statistics or explanation in this appendix, as well as references

References

- Banco de España, Memoria de Supervisión 2022, 2023, LINK
- Banco de España, Memoria de Reclamaciones 2022, 2023, LINK
- Banco de Portugal, Report on payment systems, 2022, LINK
- Banque de France, Observatoire de la sécurité des moyens de paiement Rapport Annuel 2022, 2023, LINK
- Euro Banking Association, Fraud Taxonomy, 2023, LINK
- European Association for Secure Transactions (EAST) report, shared confidentially with the Working Group
- European Banking Authority, Discussion Paper on the EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry, 2022, LINK
- European Banking Authority, EBA Consumer Trends Report 2022/23, 2023, LINK
- European Central Bank, Report on card fraud in 2020 and 2021, 2023, LINK
- European Data Protection Supervisor, TechDispatch 2/2021 - Card-based Payments, 2021, LINK
- European Payments Council, SEPA Credit Transfer, 2023, LINK\
- European Payments Council, 2022 Payment Threats and Fraud Trends Report, 2022, LINK
- Febelfin, Numbers 2022: 'Don't be fooled by a phish', 2023, LINK
- Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023
- Which? study – The psychology of scams. Understanding why consumers fall for APP scams
- EMPACT Online Fraud Schemes (OFS) Operational Action (OA) 7.1

Card payments

- **Decrease in card payment fraud** within SEPA
  - In 2021, lowest level since 2008 (0.028%)
  - After decreasing by 8% in 2020, the value of overall card fraud declined by 11% in 2021
- **Card-not-present** fraud accounts for 84% of total card fraud by value (e.g. via internet)
  - CNP fraud declined by 12% in 2021
- **Card-present** fraud accounts for 16% of total card fraud by value (e.g. at ATMs/POS)
  - CP fraud declined by 42% in 2021 and by 37% in 2020



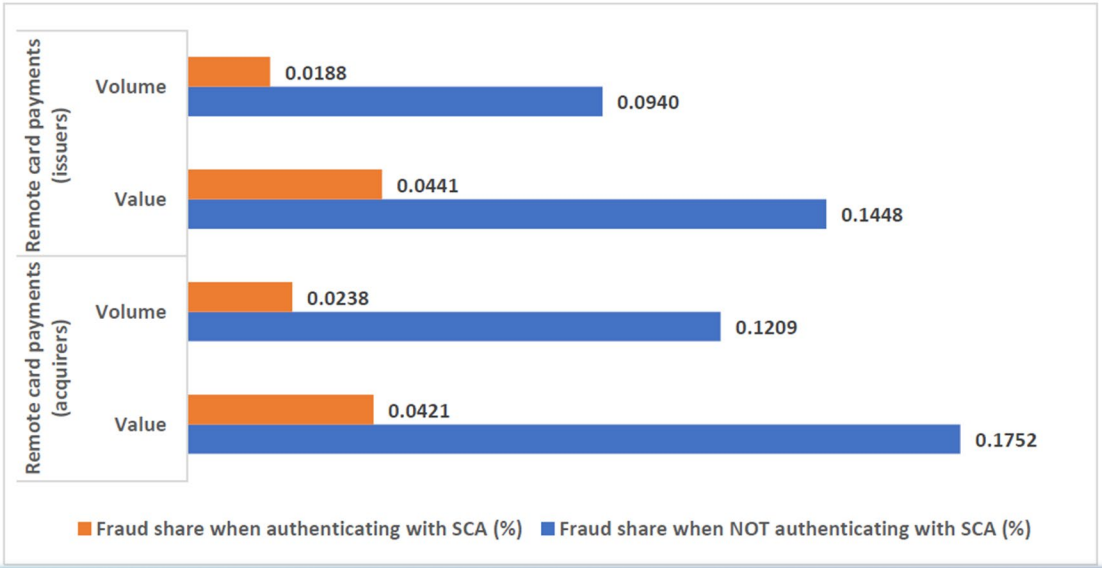
Source: ECB, Report on card fraud in 2020 and 2021, 2023

Card payment = process where a payer uses a credit or debit card to pay for goods or services
Credit transfer = an electronic payment from one payment account to another

Positive impact of Strong Customer Authentication

- Payments authenticated with SCA have **lower** fraud rates both in volume and value than non-SCA payments
- SCA has a positive impact on reducing fraud in both remote and non-remote card payments
- National level examples:
  - **FRANCE:** fraud decreased by 4% in volume and value, to €1.192 billion in 2022 in comparison to 2021
  - **SPAIN:** the fraud rate of online operations in 2022 (0.14%) decreased from 2021 (0.21%)

Figure 8: Fraud rate for remote card payments reported by issuers and acquirers, with and without SCA



Source: EBA, DP on the EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry, 2022

What do criminals do?

- Advertise their services (social platforms, search engine optimisation, websites)
- Communicate to the potential victims (communication tools, emails, spoofing services)
- Hide their identity when communicating (VPN services, bullet proof hosting services, anonymous SIM cards, money mule networks, fake companies to register these services)
- Move the criminal proceeds (bank accounts in both EU and beyond, money mule services for this, and possibly cashing out and breaking the digital trace with crypto currency transactions and mixing services)
- Enjoy their criminal proceeds (move the money back to the financial system with crypto wallet linked payment cards)