



The European Fraud Landscape

Welcome to the Visa Insights for Issuers, a new newsletter series where you can dive into Visa's latest perspective on the payments ecosystem. This quarter's edition centres around the key fraud trends across Europe and the risks this brings to you as an issuer.

2022 saw a decline in overall fraud rates and Visa's 2023 risk strategy aims to further advance on last year's progress to:

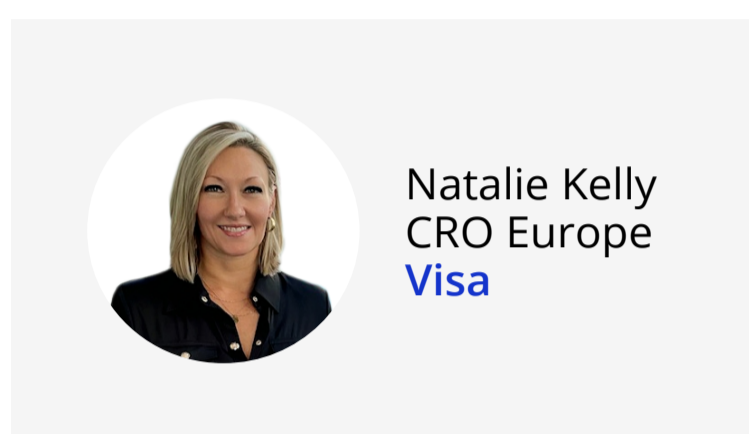
- Protect the transaction
- Empower & protect the consumer
- Protect the client's business

As a valued partner of ours, you will receive a series of communications featuring our most important updates, learning opportunities and strategic recommendations to help you manage your current and future risk priorities.

I look forward to working with you all, to ensure our customers continue to have the best way to pay and be paid, for everyone, everywhere.

Sincerely,

Natalie



Risks to Issuers: Did you know?

80%
of all disputes are due to fraud¹

70%
of all fraud is online¹

99%
of fraudulent transactions occurred on non-3DS rails¹

Despite improvements in mitigating fraud, vulnerabilities remain, and issuers face a continuous battle.

The impact of threats that penetrate the ecosystem can be far-reaching and significant, particularly online. This greatly impacts operational and servicing costs. On top of this, issuers also face reputational damage, decreased revenues and impacted customer satisfaction.

All these issues help to emphasise the importance of a world-class, innovative fraud prevention strategy.

Key Fraud Trends

Fraudsters continue to explore new and tried techniques to commit fraud. The top trends that are contributing to the risks issuers like you face include:



Phishing

285% increase in phishing scams was seen in the first half of 2021 across Europe², with some of the latest trends seeing fraudsters trying to circumvent Strong Customer Authentication.

Fraudsters have been utilising One-Time-Password bypass schemes as well as phishing attempts that use impersonation tactics. Last year, a UK financial institution was targeted by an email attack, impacting over **50,000** customers³.



Malware

5.4 billion malware attacks were detected globally last year⁴, whilst associated card-not-present compromises have increased 4-fold⁵.

As we become more technologically advanced, criminals are using increasingly sophisticated malware to successfully breach defences. In March 2022, one issuer saw an unidentified malware variant infect their user endpoints, enabling access to their customer details⁶.



Purchase return fraud

56% of UK Authorised Push Payment fraud reported in H1 2022 were related to purchase scams⁷.

Card present fraud schemes have once again become a popular tactic with one recent example seeing fraudsters initiate purchases for high-value goods whilst simultaneously requesting cash back as part of the transaction.

1. VisaNet Data, 2022
 2. 2022 Financial Crime Market Outlook | UK & Europe, arachnys, 2022
 3. Fintech Futures, September 2022
 4. Annual number of malware attacks worldwide from 2015 to first half 2022, Statista, 2022
 5. Cisco Annual Internet Report (2018-2023) White Paper, Cisco, 2020
 6. Biannual Threats Report, Visa Payment Fraud Disruption, 2022
 7. 2022 Half Year Fraud Update, UK Finance, 2022

N.B. 3DS rails account for 39% of total transactions