



Scams and Darknet: Securing the network



Bettina Wagner

Director, Security Solutions Lead DACH

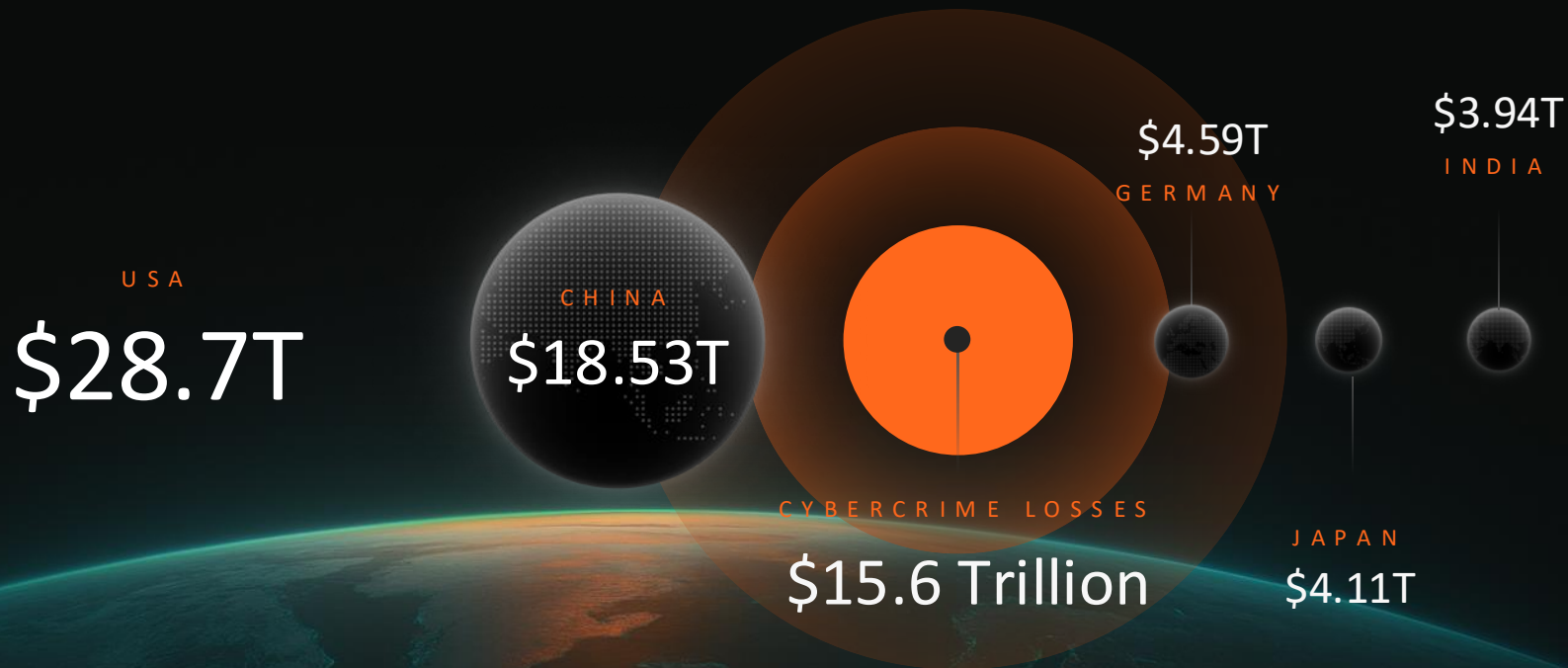
Legal Notice

Disclaimer

The information in this presentation is intended solely to facilitate discussion between the parties, is for informational purposes only and should not be relied upon for the purposes of entering any agreements between the parties. Information in this presentation or in any report or deliverable provided by Mastercard in connection herewith relating to the projected impact on your financial performance, as well as the results that you may expect generally are estimates only. No assurances are given that any of these projections, estimates or expectations will be achieved, or that the analysis provided is error-free. This presentation contains the proprietary and confidential information of Mastercard International Incorporated d/b/a Mastercard Worldwide ("Mastercard"). This information shall be viewed as confidential and is subject to Rule 3.12 of the Mastercard Rules. You shall not disclose the contents of this document or its existence with any third parties or use this document in any manner other than in connection with the relationship with Mastercard. You shall limit dissemination of this document within your company only to those employees or officers who have a need to know for the purposes of enhancing such relationship. By accepting and reading this document, you agree and acknowledge that the contents of this document and the fact and substance related to the existence of this document are confidential and proprietary information of Mastercard.

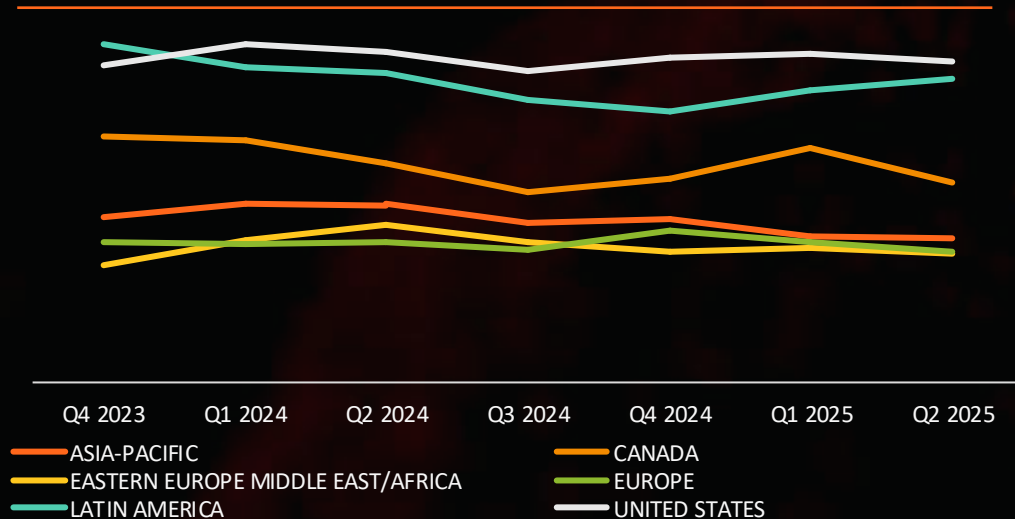


Cyber crime is growing rapidly – losses are almost as big as China's national economy



The fraud level in Europe is among the lowest globally and rather stable with CNP fraud making up the lion's share of overall fraud

**Gross Fraud Rate
(bps, per region)**

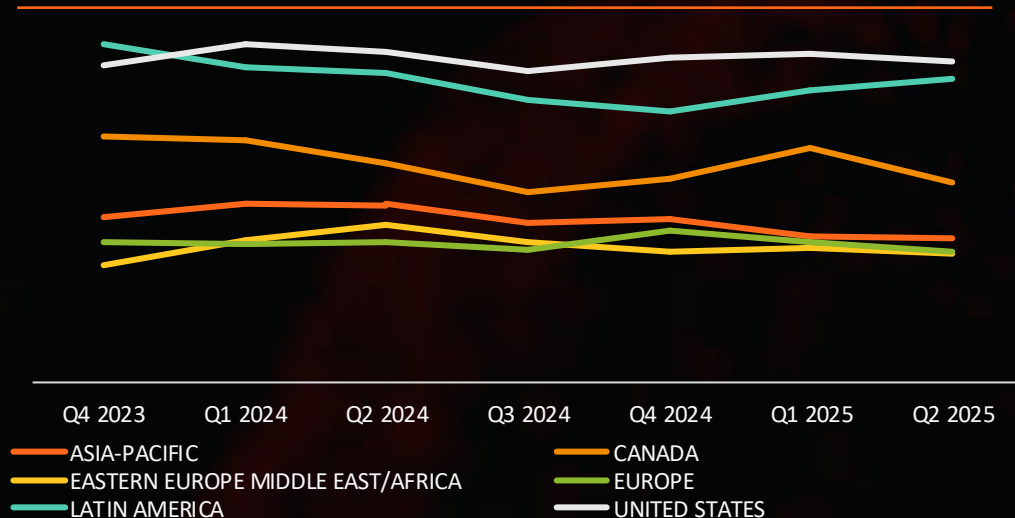


Europe's fraud rate stabilized in Q2 2025, declining 7.5% quarter over quarter and 6.8% year over year



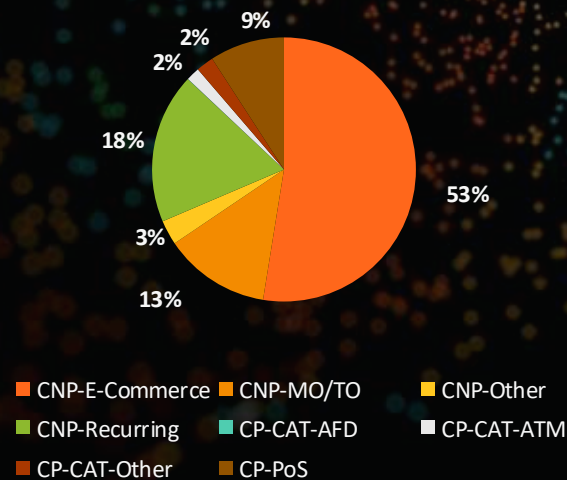
The fraud level in Europe is among the lowest globally and rather stable with CNP fraud making up the lion's share of overall fraud

Gross Fraud Rate
(bps, per region)



Europe's fraud rate stabilized in Q2 2025, declining 7.5% quarter over quarter and 6.8% year over year

EUROPE gross fraud
by channel (USD, Q2 2025)

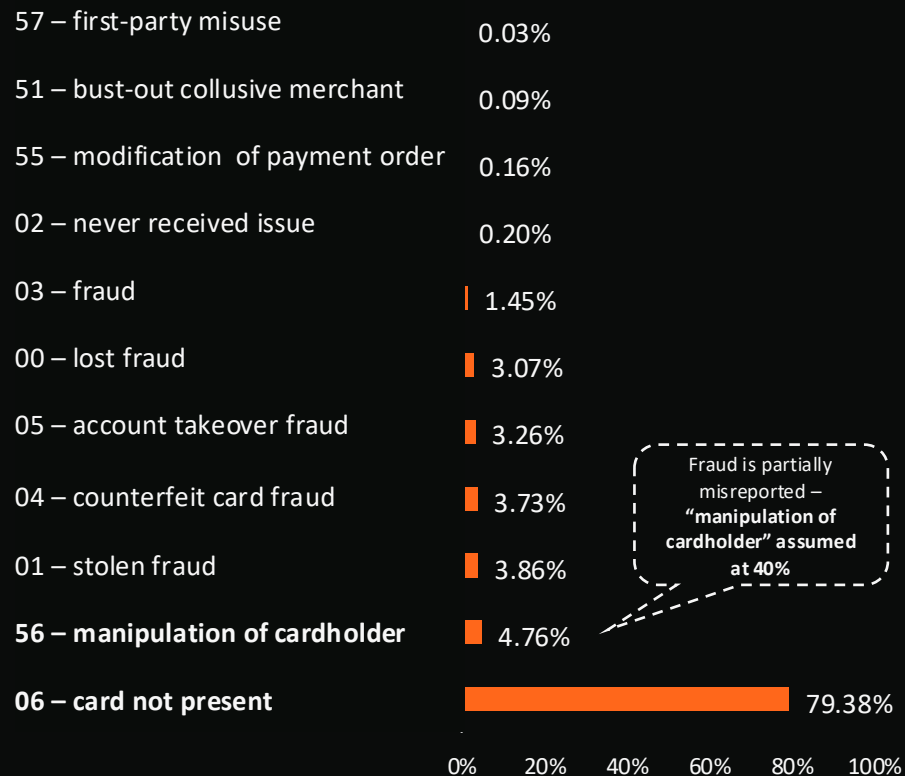


Card-not-present (CNP) fraud remained dominant, accounting for 86.9% of all payment fraud cases, up slightly from 86.6% in Q1 2025



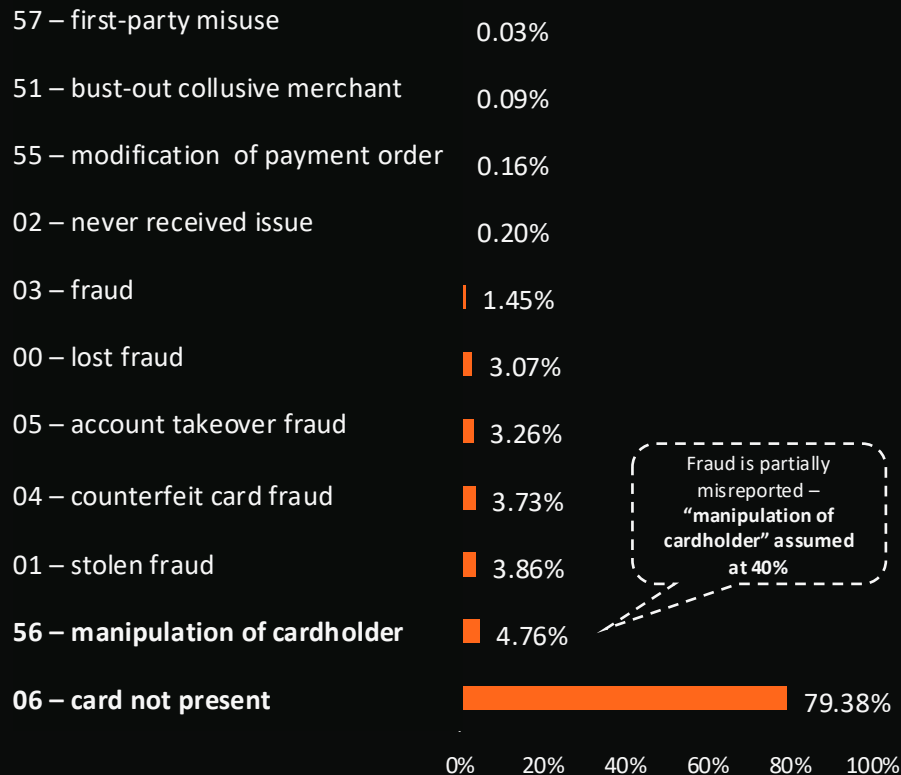
Fraud in Europe is mainly driven by international and no 3DS transactions

% EU total fraud by Fraud Type Code (Q2 2025)

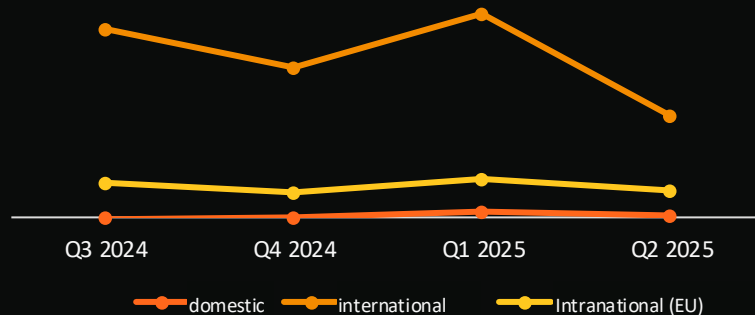


Fraud in Europe is mainly driven by international and no 3DS transactions

% EU total fraud by Fraud Type Code (Q2 2025)

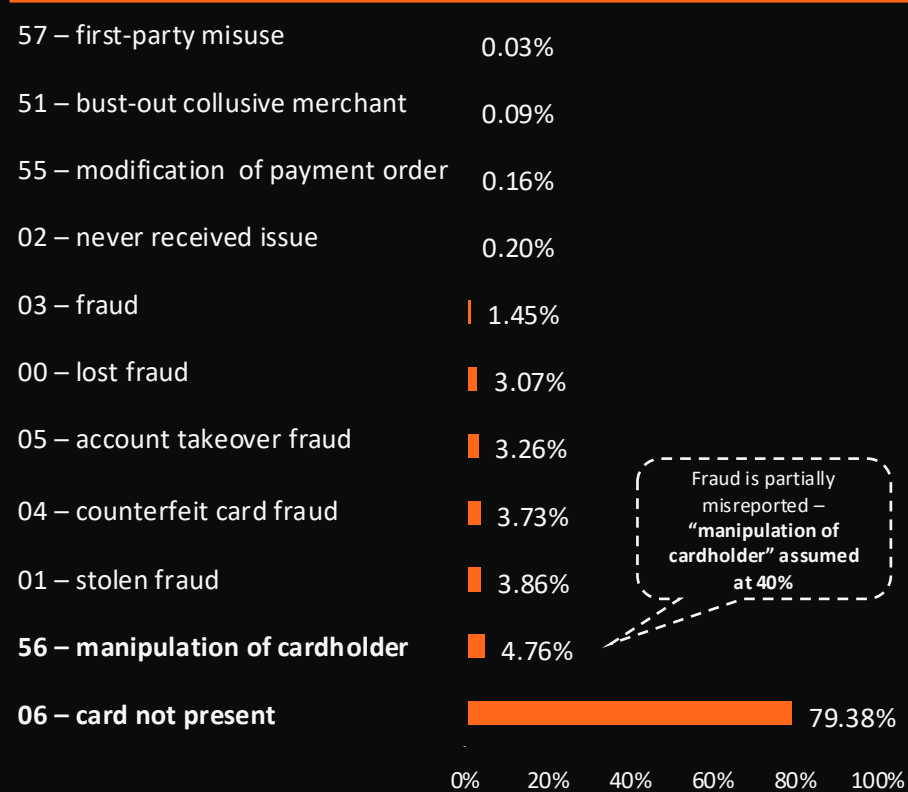


EU gross Fraud by region

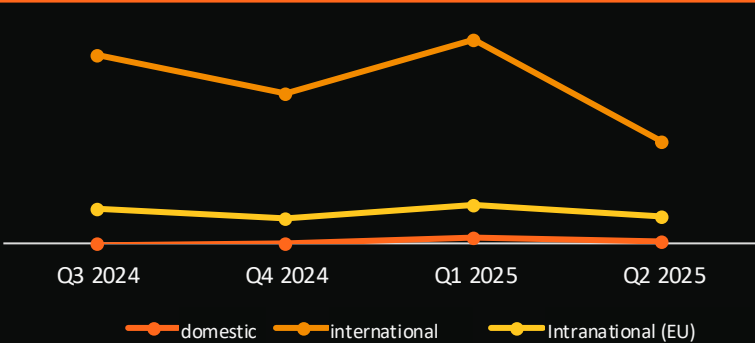


Fraud in Europe is mainly driven by international and no 3DS transactions

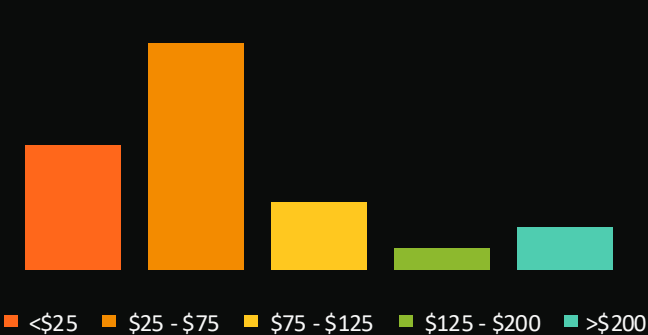
% EU total fraud by Fraud Type Code (Q2 2025)



EU gross Fraud by region



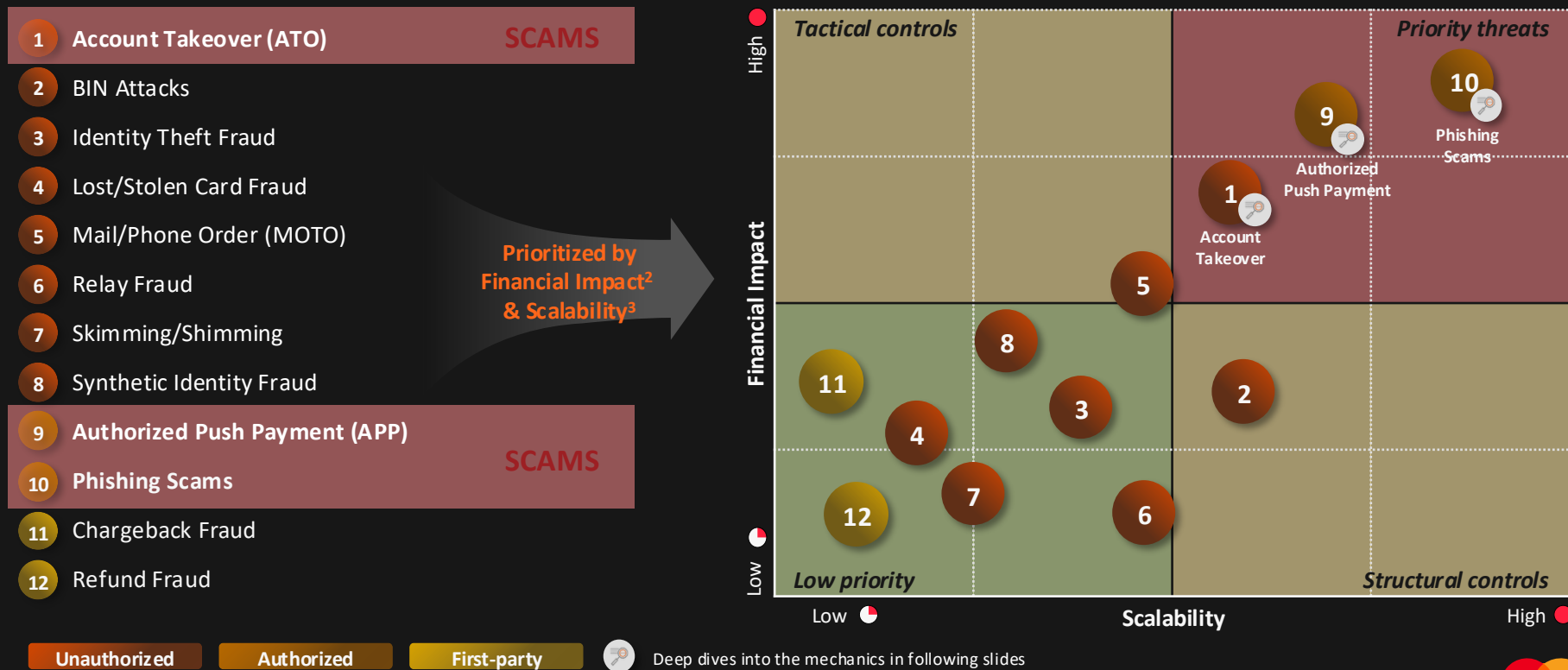
of transactions by fraud amount (Q2 2025)



Phishing Scams, Authorized Push Payment and Account Takeover are the most significant threats in the German market

ENRICHED BY ISSUER INTERVIEWS

Directional threat sizing in Germany per fraud type¹



Unauthorized

Authorized

First-party



Deep dives into the mechanics in following slides

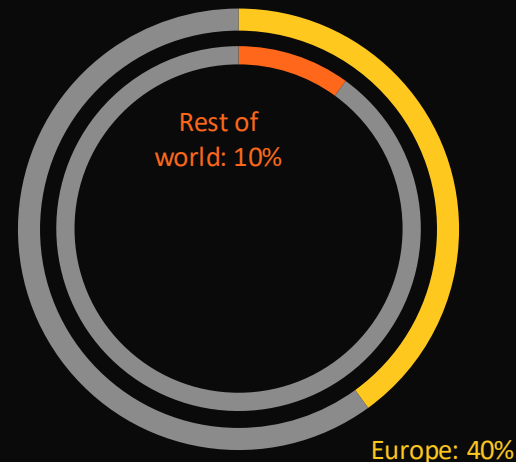
Fraud levels in Europe are significantly lower than in the rest of the world, driven by Europe's leading 3DS adoption rate

Fraud in Europe...

-70%

...is lower than rest of world

3DS adoption rate



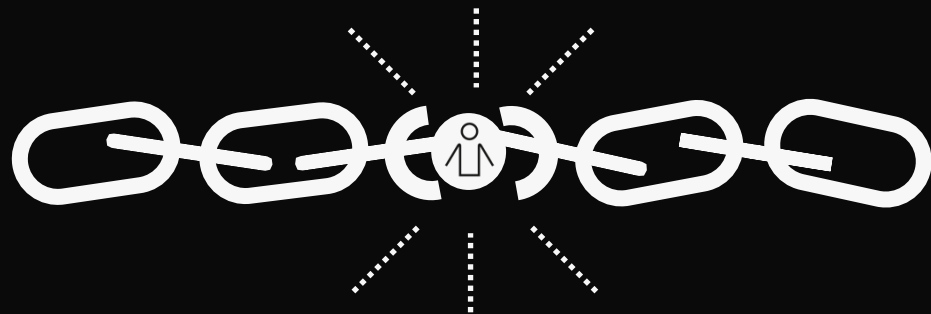
However, stronger authentication security in Europe has shifted fraud towards scams involving genuine customer authentication

Scam Fraud in Europe...

x8

...is significantly higher
than rest of world

The human element remains the weakest link in the chain

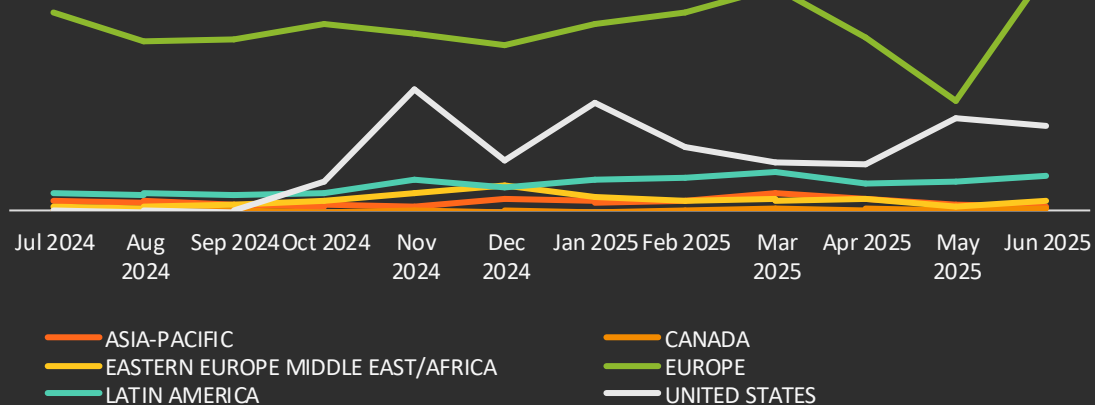


Scams currently present the highest risk, as those transactions are being authenticated by the cardholder



The Economist, 8 February 2025:
Scams present the most dangerous
illegal industry, growing faster than
illegal drug trafficking

Global scam reporting by region



Scams are now the dominant form of digital fraud, with 73% of fraudulent transactions fully authenticated

- Between July 2024 and June 2025, Europe accounted for 57% of reported fraud losses globally and 38% of reported fraud transactions
- The UK leads Europe in reported fraud (34% losses) followed by Sweden and Germany



Scams can be classified into two major categories, challenging existing issuer and acquirer processes

PURCHASE SCAMS



Fraudulent merchants or rogue affiliates **impersonate legitimate businesses** to collect payments for goods or services that are never delivered, significantly misrepresented, or entirely fictitious.

Common Tactics:

- Exploit gaps in acquirer onboarding and KYC verification processes.
- Vanish after collecting payments, leaving issuers and acquirers with chargebacks and unrecoverable losses.
- Erode consumer trust in digital commerce and cause lasting reputational damage.

SOCIALLY ENGINEERED SCAMS



Attackers use **psychological manipulation** to coerce individuals into revealing sensitive information (e.g. card details, credentials, OTP), completing authentication steps, or authorising fraudulent transactions.

Common tactics:

- Phishing / Vishing / Smishing: Fraudulent emails, calls, or texts that impersonate trusted entities.
- Business Email Compromise (BEC): Infiltrating corporate email systems to redirect legitimate payments.
- Romance / Impersonation scams: Building false emotional trust to extract money over time.
- Pretexting: Fabricating a credible scenario to justify requests for confidential data.



Why is the number of
digital scams increasing?



1. Expanding attack surface

As everything becomes interconnected, every connection creates a potential vulnerability



280,000

Cybersecurity vulnerabilities recorded in the EU vulnerability database ²



2. Rising geopolitical threats

Cyberattacks have become a strategic weapon in an increasingly unstable world

6%

of all cyberattacks detected in EMEA in 2024 were driven by espionage³



3. Democratization of cybercrime

More accessible tools enable
higher returns and wider reach

57%

detected threats are Malware-as-a-Service (MaaS), up 17% year over year ⁶



4. The AI acceleration era

Smarter systems operating with greater speed and autonomy

38%



38% of U.S. organizations reported an AI-powered cyberattack within the last 12 months⁴

1/3



of all internet traffic is generated by malicious bots⁵



Fraudsters are using generative AI as a force multiplier

AI simplifies and
automates fraud

AI expands the reach of
fraud into **new regions**

AI enables **unlimited
scalability**

AI enables
Agentic Commerce



As Agentic AI drives a new wave of sophisticated fraud, Mastercard applies advanced intelligence to ensure E-commerce remains secure

Agentic AI used in fraud

Agentic AI is transforming fraud by allowing criminals to automate manipulation, impersonation, and adaptation on a large scale in real time

Emerging Fraud Types Enabled by Agentic AI^{1,2}



Hyper-personalized scams: Deeply personalized scam messages at scale, adapting content in real time based on user behavior



Synthetic identity fraud: Fake identities and documents, bypass controls, and apply for credit or loans using synthetic profiles



Fake merchant fraud: Seemingly legitimate merchants that pass security checks, offering low prices, and harvest payment data for misuse



Agentic AI transforms fraud into **dynamic, self-directed attacks**, making **traditional rule-based controls ineffective** against learning and adaptive agents

Agentic AI used in E-commerce



Human buying
in-store

Human buying
online

AI agent buying
for human, online!

45%

of e-commerce tasks are expected to be handled by agentic AI by 2027³

Mastercard Agent Pay solution applies transaction principles for Agentic Commerce, making it safer and reliable while also reducing fraud risks



Agentic token: Increases safety and security
Masks card number, ties agents to users



Consent capture: Authorizing agent to buy on behalf of the consumer
Purchase confirmation connected to the order



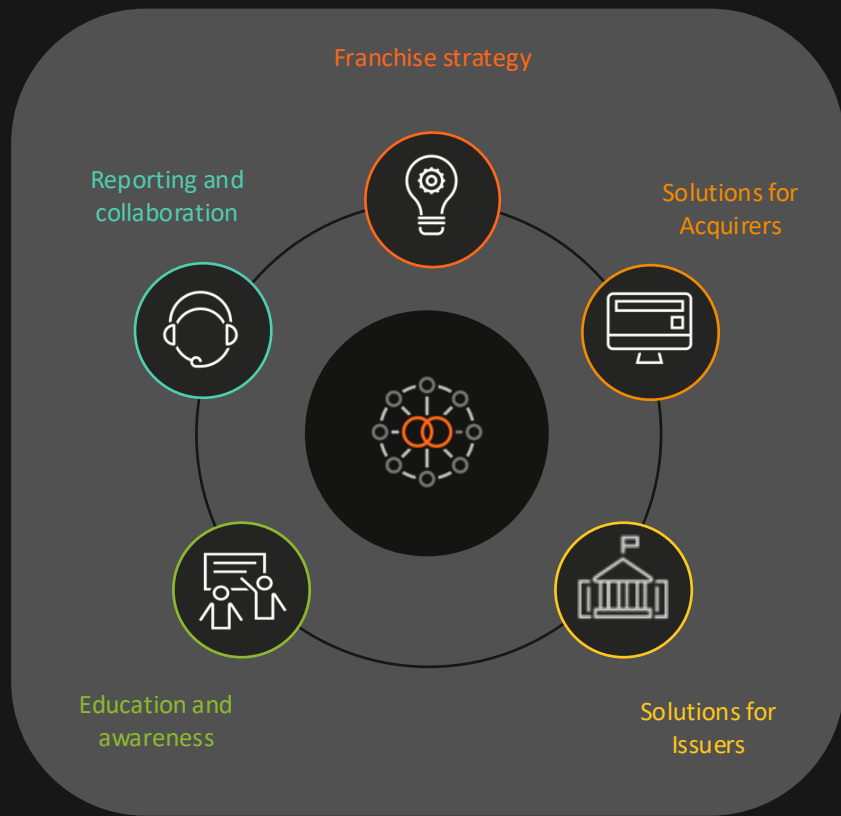
Intent capture: Documents what the consumer wants to buy
Full order details, including items, size and color



How does Matercard tackle
these challenges?



No single player can stop scams alone – success depends on collaboration and partnership across the entire ecosystem



Franchise strategy

- Scam reporting and GRIP alignment, Questionable Merchant Audit Program, MATCH Pro

Solutions for Acquirers

- Acquirer Security Program (Onboarding & Scam merchant monitoring); Merchant Risk Predict

Solutions for Issuers

- DI PRO, Fraud Rule Manager (FRM), Rules Cartridge, Merchant Scam Risk Indicator, MTI, PFI

Education and awareness

- Anatomy of a Scam Series, Scam Protect & Trust Center, Scam Sparks & Dynamic Yield, Global Atiscam Alliance

Reporting and collaboration

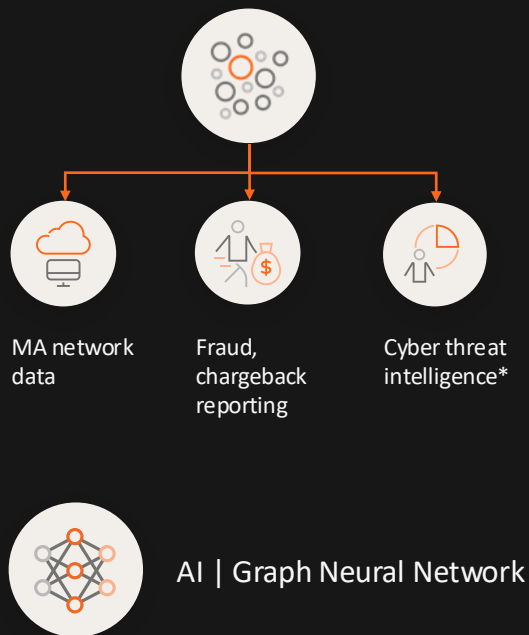
- FLD, Fraud Insights, Purchase Scam Risk Intelligence Exchange*

*In development



Mastercard's expansive view of the payments network enables Merchant Scam and Risk Indicator to provide issuers with predictive merchant risk scores

Data and technology



Merchant Scam and Risk Indicator (MSRI)

95A

- **Merchant-level score** on all merchants (~200m) provided at sub-MID level
- **2-digit predictive score** (ranging 00-99)
- **1-digit reason code** identifying driver of the risk
- Delivered within the **auth message**
- **FRM** integration and report

Action



Use predictive merchant-level insight in real-time to enhance fraud strategy



The Token Provisioning Insights (TPI) model enhances fraud detection by providing issuers with a consistent, explainable signal across all wallet types

TPI Score



Devices

Enhances issuers' decisioning by supplementing the wallet's insights (if available/used).



Card on File

Provides the first risk insight available to issuers, leveraging the data provided by the merchant in the model.

Model Outputs



Risk Score

The predicted risk level, ranging from 0 to 9, with 0 being the lowest and 9 being the highest.



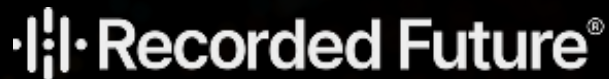
Reason Code

2-character reason code, which explains the rationale behind the score. Reason codes follow an alphabetical scale, with AA representing the highest predicted risk and ZZ the lowest.



Recorded future offers proactive threat detection systems – with Payment Fraud Intelligence identifying stolen card and personal data

Intelligence is the new defense. Insights are the new advantage.



Recorded Future combines intelligence from millions of digital sources to deliver real-time threat insights to nearly 2,000 organizations. Its AI-driven Intelligence Graph enables businesses and governments worldwide to detect threats before they become attacks.

200

BILLION NODES

50

BILLION ENTITIES

150

MILLION REFERENCES



Fraud doesn't happen at a single point, so neither does Mastercard's protection.

By applying intelligence and risk assessment at **multiple stages of the transaction journey**, Mastercard helps **prevent fraud before it impacts** customers, merchants, or issuers, creating a **safer and more resilient payments ecosystem for all participants.**

