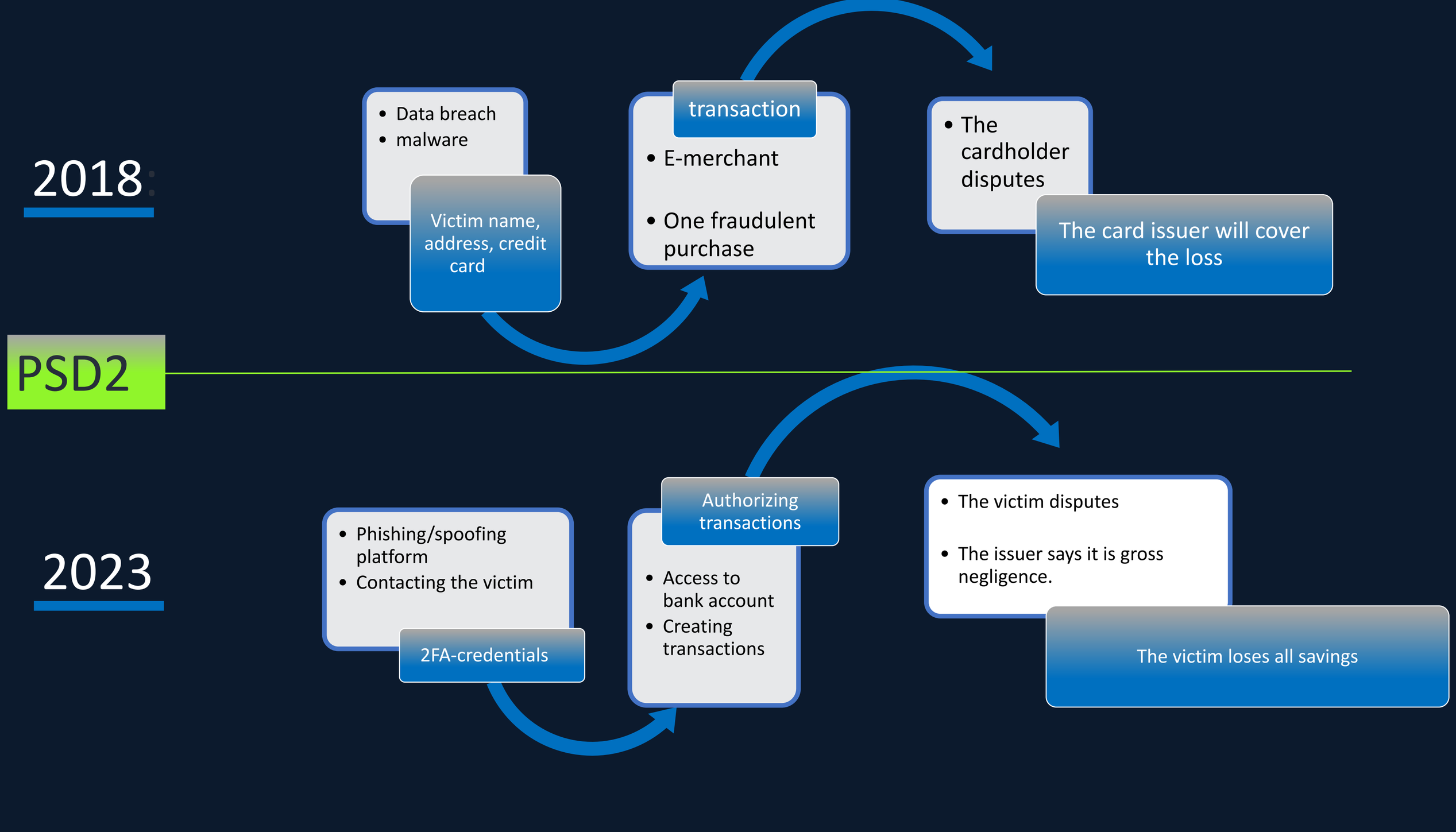


PCI SSC Europe Community Meeting

The Evolving Landscape of payment fraud: A Law Enforcement Perspective on Trends, Challenges, and Solutions

EUROPOL

Europol Unclassified – Basic Protection Level


2018:
• Data breach
• malware
Victim name, address, credit card
transaction
• E-merchant
• One fraudulent purchase
• The cardholder disputes
The card issuer will cover the loss
PSD2
2023
• Phishing/spoofing platform
• Contacting the victim
2FA-credentials
Authorizing transactions
• Access to bank account
• Creating transactions
• The victim disputes
• The issuer says it is gross negligence.
The victim loses all savings

KEY FINDINGS & COMMON ELEMENTS

Online fraud schemes target private individuals, businesses and public sector organisations

AI tools and deepfakes are expanding social engineering opportunities

Citizens are now the direct target

Fraudsters are avid customers of cybercrime as-a-service

Social engineering and impersonation are the most used techniques.

OCGs have access to and make use of money laundering services

Fraudsters leverage new technologies

Re-victimisation of targets is a common practice

KEY FINDINGS

The role of AI as a game changer



Increased efficiency and reach



Increased automation



Misuse of legitimate AI tools (e.g. LLMs)

EMERGING THEATS

MO SIM Boxes

EUROPOL EC3 European Cybercrime Centre



SIM Farm

Group of SIM boxes



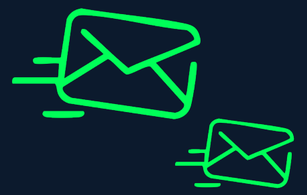
SIM Box

Device that houses hundreds of SIM cards used as part of a Voice-over-IP gateway installation

- Mask communication data
- Makes calls or send SMS messages at cheaper rates



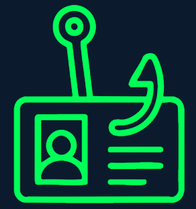
Facilitate the dissemination of thousands of SMS, calls and social media posts to enable large-scale fraud



Global scale
Technology used worldwide to target the EU



Mass-scale anonymity for phishing campaigns
Facilitates bypassing of KYC protocols and subscription to thousands of services simultaneously



Fraudulent platforms can be localised to the targeted country
concealing the fraudsters' identity and location



Europol Unclassified – Basic Protection Level

EMERGING THEATS

Relay Attacks

TERMINAL TO TERMINAL



Shimming device installed in ATM or UPT*



Victim presents card or digital wallet.
PIN is captured e.g via hidden camera



Data transmitted to relay device installed nearby

Transaction data relayed



Data received by relay device in criminal possession



Device presented to ATM or POS* for cashout using captured PIN

Withdrawal by money mule

CARD TO TERMINAL

Social Engineering



Victim deceived into installing malicious app



Victim deceived into presenting card and PIN

Transaction data relayed

UPT - Unmanned Payment Terminal *
POS - Point of Sale

Europol Unclassified – Basic Protection Level

CHALLENGES

- *Underreporting*
- *Jurisdiction*
- *Coordination & efficiency*

Looking Ahead: Fighting payment fraud



Information sharing

- Set up multi-stakeholder platform
- Real-time threat data exchange
- Standardized reporting mechanisms



Regulatory and Policy alignment

- Data protection
- Data retention
- KYC policies
- …



PPP

- Capacity building
- Task forces
- Prevention and awareness



AI Technologies

- Deploy AI for LEAs
- Automated data analysis

Thank you for your attention

Jorge Rosal Cosano

AP Terminal

European Cybercrime Centre (EC3)

Jorge.Rosal-Cosano@europol.europa.eu

EUROPOL

Europol Unclassified – Basic Protection Level