

Payment fraud: an updated analysis

Note for DENARIA Europe

Executive summary

This paper updates recent analyses of payment fraud. Their central thesis —the shift of fraud from face-to-face environments to remote channels— remains valid, but it is incomplete as a description of recent years and emerging trends. The most significant transformation is no longer just the shift from *card-present* to CNP, but the move from fraud based on stolen credentials to the manipulation of the legitimate payer. Strong customer authentication has notably reduced the card fraud it was designed to address, while criminals now induce users to authenticate transfers, share one-time passcodes, enrol compromised cards in digital wallets or invest in fraudulent platforms. The European Central Bank and the European Banking Authority consider that this adaptation requires controls that go beyond traditional authentication (ECB and EBA, 2025). [1]

The best harmonised supranational series available covers the European Economic Area. Fraud reported by payment service providers amounted to €3.4 billion in 2022, €3.5 billion in 2023 and €4.2 billion in 2024. Despite the nominal increase, the aggregate rate remained at around 0.002% of the value of all payment transactions. In 2024, credit transfers generated €2.2 billion in losses, 16% more than the previous year, and cards issued in the EU/EEA accounted for €1.329 billion, an increase of 29%. Users bore approximately 85% of credit transfer losses, mainly as a result of scams that induced them to initiate the payment themselves (ECB and EBA, 2025). [2]

The EEA aggregate rate of 0.002% cannot be compared directly with the global card fraud rate of 0.066% estimated for 2018, nor with the 0.139% projected for 2025. The former divides fraud across multiple instruments by the total value of all payments —including very high-value transfers—, whereas the figures in the original report referred specifically to cards and came from a regional model. The 2020 projection can therefore be neither confirmed nor refuted with current series: there is no official global statistic that replicates, for 2025, the same universe, denominator and estimation procedure.

CNP fraud continues to dominate card losses in the markets that publish a detailed breakdown. In Australia, fraud on locally issued cards amounted to AUD 912.8 million in 2024, equivalent to 0.0788% of spending; AUD 816.36 million was CNP, approximately 89.4% of the total. Although only 3% of spending took place overseas, those transactions accounted for 50% of total fraud. In the United States, the Federal Reserve put the incidence of debit card fraud at 0.108% of transactions in 2023; CNP accounted for 0.061 percentage points, approximately 56.5% of incidents. In the EEA, card fraud was seventeen times higher when the payee was located outside the EEA, where strong authentication is not mandatory and is applied less frequently (AusPayNet, 2025; Board of Governors of the Federal Reserve System, 2025; ECB and EBA, 2025). [3]

Credit transfers and instant payments are the second major area of concern. In the United Kingdom, authorised push payment (APP) fraud losses stood at £450.7 million in 2024, 2% less than in 2023, while the number of cases fell by 20% to fewer than 186,000. Investment fraud was the highest-value type of APP fraud, at £144.4 million, and purchase scams the most frequent, with £87.1 million in losses. 70% of cases began on online platforms and 16% on telecommunications networks, which shows that victims are usually targeted outside the banking infrastructure (UK Finance, 2025). [4]

Cash presents a different risk profile. In the euro area, 444,000 counterfeit banknotes were withdrawn from circulation in 2025, 20% fewer than in 2024 and equivalent to 14 counterfeits per million genuine banknotes. Counterfeiting remains exceptionally low, while cash continues to be relevant: it accounted for 52% of the number of point-of-sale payments in the euro area in 2024, compared with 72% in 2019. It also retains its role in inclusion, privacy and contingency in the event of digital outages (ECB, 2024, 2026). [5]

Mobile payments, BNPL and crypto-assets are the areas with the largest statistical gaps. Mobile money processed more than USD 2 trillion in 2025 and reached 2.3 billion registered accounts and 593 million monthly active accounts, but there is no harmonised global fraud rate comparable to that of the EEA. For BNPL, authorities publish data on usage, default, loan stacking and over-indebtedness, but rarely distinguish account takeover, identity fraud, merchant collusion, refund abuse and first-party fraud. For crypto-assets, Chainalysis estimated that scams and fraud took around USD 17 billion in 2025 and that technical attacks stole more than USD 3.4 billion; these are private estimates, subject to revision and conceptually different from a conventional payment fraud rate (GSMA, 2026; CFPB, 2025; Chainalysis, 2026). [6]

The operational conclusion is that security must expand from authenticating identity to validating intent, the payee and the flow of funds. The priorities are a common statistical taxonomy; confirmation of payee; configurable limits; phishing-resistant authentication; tokenisation; mule account detection; real-time behavioural analytics; signal sharing between banks, merchants, digital platforms and telecommunications operators; rapid freezing and recovery of funds; and liability rules that allocate costs among the actors able to prevent fraud.

Introduction

The digitalisation of payments has reduced transaction costs, broadened financial inclusion and facilitated distance commerce, but it has also radically altered the attack surface. Since 2019, e-commerce, digital wallets, tokenisation, contactless payments, instant transfers, embedded BNPL credit and the retail and institutional use of crypto-assets have become firmly established. The growth of connectivity and financial accounts has simultaneously expanded the universe of legitimate users and that of potential victims.

The Global Findex 2025, based on surveys conducted in 2024 of some 148,000 adults in 141 economies, estimates that 79% of adults worldwide have a financial account, up from 74% in 2021. 86% own a mobile phone and 68% have a smartphone. In low- and middle-income economies, 61% of adults made or received a digital payment, 27 percentage points more than in 2014, and 42% made a digital merchant payment in 2024, up from 35% in 2021. However, only about half of adults with a mobile phone in those economies protect their device with a password, creating a gap between access and security (World Bank, 2025). [7]

The COVID-19 pandemic accelerated pre-existing trends. Mobility restrictions, the temporary closure of shops and the perceived hygiene risk associated with cash boosted e-commerce and digital payments. In developing economies excluding China, around 40% of those who made digital payments from an account said they had done so for the first time after the start of the pandemic. The BIS also observed that digital payments continued to rise, cash withdrawals fell temporarily and fast payment systems became one of the main drivers of growth (World Bank, 2022; BIS, 2021). [8]

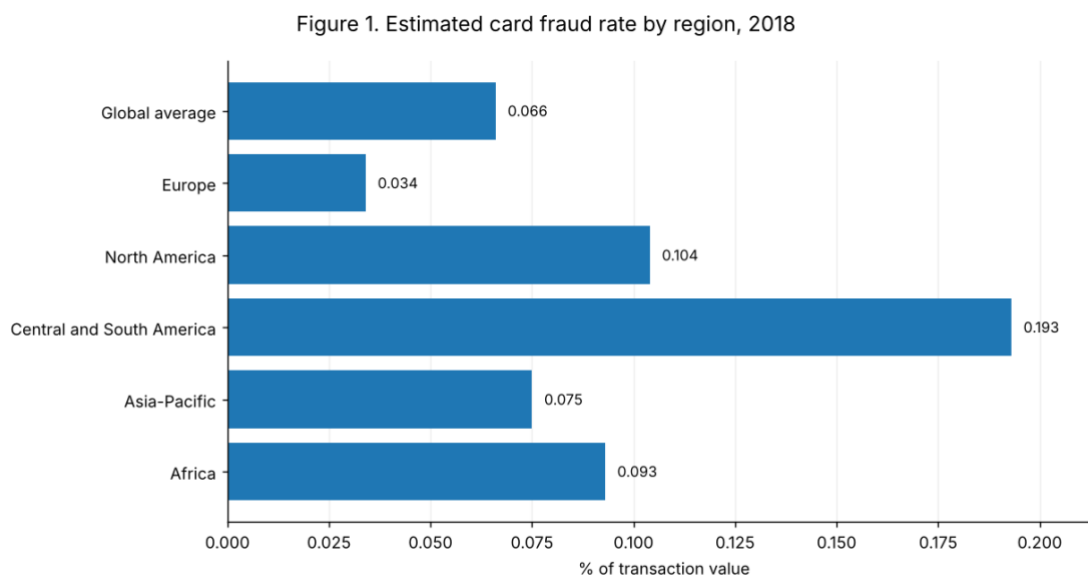
The expansion of the transaction denominator makes it necessary to distinguish between absolute losses and rates. A market can experience higher losses while keeping its fraud rate stable or even reducing it, if legitimate transactions grow faster. It can also have an extremely small rate and yet bear billions in damage because of its scale. This paper therefore distinguishes four indicators:

Indicator	Numerator	Denominator	Interpretation
Rate by value	Value of fraudulent transactions or losses	Total value of transactions in the same universe	Relative monetary risk
Incidence by volume	Number of fraudulent transactions	Total number of transactions	Frequency of fraud
Share by fraud type	Fraud of one type, e.g. CNP	Total fraud in the channel	Composition of fraud
Reported losses	Amount reported or notified	Usually no transaction denominator	Observed harm, subject to under-reporting

A distinction is also drawn between unauthorised fraud, in which the criminal initiates or executes a transaction without valid consent, and authorised fraud (scams), in which the account holder orders the transaction after being deceived. This distinction is essential: strong authentication can correctly confirm the payer's identity without detecting that their intent has been manipulated.

The report published by The Lige in 2020 was an ambitious contribution, building a global picture from fragmented data. In the pages devoted to regional results, it estimated that Central and South America had the highest card fraud rate in 2018, at 0.193%, followed by North America, 0.104%, Africa, 0.093%, Asia-Pacific, 0.075%, Europe, 0.034%, and a global average of 0.066%. In another table it put the global CNP share at 58.19%, with a European high of 69.94%. However, its very design required countries and channels to be filled in through modelling, which calls for caution when comparing it with today's observed regulatory data.

Figure 1. Estimated card fraud rate by region in 2018. The figure reproduces the baseline of the original report; it should not be automatically spliced with later regulatory series, as coverage and denominator change.



Source: Carbó-Valverde and Rodríguez-Fernández (2020). Estimates combining official data, industry sources and econometric imputations; they are not a homogeneous observed global statistic.

Source: The Lige (2020).

The update pursues five objectives. First, to establish whether the predominance of CNP continues. Second, to measure the growing importance of fraud through credit transfers and manipulation of the payer. Third, to compare the risk profiles of cash, cards, mobile payments, e-commerce, BNPL and crypto-assets. Fourth, to assess the impact of COVID-19, regulation and new technologies. Fifth, to propose measures that reduce losses without imposing disproportionate exclusion, surveillance or friction.

Methodology

The research covers the period from January 2019 to 31 July 2026, using 2018 as the baseline to link with the original report. Publications from central banks, supervisory and consumer authorities, international organisations, police forces, payment associations, card schemes and the academic literature were reviewed. Primary or official documents were prioritised; private sources were used where there was no official equivalent or where they provided operational information, which is expressly identified as such.

The hierarchy of evidence applied was as follows: first, data collected under regulatory reporting obligations; second, central bank statistics; third, national payment associations with defined coverage; fourth, police and consumer authority data; fifth, operational data from card schemes; sixth, private estimates; and seventh, academic studies that help interpret exposure, behaviour and causality. This hierarchy does not imply that all official sources are comparable with one another: each figure was examined according to its universe, denominator and definition.

Data collection was organised around seven channels and three cross-cutting dimensions:

Channel	Phenomena included	Phenomena excluded or treated separately
Cash	Counterfeiting, circulation of counterfeit banknotes, contingency role	Modelled shadow economy and crimes paid for in cash
Card-present	Loss or theft, counterfeiting, skimming, terminal use	CNP and e-commerce scams
CNP cards and e-commerce	Stolen credentials, card testing, fake shops, digital skimming	Transfers initiated directly from an account
Credit transfers	Unauthorised fraud, APP, BEC, fake invoices	Card payments settled through card schemes
Mobile payments	Wallets, banking apps, QR, mobile money, carrier billing	Underlying fraud is also attributed to the instrument where applicable
BNPL	Identity, account takeover, collusion, refunds and first-party fraud	Pure credit risk, unless it interacts with fraud
Crypto-assets	Scams paid in crypto, hacks, wallet compromise	General illicit volume presented as if it were payment fraud

The cross-cutting dimensions were the targeting of the victim, the authentication and execution of the payment, and the receipt, dispersal or recovery of the funds.

Four comparability tests were applied. The first checked whether the rate was calculated on value, number of transactions, users or reports. The second distinguished authorised from unauthorised fraud. The third identified whether losses were gross, refunded, recovered or ultimately borne by a particular party. The fourth verified period, currency, geography, instrument and institutional coverage.

Our own calculations were limited to arithmetic ratios within the same source and period. For example, the Australian CNP share is obtained by dividing AUD 816.36 million by the AUD 912.8 million of total fraud on locally issued cards; the approximate CNP share of US

debit card incidents is obtained by dividing 0.061% by 0.108%. These calculations add no new observed information and are identified as derived estimates.

No single global loss figure was constructed. Adding together the EEA's €4.2 billion, US complaints, UK losses and crypto flows would lead to double counting and mix fraudulent payments, scams, hacks and illicit activity. The lack of a harmonised global total is one of the central findings of the study.

Complaint data are interpreted with particular caution. The US Federal Trade Commission received reports of fraud losses totalling USD 12.5 billion in 2024, 25% more than in 2023; USD 2 billion was linked to bank transfers or payments and USD 1.4 billion to cryptocurrencies. These figures reflect consumer complaints, not total fraud in payment networks nor a global population estimate (FTC, 2025). [9]

Similarly, the FBI received 1,008,597 complaints with losses of USD 20.877 billion in 2025, of which cyber-enabled fraud accounted for USD 17.697 billion. Categories included investment fraud, business email compromise, tech support and cases with a cryptocurrency descriptor. The IC3 report is valuable for observing typologies and severity, but it relies on voluntary reporting and is heavily weighted towards the United States; it should not be used as a global per-transaction fraud rate (FBI, 2026). [10]

Results

Summary comparison by channel. The following table presents the latest sufficiently documented indicators. Its rows do not form a homogeneous ranking: some express rates, others losses and another transaction exposure.

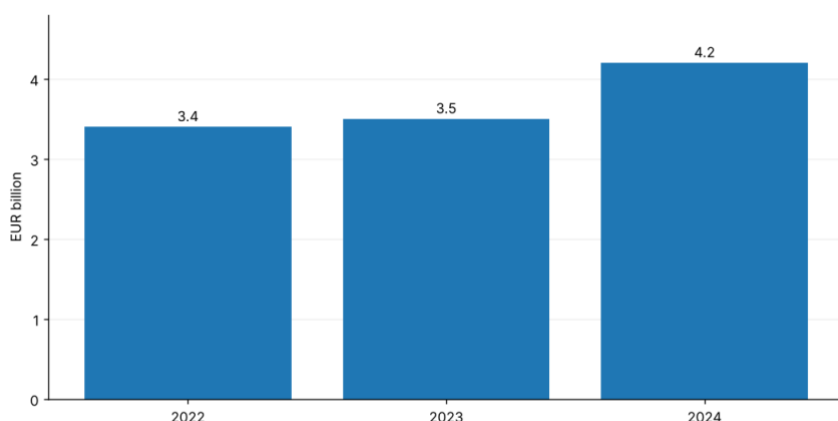
Channel and indicator	Region and period	Share of transactions or exposure	Rate or incidence	Observed or estimated losses	Caveat
All regulated payments	EEA, 2024	All reported instruments	≈0.002% of value	€4.2bn	Aggregate rate dominated by the value of credit transfers
Credit transfers	EEA, 2024	No volume share published in the press release	Not published in a homogeneous form	€2.2bn	Users bore ≈85%
Cards issued in the EU/EEA	EEA, 2024	High-frequency retail instrument	Not summarised in the press release	€1.329bn	+29% year on year
Unauthorised payments	United Kingdom, 2024	3.13 million cases	No total denominator	£722m	Over 98% of victims fully reimbursed
APP	United Kingdom, 2024	<186,000 cases	No total denominator	£450.7m	59% reimbursed over the year as a whole
Locally issued cards	Australia, 2024	Spending: AUD 1.1577 trillion	0.0788% of value	AUD 912.8m	CNP ≈89.4%

Regulated debit	US, 2023	100.7 billion purchases	0.108% by number; 17.6 bp by value	≈USD 17.63 per USD 10,000	Coverage of issuers subject to Regulation II
Counterfeit cash	Euro area, 2025	Not a share of payments	14 counterfeits per million	444,000 banknotes	Does not measure the shadow economy
Mobile money	Global, 2025	>USD 2 trillion processed	No harmonised global rate	Not available	2.3 billion registered accounts
BNPL	US, 2022–2023	Growing use	No harmonised public rate	Not available	Publication focused on credit, not fraud
Crypto scams	Global, 2025	Identified on-chain activity	Not equivalent to a payment fraud rate	≈USD 17bn	Private estimate, subject to revision
Crypto theft through attacks	Global, 2025	Platforms and wallets	No common denominator	>USD 3.4bn	Includes an outlier attack of USD 1.5bn

Sources: ECB and EBA (2025), UK Finance (2025), AusPayNet (2025), Federal Reserve (2025), ECB (2026), GSMA (2026), CFPB (2025) and Chainalysis (2026). [11]

Aggregate trend in the EEA. The increase from €3.4 billion in 2022 to €4.2 billion in 2024 represents cumulative nominal growth of approximately 23.5%. However, the rate remained close to 0.002%, indicating that the total value of transactions grew at a similar pace. Credit transfers accounted for approximately 52.4% of losses in 2024 and cards for 31.6%; the remaining 16.0% corresponds jointly to direct debits, cash withdrawals and e-money. This last percentage is a calculated residual and should not be interpreted as an official figure for each sub-channel (ECB and EBA, 2025). [2]

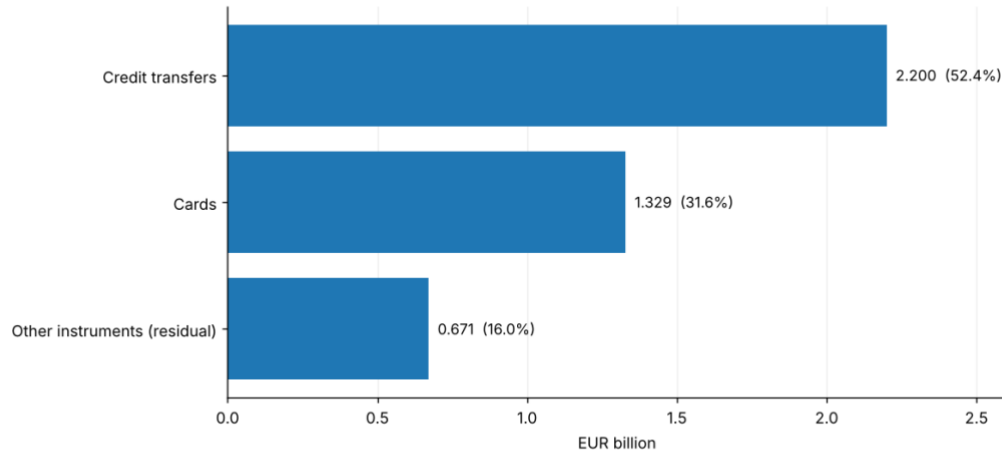
Figure 2. Total reported fraud in the EEA, 2022-2024



Source: ECB and EBA (2025). Fraud reported by payment service providers for credit transfers, direct debits, cards, cash withdrawals and e-money.

Source: ECB and EBA (2025). [2]

Figure 3. Distribution of losses by instrument in the EEA, 2024



Source: own elaboration based on ECB and EBA (2025). "Other instruments" is the residual between the total (EUR 4.2 billion), credit transfers (EUR 2.2 billion) and cards (EUR 1.329 billion); it is not an official breakdown by instrument.

Source: own elaboration based on ECB and EBA (2025). [2]

Regional differences. There is no recent global table in which all regions publish the same rate and definition. The most rigorous comparison is to present the available indicators and flag their lack of homogeneity.

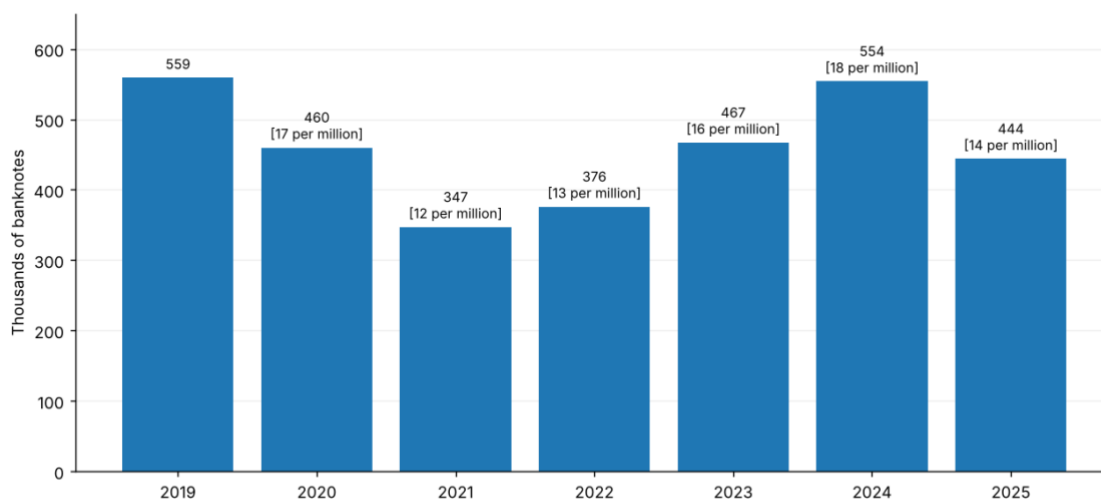
Region	Market feature	Recent indicator	Main takeaway
EEA	PSD2, strong authentication and mandatory reporting	0.002% of value; €4.2bn in 2024	Low aggregate rate, but absolute increase and heavy weight of credit transfers
United Kingdom	Detailed APP and reimbursement statistics	£1.17bn in total in 2024	Victims targeted mainly on platforms and telecoms
Australia	Detailed card breakdown	0.0788% of spending; AUD 912.8m	Cross-border CNP accounts for a disproportionate share
United States	Debit series and consumer complaints	17.6 bp of debit losses; USD 12.5bn reported to the FTC	Important to distinguish payment network data from scam complaints
Euro area	Persistent use of cash and high digitalisation	Cash 52% of the number of POS payments in 2024	Cash is declining but still the majority by number
Sub-Saharan Africa	High mobile money penetration	Main source of new mobile money accounts	Growing scale and poorly harmonised fraud data
South Asia	Major expansion of accounts and digital payments	Almost 80% account ownership	Uneven device security and literacy
Latin America and the Caribbean	Growth in accounts, instant payments and mobile commerce	Account ownership close to 70%	National heterogeneity prevents a single regional rate

Crypto, global	Cross-border and pseudonymous infrastructure	Scams $\approx$ USD 17bn; thefts >USD 3.4bn in 2025	High absolute values, but a different universe from regulated payments
----------------	--	---	--

Sources: ECB and EBA (2025), UK Finance (2025), AusPayNet (2025), FTC (2025), ECB (2024), World Bank (2025), GSMA (2026) and Chainalysis (2026). [12]

Cash. Counterfeiting of euro banknotes fell from 559,000 pieces in 2019 to 460,000 in 2020 and 347,000 in 2021. After the economy reopened it rose to 376,000 in 2022, 467,000 in 2023 and 554,000 in 2024, before falling to 444,000 in 2025. The rate was 12 counterfeits per million in 2021, 13 in 2022, 16 in 2023, 18 in 2024 and 14 in 2025. The 2022–2024 increase should be interpreted partly as a normalisation of face-to-face activity after the pandemic lows, not as a change that makes counterfeiting a risk comparable to digital scams (ECB, 2020–2026). [13]

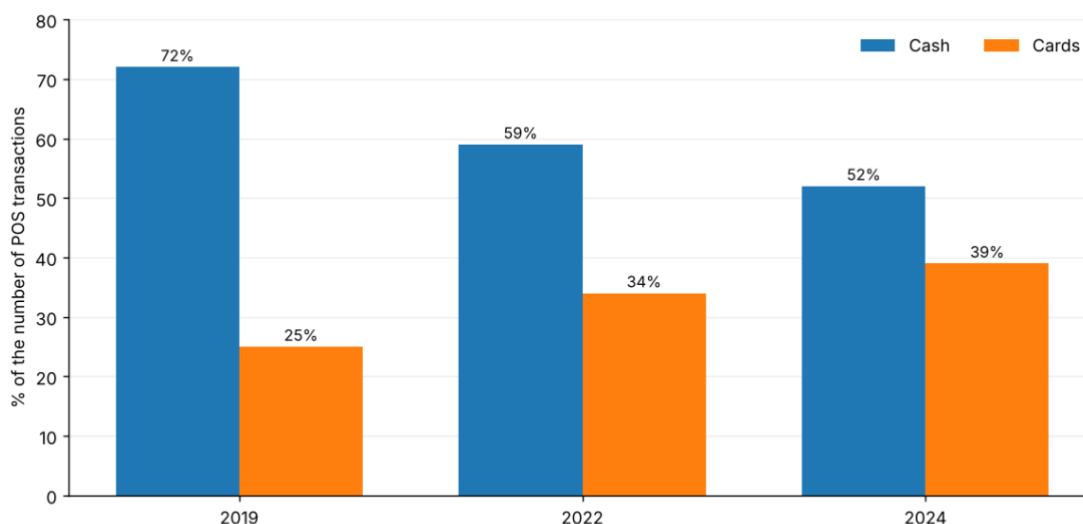
Figure 4. Counterfeit euro banknotes withdrawn from circulation, 2019–2025



Source: ECB (2020–2026). Figures in square brackets show counterfeits per million genuine banknotes. The 2019 rate is not shown because the exact rounded figure is not given in the official text used.

Source: ECB. [13]

Figure 5. Cash and cards in point-of-sale payments in the euro area



Source: ECB, SPACE 2022 and SPACE 2024. Categories do not add up to 100 because mobile payments and other instruments are omitted to keep a consistent comparison over time.

Source: ECB, SPACE 2024. [15]

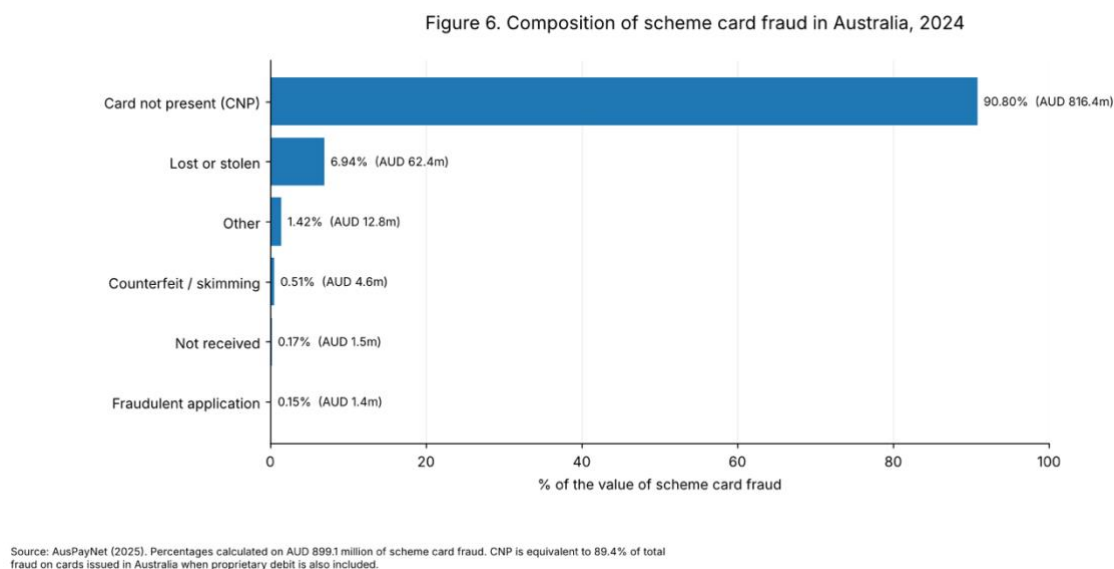
Cash lost market share in the euro area, but it remains the most used instrument by number at the point of sale. In 2024 it accounted for 52% of point-of-sale payments, cards for 39% and mobile payments for 6%. By value, cards accounted for 45%, cash for 39% and mobile for 7%. Online payments reached 21% of the number and 36% of the value of day-to-day payments; within these, cards accounted for 48% and apps or wallets for 29%. 62% of consumers considered it important to retain the option of paying in cash (ECB, 2024). [14]

The original estimate linking cash to an illegal economy of 4.8% of global GDP in 2018 cannot be updated using the counterfeit banknote series or payment statistics. Replicating it would require rebuilding the macroeconomic currency demand model, separating transactional demand from hoarding, controlling for interest rates, taxation, banking structure and informality, and carrying out new national imputations. Presenting a current figure without such a replication would amount to inventing unsupported precision.

Card-present. The roll-out of EMV and dynamic authentication has reduced the appeal of physical counterfeiting and of the face-to-face use of copied data, although loss or theft, skimming, terminal tampering and contactless fraud persist. In Australia, in 2024, losses from lost or stolen cards amounted to AUD 62.44 million and those associated with counterfeiting or skimming to AUD 4.60 million, far below the AUD 816.36 million of CNP fraud. In the United Kingdom, contactless fraud losses fell by 1% in 2024, the first decline since 2020 (AusPayNet, 2025; UK Finance, 2025). [16]

CNP cards and e-commerce. Australia provides some of the clearest evidence of the shift. CNP accounted for approximately 89.4% of total fraud on locally issued cards in 2024. The concentration in cross-border transactions was extreme: international spending was 3% of

the total but generated 50% of fraud; the international CNP rate reached AUD 12.08 per 1,000 spent, compared with 0.97 in the domestic market. This reflects differences in authentication, merchants, acquirers, jurisdiction and recovery capacity (AusPayNet, 2025). [17]



Source: AusPayNet (2025). [17]

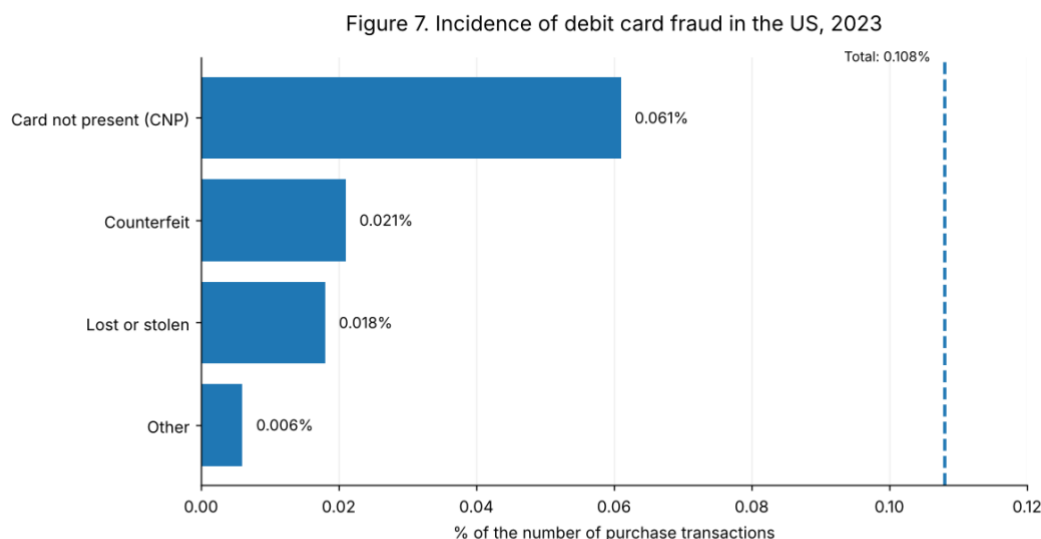
In the United Kingdom, remote purchase fraud grew again in 2024: cases rose by 22% to around 2.6 million, and losses by 11% to just under £400 million. Criminals used social engineering to obtain one-time passcodes, authenticate purchases or enrol compromised cards in digital wallets. In the first half of 2025, CNP cases rose by a further 22%, although total unauthorised losses fell by 3% (UK Finance, 2025). [18]

E-commerce attack vectors frequently precede the transaction. They include fake shops, compromised content management systems, tampering with checkout code, digital skimming, session hijacking, credential stuffing, malware and enumeration or card testing attacks. In 2023, Europol, ENISA and authorities from 17 countries notified 443 merchants that their customers' payment data had been compromised through digital skimming. Mastercard reported in 2025 that malicious domains observed during a six-month trial had affected almost 9,500 e-commerce sites and were linked to some USD 120 million in estimated fraud (Europol, 2023; Mastercard, 2025). [19]

Visa estimates that enumeration attacks generate USD 1.1 billion in fraud a year. Its VAMP programme, effective from April 2025, incorporated enumeration criteria and global fraud and dispute thresholds for acquirers. The network also reported that its tokenisation technology had issued more than 10 billion tokens and prevented USD 650 million in fraud in the year to June 2024. These are operational metrics from a commercial network and should be used as evidence of scale and preventive capacity, not as an independent assessment of causality (Visa, 2024). [20]

US debit and loss allocation. Issuers covered by Regulation II processed 100.7 billion purchases worth USD 4.658 trillion in 2023. Fraud losses for all parties amounted to 17.6 basis points —USD 17.63 per 10,000—, compared with 7.8 basis points in 2011. Incidence by number reached 0.108%: 0.061% CNP, 0.021% counterfeit, 0.018% lost or stolen and 0.006% other types. Merchants bore 49.9% of losses, issuers 28.3% and cardholders 21.8% (Board of Governors of the Federal Reserve System, 2025). [21]

Incidence of debit card fraud in the United States



Source: Board of Governors of the Federal Reserve System (2025), issuers covered by Regulation II. The published types add up to 0.106%, not 0.108%, due to rounding.

Source: Federal Reserve. [21]

Credit transfers and APP. In the EEA, credit transfers have become the channel with the highest absolute reported losses. The €2.2 billion recorded in 2024 far exceeded card losses and grew by 16% year on year. The attribution of 85% of losses to users reflects the fact that many transactions were technically authorised. This undermines an approach based solely on detecting unknown credentials or devices: the session may be genuine, the device the usual one and the code correct, while the payee and the economic purpose are fraudulent (ECB and EBA, 2025). [2]

In the United Kingdom, criminals stole £1.17 billion through authorised and unauthorised fraud in 2024. Of that total, £722 million came from 3.13 million unauthorised cases and £450.7 million from APP fraud. Firms prevented £1.45 billion of unauthorised fraud, equivalent to 67 pence in every pound attempted. 59% of APP losses were returned during the year, while the new mandatory reimbursement rules introduced in October achieved higher reimbursement rates for the cases covered (UK Finance, 2025). [4]

In the first half of 2025, UK APP losses rose by 12% to £257.5 million, even though cases fell by 8%. Investment fraud increased by 55% to £97.7 million, and purchase scams accounted for 72% of APP cases. Online platforms were the source of 66% of cases and 30%

of losses; telecommunications, of 17% of cases. £159.2 million was returned, 62% of the total APP amount, and the regulator reported reimbursement of 88% for transactions covered by the new rules (UK Finance, 2025). [22]

The European Instant Payments Regulation requires providers to offer payee verification free of charge. Before authorisation, the payer's bank must check whether the name provided matches, nearly matches or does not match the holder of the IBAN. The measure began to apply in the euro area in October 2025 and is complemented by the option of setting individual limits for instant transfers. It does not eliminate all fraud—a victim may be deliberately sending money to an account whose holder is indeed the fraudster—but it reduces diversions through IBAN substitution, manipulated invoices and errors (European Union, 2024; Banco de España, 2025). [23]

Mobile payments. The term covers wallets that tokenise cards, banking apps, QR codes, telecom-based mobile money and direct carrier billing. In 2025, mobile money processed USD 2.1 trillion and reached 2.3 billion registered accounts and 593 million accounts active in the previous thirty days. Merchant payments grew by almost 50% to USD 155 billion. Sub-Saharan Africa accounted for most of the new accounts, while South Asia had the largest number of accounts outside that region (GSMA, 2026). [24]

The absence of a harmonised global rate makes it impossible to say what proportion of the USD 2.1 trillion was fraudulent. The main documented vectors are account takeover, SIM swap, device theft, malware, social engineering, dishonest agents, QR code substitution, fake apps and enrolment of compromised credentials in wallets. The GSMA notes that fraud remains widespread and may contribute to users returning to cash, but its summary does not publish a global loss figure from which a rate could be calculated (GSMA, 2026). [25]

The integration of telecom signals is promising. Scam Signal correlates calls or network patterns with suspicious transfers. A UK pilot reported a 30% improvement in detection, and the subsequent roll-out, covering around 85% of UK mobile users, reported improvements of up to 40%. In Spain, Orange, Telefónica and Vodafone launched number verification and SIM swap detection APIs within GSMA Open Gateway. These figures come from the technology's promoters and require independent assessment of false positives and fraud displacement (GSMA, 2024–2026). [26]

BNPL. BNPL fraud can occur at origination—false, synthetic or stolen identity—, during use—account takeover, purchase and resale—, in the relationship with the merchant—triangulation or collusion— and during disputes—refund abuse or first-party fraud—. However, public reporting focuses on credit risk and consumer protection.

In the United States, 21.2% of consumers with a credit record used BNPL in 2022, up from 17.6% in 2021. Approximately 63% of users took out simultaneous loans at some point and 33% used several providers; the average number of originations per user rose from 8.5 to 9.5. These data show fragmentation and the potential for loan stacking, but they are not a measure of fraud. The market report published in December 2025 examined six large providers and confirmed the expansion between 2019 and 2023, without offering a universal per-transaction fraud rate (CFPB, 2025). [27]

The EBA identified payment fraud and indebtedness as the two main issues affecting European consumers in 2024–2025, highlighting the growth of BNPL and other small, fast-access credit. The 2023 Consumer Credit Directive expressly brought many BNPL products within scope, requires creditworthiness assessments and extends information obligations. These measures reduce the risk of over-indebtedness, but they are no substitute for anti-fraud controls or for publishing data broken down by identity, account takeover, merchant and first-party fraud (EBA, 2025; European Union, 2023). [28]

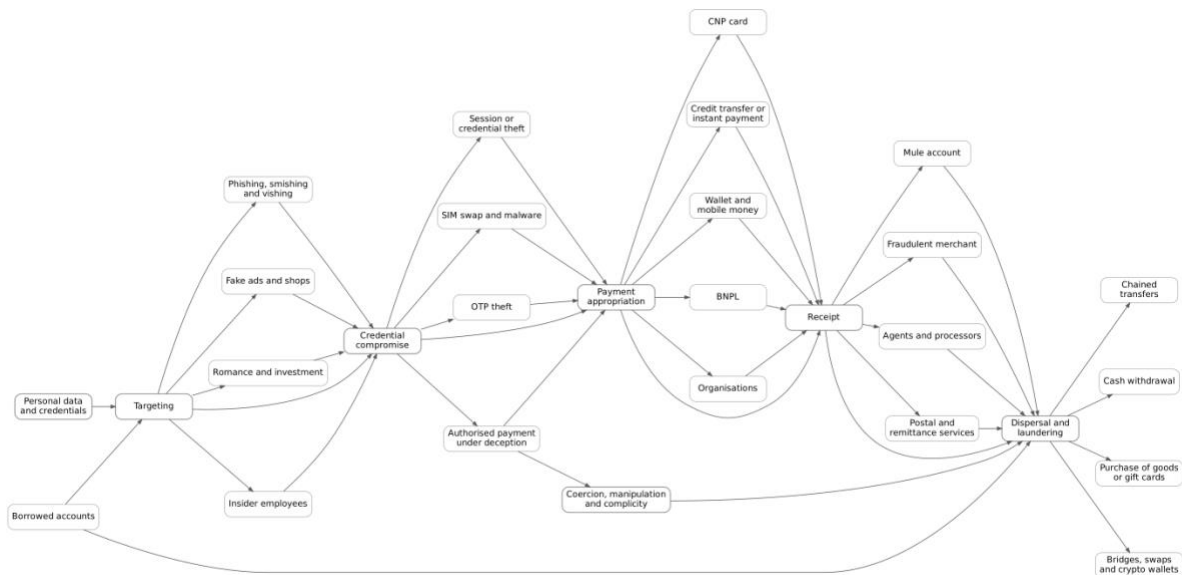
Crypto-assets. Four universes must be distinguished. Scams are payments voluntarily sent by a deceived victim. Hacks are thefts through technical compromise. Funds received by illicit addresses include markets, sanctions, ransomware and other activities. Finally, traditional crimes paid for or laundered in crypto cannot always be identified on-chain alone. Mixing these categories would lead to double counting.

Chainalysis initially estimated that scam addresses received at least USD 9.9 billion in 2024; the figure was later revised to around USD 12 billion as more addresses were identified. For 2025 it observed at least USD 14 billion and projected that the total could exceed USD 17 billion. The average scam payment rose from USD 782 in 2024 to USD 2,764 in 2025. According to the company, operations linked on-chain to AI vendors generated 4.5 times more revenue than those not linked; this relationship is observational and does not demonstrate causality (Chainalysis, 2025–2026). [29]

Technical attacks stole approximately USD 2.2 billion in 2024 and more than USD 3.4 billion in 2025. The attack on Bybit in February 2025 accounted for around USD 1.5 billion, close to 44% of the annual total. According to Chainalysis, actors linked to North Korea were responsible for at least USD 2.02 billion in 2025. The FBI publicly attributed the Bybit attack to North Korea, providing official corroboration for the largest incident, although this does not automatically validate all private attributions (Chainalysis, 2024–2025; FBI, 2025). [30]

The total volume received by illicit addresses reached at least USD 154 billion in 2025, driven largely by an increase in activity associated with sanctioned entities. Even so, Chainalysis estimates that the illicit share of attributed crypto volume remained below 1%. This figure does not contradict the high losses suffered by victims: a small percentage of a growing market can generate significant absolute amounts. Moreover, the estimates are lower bounds subject to retrospective re-attribution (Chainalysis, 2026). [32]

The fraud ecosystem. The following diagram summarises the sequence from targeting to monetisation. Not all cases go through every stage, but the structure shows why the institution executing the payment sees only part of the attack. Europol and INTERPOL document the combination of phishing-as-a-service, social engineering, AI, money mule networks, cryptocurrencies and transnational organisations; INTERPOL also notes the growing link with human trafficking and scam centres (Europol, 2024; INTERPOL, 2024, 2026). [33]



Typologies and controls.

Stage	Main vectors	Most exposed channels	Priority controls
Selection and targeting	Fake ads, phishing, romance, investment, impersonation, deepfakes	Credit transfers, e-commerce, mobile, crypto	Advertiser verification, blocking of domains and numbers, shared intelligence
Compromise	Credential stuffing, info stealers, session hijacking, SIM swap	CNP cards, mobile banking, wallets	Passkeys/FIDO, device binding, session detection and SIM swap API
Credential testing	Enumeration, card testing, micro-charges	Cards and e-commerce	Velocity limits, bot management, enumeration scoring
Authorisation	OTP theft, push bombing, APP manipulation	Cards, credit transfers and mobile	Phishing-resistant authentication, contextual confirmation, limits and pauses
Receipt	Mule accounts, synthetic identity, merchant laundering	Credit transfers, BNPL, cards and crypto	Ongoing KYC, graph analytics, payee reputation
Dispersal	Chained transfers, cash-out, swaps and bridges	All	24/7 freezing, tracing and international cooperation
Dispute	Friendly fraud, chargebacks and refund abuse	E-commerce, cards and BNPL	Standardised digital evidence and first-party fraud detection

Discussion

The evidence confirms that curbing one type of fraud tends to displace activity towards another. EMV, tokenisation and strong authentication made face-to-face fraud and certain

unauthorised CNP transactions more difficult. Criminals responded by attacking the merchant, the session, the device and, above all, the victim's decision-making. The result is a transition from "credential security" to "intent security".

Strong authentication remains effective within its scope. The ECB and the EBA found that transactions verified with SCA were generally less susceptible to fraud, especially for cards. Card fraud was seventeen times higher when the payee was outside the EEA. However, the effect was less clear for credit transfers, because users themselves can complete authentication correctly. There is no contradiction: SCA confirms who is authorising, but not necessarily whether the payment serves a legitimate purpose (ECB and EBA, 2025). [2]

The 2020 projection of a global card fraud rate of 0.139% in 2025 should be considered unverifiable with the available evidence. Comparing it with the EEA aggregate of 0.002% would lead to a denominator error. Nor is it appropriate to compare it with the Australian 0.0788% without adjusting for coverage, currency, cards issued, domestic transactions and year. The methodologically correct update is to replace a modelled global figure with a panel of regional indicators that are explicitly non-equivalent.

CNP remains the main type of card fraud, but its nature has changed. The theft of card numbers and expiry dates coexists with digital skimming, account takeover, automated attacks, enrolment of credentials in wallets and fraudulent shops that obtain payment voluntarily. Some transactions classified as CNP are also the final step in a scam that began on social media or through telecoms; a purely instrument-based classification conceals the origin of the harm.

Credit transfers have become more important than the CP/CNP framework anticipated. The speed and round-the-clock availability of instant systems reduce the time available to detect, hold and recover funds. Confirmation of payee solves part of the problem, but it is insufficient against fake investments, romance baiting or impersonation scams in which the account really belongs to the criminal or to a mule identified under their legal name.

The allocation of losses creates incentives. When users bear 85% of credit transfer fraud in the EEA, the providers involved where the victim is targeted, where the payment is executed and where it is received may not fully internalise the cost. Conversely, automatic reimbursement without investigation may encourage first-party fraud. The UK rules are a significant regulatory experiment because they increase victim protection and require sending and receiving firms to pay closer attention, although their effects on prevention, exclusion and disputes will need to be studied.

Platforms and telecoms are components of the payment system in a functional sense, even though they do not carry out settlement. In 2024, 70% of UK APP cases began on online platforms and 16% through telecoms; in the first half of 2025, the shares were 66% and 17%. Digital origination accounted for a larger share of cases than of losses, while some telephone contacts generated higher average losses. This pattern justifies channel-specific prevention obligations (UK Finance, 2025). [18]

Generative AI increases the capacity to personalise, translate and produce convincing material. INTERPOL warns that language models, cryptocurrencies and phishing services

lower the skills required and the cost of campaigns. Europol expects online fraud to grow faster than other forms of serious organised crime because of AI's support for social engineering and data access. However, claims such as that AI-assisted fraud is 4.5 times more profitable come from observational samples of identified operations and should not be generalised as a universal causal estimate (INTERPOL, 2024, 2026; Europol, 2025; Chainalysis, 2026). [34]

COVID-19 had both temporary and permanent effects. Counterfeiting and face-to-face transactions fell during the lockdowns; when the economy reopened, part of physical fraud recovered. However, e-commerce, contactless payments and app usage remained at structurally higher levels. In the euro area, the share of contactless payments in card transactions rose from 41% in 2019 to 62% in 2022; mobile payments doubled their share between 2022 and 2024 (ECB, 2022–2024). [35]

Regional differences are also differences in observability. The EEA has mandatory reporting under PSD2; the United Kingdom publishes detailed APP statistics; Australia breaks down domestic and cross-border CNP; the United States combines regulatory debit data with complaint systems; mobile money is concentrated in markets where fraud reporting is less homogeneous. A lower rate may reflect greater security, but also different coverage, classification or propensity to report.

Financial education is necessary but not sufficient. A study of 6,207 people in Spain found that greater financial inclusion and product use increased exposure and the likelihood of victimisation; financial knowledge alone did not eliminate the risk. Campaigns should complement, not replace, security by design and institutional responsibility (Rey-Ares, Fernández-López and Álvarez-Espino, 2024). [36]

Cash should not be assessed solely on the basis of its lower traceability. Counterfeiting is rare, and cash provides continuity during power cuts or outages, as well as access for vulnerable people. The ECB describes cash as a “spare tyre” for the payment system. Reducing it without contingency infrastructure could concentrate operational risk and exclude groups with less digital access (ECB, 2026). [37]

European regulation has evolved in three complementary directions. PSD2 and SCA strengthened authentication; the Instant Payments Regulation introduced payee verification and limits; DORA, applicable since 17 January 2025, harmonised ICT risk management, incident reporting and the oversight of critical technology providers. The Consumer Credit Directive extended protection to BNPL. No single measure covers the whole ecosystem, but together they shift the framework from the individual transaction towards identity, infrastructure, the payee and resilience (EBA, 2025; European Union, 2023–2024). [38]

Public policy recommendations

Create a minimum, mandatory global taxonomy. Supervisors should require, for each instrument, the total number and value of transactions; fraudulent number and value; authorised or unauthorised type; presence of authentication; origin of the contact; location of payer and payee; gross losses; recoveries; reimbursements and final burden. The classification should cover cards, credit transfers, wallets, mobile money, BNPL and crypto service providers. The ECB and the EBA show that a harmonised reporting flow is possible; INTERPOL expressly identifies insufficient data as an obstacle to combating fraud globally (ECB and EBA, 2025; INTERPOL, 2024). [39]

Always publish the denominator. Every rate should specify whether it is calculated on value, transactions, cards, users or complaints. Press releases should accompany amounts with total volume, the domestic/cross-border split and methodology. This practice would avoid misleading comparisons between the EEA's aggregate 0.002%, Australia's 0.0788% for cards and losses reported to the FTC.

Extend security to the pre-authorisation stage. Firms should assess the addition of new payees, device changes, active calls, recent SIM swaps, remote control of the device, changes to limits, browsing behaviour and signs of pressure. This information should not automatically trigger refusals, but feed a contextual model with proportionate interventions.

Transform payment confirmation. A generic one-time passcode does not tell the user what is being authorised. Confirmation should show the payee's verified name, amount, purpose, country, whether the recipient is new and specific warnings. Higher-risk transactions may require a second independent confirmation or a cooling-off period, especially for new payees and large investments.

Generalise confirmation of payee. The European model should be extended to standard and instant credit transfers, business payments and, where feasible, cross-border networks. "No match" or "close match" results should be recorded and fed into risk scoring. Users may retain the option to proceed, but the firm should apply additional controls when multiple risk signals coincide.

Allow user-configurable limits. Daily, per-transaction, per-payee and per-channel limits reduce the maximum impact. They should be easy to change, but significant increases may be subject to a waiting period or additional verification. Regulation (EU) 2024/886 expressly recognises this measure for instant credit transfers (European Union, 2024). [40]

Adopt phishing-resistant authentication. Passkeys and FIDO standards, strong device binding, transaction signing and in-app confirmation reduce reliance on SMS OTPs. The migration should retain accessible alternatives for users without a smartphone, with disabilities or in areas with limited connectivity.

Tokenise card credentials and reduce their reuse. Device-, merchant- or domain-specific tokenisation limits the value of stolen data. It should be combined with provisioning controls for wallets, because fraud shifts towards the initial enrolment of the token. Issuers should

show users which device and wallet are requesting enrolment, and check for recent SIM or account changes.

E-commerce security. Merchants should apply script integrity, content security policies, plugin inventories, monitoring of checkout changes, bot management, velocity limits and regular compromise testing. Acquirers and card schemes should monitor enumeration, dispute rates, related merchants and merchant laundering patterns. The actions of Europol concerning 443 merchants and of Mastercard concerning thousands of domains show that fraud often begins in the cyber layer before appearing in the transaction (Europol, 2023; Mastercard, 2025). [19]

Share signals between banks and telecoms. APIs for number verification, SIM change, call status and approximate location can detect manipulation, always subject to data minimisation, purpose limitation and auditing. The Scam Signal pilots are promising, but they should be assessed with public metrics on fraud prevented, false positives and bias (GSMA, 2024–2026). [26]

Make digital platforms accountable. Platforms should verify advertisers of financial products, detect impersonation, retain evidence, respond quickly to indicators of fraudulent accounts and share intelligence with authorities and payment providers. Given that they are the source of most UK APP cases, their contribution cannot be limited to education campaigns.

Tackle mule accounts and the receiving end. Firms should apply ongoing KYC, graph analytics, velocity of inflows and outflows, detection of new accounts with multiple payers, consistency between profile and activity, and controls on repeat payees. The receiving institution is often better placed than the sending one to detect that an account is concentrating payments from unrelated victims.

Build 24/7 freezing and recovery. Instant payments require equally instant alert, hold and return mechanisms. INTERPOL reported that its I-GRIP mechanism had intercepted more than USD 500 million in criminal funds since 2022, demonstrating the value of rapid cross-border cooperation (INTERPOL, 2024). [41]

Design reimbursement to align incentives. Consumer protection should be broad when the victim acted reasonably, with narrow exceptions for proven fraud or gross negligence. The cost can be shared between sending and receiving institutions according to their control failures, and include contributions from platforms or telecoms when the victim was targeted through them. First-party fraud should be monitored through behavioural evidence and an independent complaints process.

Require BNPL-specific metrics. Providers should report identity fraud, account takeover, merchant fraud, refund abuse and first-party fraud; rejected attempts; losses; recoveries; and users' aggregate exposure. Data sharing between providers, with privacy safeguards, would make it possible to detect synthetic identities and simultaneous loan stacking.

Adapt controls to mobile money. Priorities in Africa and Asia include agent protection, SIM swap blocking, secure PINs, withdrawal limits, account recovery, localised education and

coordination between operators. Design should recognise that the phone may be the user's main financial asset and that a forced return to cash may reduce inclusion.

Separate crypto security from the supervision of illicit flows. Exchanges and custodians need robust key management, segregation, multi-signature, independent validation of signing screens, withdrawal limits and vendor oversight. For scams, on-chain analytics, address lists, risk warnings, counterparty verification and coordinated freezing should be combined. For self-custody, wallets should simulate the outcome of contracts and warn about draining permissions or address changes.

Assess anti-fraud technologies causally. Networks report large amounts blocked: Visa stated that it prevented USD 40 billion in attempted fraud in 2024 and USD 350 million through its scam disruption unit; in 2026 it reported USD 2.6 billion identified since the unit was set up. These figures reveal scale, but they are no substitute for evaluations with a comparison group, approval rates, false positives and possible displacement towards other instruments (Visa, 2025–2026). [42]

Preserve cash and contingency arrangements. Secure banknotes, training for professionals, verified machines and reasonable access should be maintained. Digitalisation should not create a single point of failure. Continuity plans should provide for power cuts, telecom outages, cyber incidents and users who cannot use mobile authentication.

Conclusions

Between 2019 and 2026, payment fraud did not follow a linear continuation of the trends estimated for 2014–2018. Digital expansion increased exposure, while EMV, strong authentication, tokenisation and detection models reduced some types of fraud. Criminals responded by shifting towards cross-border channels, e-commerce, account takeover, automation and manipulation of the user.

The available evidence confirms that CNP continues to dominate card losses. In Australia it accounted for approximately 89.4% of fraud in 2024; in US debit it represented around 56.5% of incidents in 2023; in the United Kingdom, remote purchase fraud grew again. The risk is particularly high when the transaction crosses borders or leaves jurisdictions with homogeneous authentication.

The most important new development is the weight of transfers authorised under deception. In the EEA, credit transfers caused €2.2 billion in losses in 2024, and users bore approximately 85%. In the United Kingdom, APP fraud caused £450.7 million in losses, and most cases originated on platforms or through telecoms. This pattern shows that correct authentication does not necessarily mean a legitimate payment.

Cash retains a very low counterfeiting rate and a role in inclusion and contingency. Its smaller share of transactions does not justify equating all cash with the illicit economy, nor mechanically updating the 2018 macroeconomic estimate. Producing a comparable contemporary figure would require fully replicating the monetary model of the original report.

Mobile payments, BNPL and crypto-assets are the main measurement gaps. Their growth is documented, but harmonised denominators and taxonomies are lacking. Crypto-assets offer greater on-chain visibility, although estimates are subject to revision and must separate scams, hacks, money laundering and sanctions. For BNPL and mobile money, the lack of public rates prevents robust comparisons.

The projection of a global card fraud rate of 0.139% in 2025 cannot be validated with current data because there is no equivalent global series. The most rigorous outcome is not to replace it with another synthetic estimate, but to present a panel of regional rates, losses and compositions with complete metadata.

The main conceptual update can be summarised as follows: anti-fraud policy must evolve from credential security to the security of intent, the payee and the flow of funds. Authentication, confirmation of payee, the reputation of receiving accounts, telecom signals, behavioural analytics, rapid freezing, liability sharing and cross-border recovery must operate as an integrated system.

Methodological appendix and references

Glossary

Term	Definition applied
Fraud by value	Fraudulent value divided by the total value of the same instrument and universe
Fraud by volume	Number of fraudulent transactions divided by the total number
Unauthorised fraud	Transaction executed without the payer's valid consent

APP or authorised scam	Transaction ordered by the payer after manipulation
Gross loss	Amount before reimbursement or recovery
Final burden	Amount ultimately borne by the user, institution, merchant or other party
Reported loss	Amount reported to an authority, subject to under-reporting
On-chain illicit flow	Value received by addresses identified as illicit
Crypto theft	Assets stolen through technical compromise of a key, contract or service
CNP	Transaction without physical presentation of the card
CP	Transaction in which the card or its equivalent is presented at the point of sale

References

AusPayNet. (2025). Australian payment fraud report: Calendar year 2024. Australian Payments Network. [17]
European Central Bank. (2020). Euro banknote counterfeiting remained low in the second half of 2019. [43]
European Central Bank. (2021). Euro banknote counterfeiting at historically low level in 2020. [44]

European Central Bank. (2022). Euro banknote counterfeiting at historically low level in 2021. [45]

European Central Bank. (2023). Number of counterfeit euro banknotes remains low in 2022. [46]

European Central Bank. (2024). Study on the payment attitudes of consumers in the euro area — SPACE 2024. [14]

European Central Bank. (2024). Number of counterfeit euro banknotes remains low in 2023. [47]

European Central Bank. (2025). Number of counterfeit euro banknotes continues to be low in 2024. [48]

European Central Bank. (2026). Number of counterfeit euro banknotes remains low in 2025. [49]

European Central Bank. (2026). Annual Report 2025. [37]

European Central Bank, & European Banking Authority. (2025). Joint EBA–ECB report on payment fraud: Strong authentication remains effective but fraudsters are adapting. [2]

Banco de España. (2025). Nuevo servicio gratuito de verificación del beneficiario a partir del 9 de octubre de 2025 [New free payee verification service from 9 October 2025]. [50]

Banco de España. (2026). El número de operaciones de pago con instrumentos distintos del efectivo aumentó un 8,5 % en el primer semestre de 2025 [The number of non-cash payment transactions rose by 8.5% in the first half of 2025]. [51]

Banco de España. (2026). El número de operaciones de pago con instrumentos distintos del efectivo aumentó un 10,8 % en el segundo semestre de 2025 [The number of non-cash payment transactions rose by 10.8% in the second half of 2025]. [52]

World Bank. (2022). The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19. World Bank. [53]

World Bank. (2025). The Global Findex Database 2025: Connectivity and financial inclusion in the digital economy. World Bank. [54]

Bank for International Settlements. (2021). Covid-19 accelerated the digitalisation of payments. Committee on Payments and Market Infrastructures. [55]

Board of Governors of the Federal Reserve System. (2025). 2023 interchange fee revenue, covered issuer costs, and covered issuer and merchant fraud losses related to debit card transactions. [21]

Carbó-Valverde, S., & Rodríguez-Fernández, F. (2020). Fraud in cash and electronic payments: Taxonomy, estimation and projections. International Security Ligue.

Chainalysis. (2024). \$2.2 billion stolen from crypto platforms in 2024, but hacked volumes stagnate toward year-end. [56]

Chainalysis. (2025). 2025 crypto crime trends. [57]

Chainalysis. (2025). Crypto scam revenue 2024: Pig butchering grows nearly 40% year over year. [58]

Chainalysis. (2026). 2026 Crypto Crime Report: Scams. [59]

Chainalysis. (2026). 2026 Crypto Crime Report: Stolen funds. [60]

Chainalysis. (2026). 2026 Crypto Crime Report: Introduction. [61]

Consumer Financial Protection Bureau. (2025). Consumer use of Buy Now, Pay Later and other unsecured debt. [62]

Consumer Financial Protection Bureau. (2025). CFPB research reveals heavy Buy Now, Pay Later use among borrowers with high credit balances and multiple pay-in-four loans. [63]

Consumer Financial Protection Bureau. (2025). The Buy Now, Pay Later market. [64]

European Banking Authority. (2025). Consumer Trends Report 2024/25. [65]

European Banking Authority. (2025). The EBA repeals the Guidelines on major incident reporting under the revised Payment Services Directive. [66]

European Banking Authority. (2025). The EBA amends its Guidelines on ICT and security risk management measures in the context of DORA application. [67]

Europol. (2023). Action against digital skimming reveals 443 compromised online merchants. [68]

Europol. (2024). Internet Organised Crime Threat Assessment — IOCTA 2024. Publications Office of the European Union. [69]

Europol. (2025). Crypto investment fraud ring dismantled in Spain after defrauding 5,000 victims worldwide. [70]

Federal Bureau of Investigation. (2025). FBI attributes \$1.5 billion Bybit virtual asset theft to North Korea. [71]

Federal Bureau of Investigation. (2026). Internet Crime Report 2025. Internet Crime Complaint Center. [10]

Federal Trade Commission. (2025). Consumers reported losing \$12.5 billion to fraud in 2024. [72]

GSMA. (2024). Mobile and banking industries join forces to fight fraud. [73]

GSMA. (2024). Spanish mobile industry to launch online anti-fraud and identity services through GSMA Open Gateway initiative. [74]

GSMA. (2026). State of the Industry Report on Mobile Money 2026. [75]

INTERPOL. (2024). Evaluación de INTERPOL sobre estafas: un peligro mundial incrementado por la tecnología [INTERPOL scam assessment: a global threat boosted by technology]. [76]

INTERPOL. (2024). Financial Fraud Assessment: A global threat boosted by technology. [41]

INTERPOL. (2024). Financial crime operation makes record 5,500 arrests, seizures worth over USD 400 million. [77]

INTERPOL. (2026). Global Financial Fraud Threat Assessment. [78]

Mastercard. (2025). Mastercard introduces threat intelligence solution to combat payment fraud at scale. [79]

Rey-Ares, L., Fernández-López, S., & Álvarez-Espino, M. (2024). Financial literacy and financial fraud victimization in Spain. *International Journal of Bank Marketing*. [36]

UK Finance. (2025). Annual Fraud Report 2025. [4]

UK Finance. (2025). Half Year Fraud Report 2025. [22]

European Union. (2023). Directive (EU) 2023/2225 of the European Parliament and of the Council of 18 October 2023 on credit agreements for consumers. *Official Journal of the European Union*. [80]

European Union. (2024). Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 as regards instant credit transfers in euro. *Official Journal of the European Union*. [40]

Visa. (2024). Introducing the Visa Acquirer Monitoring Program. [81]

Visa. (2024). Visa announces generative AI-powered fraud solution to combat account attacks. [82]

Visa. (2024). Visa issues 10 billionth token, generating \$40 billion in incremental e-commerce globally. [83]

Visa. (2025). Visa unveils its Scam Disruption Practice, helping protect consumers and the financial ecosystem globally. [84]

Visa. (2026). Visa announces latest milestone for pioneering Scam Disruption Unit. [85]

[1] [2] [11] [12] [39]

<https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.pr251215~e133d9d683.et.html>

<https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.pr251215~e133d9d683.et.html>

[3] [16] [17] <https://auspaynet.com.au/resources/fraud-statistics/2024-Calendar-year>

<https://auspaynet.com.au/resources/fraud-statistics/2024-Calendar-year>

[4] [18] <https://www.ukfinance.org.uk/news-and-insight/press-release/fraud-report-2025-press-release>

<https://www.ukfinance.org.uk/news-and-insight/press-release/fraud-report-2025-press-release>

[5] [49]

<https://www.ecb.europa.eu/press/pr/date/2026/html/ecb.pr260227~66abdc6895.mt.html>

<https://www.ecb.europa.eu/press/pr/date/2026/html/ecb.pr260227~66abdc6895.mt.html>

[6] [24] [25] [75] <https://www.gsma.com/newsroom/press-release/mobile-money-accounted-for-2-trillion-in-transactions-in-2025-doubling-since-2021-as-active-accounts-continue-to-grow/>

<https://www.gsma.com/newsroom/press-release/mobile-money-accounted-for-2-trillion-in-transactions-in-2025-doubling-since-2021-as-active-accounts-continue-to-grow/>

[7] [54] <https://www.worldbank.org/en/news/press-release/2025/07/16/mobile-phone-technology-powers-saving-surge-in-developing-economies>

<https://www.worldbank.org/en/news/press-release/2025/07/16/mobile-phone-technology-powers-saving-surge-in-developing-economies>

[8] [53] <https://www.worldbank.org/en/news/feature/2022/07/21/covid-19-boosted-the-adoption-of-digital-financial-services>

<https://www.worldbank.org/en/news/feature/2022/07/21/covid-19-boosted-the-adoption-of-digital-financial-services>

[9] [72] <https://search.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024>

<https://search.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024>

[10] https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[13] <https://www.ecb.europa.eu/press/annual-reports-financial-statements/annual/html/ar2019~c199d3633e.en.html>

<https://www.ecb.europa.eu/press/annual-reports-financial-statements/annual/html/ar2019~c199d3633e.en.html>

[14] [15]

https://www.ecb.europa.eu/stats/ecb_surveys/space/html/ecb.space2024~19d46f0f17.en.html

https://www.ecb.europa.eu/stats/ecb_surveys/space/html/ecb.space2024~19d46f0f17.en.html

[19] [68] <https://www.europol.europa.eu/media-press/newsroom/news/action-against-digital-skimming-reveals-443-compromised-online-merchants>

<https://www.europol.europa.eu/media-press/newsroom/news/action-against-digital-skimming-reveals-443-compromised-online-merchants>

[20] [81] <https://corporate.visa.com/en/sites/visa-perspectives/security-trust/introducing-visa-acquirer-monitoring-program.html>

<https://corporate.visa.com/en/sites/visa-perspectives/security-trust/introducing-visa-acquirer-monitoring-program.html>

[21] <https://www.federalreserve.gov/paymentsystems/2023-interchange-fee.htm>

<https://www.federalreserve.gov/paymentsystems/2023-interchange-fee.htm>

[22] <https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps600-million-stolen-fraudsters-in-first-half-2025>

<https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps600-million-stolen-fraudsters-in-first-half-2025>

[23] [40] <https://eur-lex.europa.eu/eli/reg/2024/886/oj>

<https://eur-lex.europa.eu/eli/reg/2024/886/oj>

[26] [73] <https://www.gsma.com/newsroom/press-release/mobile-and-banking-industries-join-forces-to-fight-fraud/>

<https://www.gsma.com/newsroom/press-release/mobile-and-banking-industries-join-forces-to-fight-fraud/>

[27] [64] <https://www.consumerfinance.gov/data-research/research-reports/the-buy-now-pay-later-market/>

<https://www.consumerfinance.gov/data-research/research-reports/the-buy-now-pay-later-market/>

[28] [65] <https://www.eba.europa.eu/publications-and-media/press-releases/eba-identifies-payment-fraud-indebtedness-and-de-risking-key-issues-affecting-consumers-eu>

<https://www.eba.europa.eu/publications-and-media/press-releases/eba-identifies-payment-fraud-indebtedness-and-de-risking-key-issues-affecting-consumers-eu>

[29] [58] <https://www.chainalysis.com/blog/2024-pig-butcher-scams-revenue-grows-yoy/>

<https://www.chainalysis.com/blog/2024-pig-butcher-scams-revenue-grows-yoy/>

[30] [56] <https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/>

<https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/>

[31] [59] <https://www.chainalysis.com/blog/crypto-scams-2026/>

<https://www.chainalysis.com/blog/crypto-scams-2026/>

[32] <https://www.chainalysis.com/blog/crypto-sanctions-2026/>

<https://www.chainalysis.com/blog/crypto-sanctions-2026/>

[33] [69] <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024>

<https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024>

[34] [76] <https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2024/Evaluacion-de-INTERPOL-sobre-estafas-un-peligro-mundial-incrementado-por-la-tecnologia>

<https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2024/Evaluacion-de-INTERPOL-sobre-estafas-un-peligro-mundial-incrementado-por-la-tecnologia>

[35]

https://www.ecb.europa.eu/stats/ecb_surveys/space/html/ecb.spacereport202212~783ffdf46e.en.html

https://www.ecb.europa.eu/stats/ecb_surveys/space/html/ecb.spacereport202212~783ffdf46e.en.html

[36] <https://ouci.dntb.gov.ua/en/works/4kJjOYW7/>
<https://ouci.dntb.gov.ua/en/works/4kJjOYW7/>

[37] <https://www.ecb.europa.eu/press/annual-reports-financial-statements/annual/html/ecb.ar2025~b7f898b33d.en.html>
<https://www.ecb.europa.eu/press/annual-reports-financial-statements/annual/html/ecb.ar2025~b7f898b33d.en.html>

[38] [66] <https://www.eba.europa.eu/publications-and-media/press-releases/eba-repeals-guidelines-major-incident-reporting-under-revised-payment-services-directive>
<https://www.eba.europa.eu/publications-and-media/press-releases/eba-repeals-guidelines-major-incident-reporting-under-revised-payment-services-directive>

[41] <https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology>
<https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology>

[42] [84] <https://corporate.visa.com/en/sites/visa-perspectives/newsroom/visa-unveils-scam-disruption-practice.html>
<https://corporate.visa.com/en/sites/visa-perspectives/newsroom/visa-unveils-scam-disruption-practice.html>

[43] <https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr200124~242b62d123.en.html>
<https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr200124~242b62d123.en.html>

[44] <https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210122~5b82ddc7b9.en.html>
<https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210122~5b82ddc7b9.en.html>

[45] <https://www.ecb.europa.eu/press/pr/date/2022/html/ecb.pr220128~d65c3326c2.mt.html>
<https://www.ecb.europa.eu/press/pr/date/2022/html/ecb.pr220128~d65c3326c2.mt.html>

[46] <https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230130~98bc45a802.en.html>
<https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230130~98bc45a802.en.html>

[47] <https://www.ecb.europa.eu/press/pr/date/2024/html/ecb.pr240129~fb28ab2918.ro.html>
<https://www.ecb.europa.eu/press/pr/date/2024/html/ecb.pr240129~fb28ab2918.ro.html>

[48] <https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.pr250221~c0d1113d2c.en.html>
<https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.pr250221~c0d1113d2c.en.html>

[50] <https://clientebancario.bde.es/pcb/es/blog/nuevo-servicio-gratuito-de-verificacion-del-beneficiario-a-partir-del-9-de-octubre-de-2025-.html?blog=%2Fwebcb%2FBlog>
<https://clientebancario.bde.es/pcb/es/blog/nuevo-servicio-gratuito-de-verificacion-del-beneficiario-a-partir-del-9-de-octubre-de-2025-.html?blog=%2Fwebcb%2FBlog>

[51] <https://www.bde.es/wbe/es/noticias-eventos/actualidad-banco-espana/el-numero-de-operaciones-de-pago-con-instrumentos-distintos-del-efectivo-aumento-un-85-en-el-primer-semester-de-2025-respecto-al-mismo-periodo-de-2024.html>
<https://www.bde.es/wbe/es/noticias-eventos/actualidad-banco-espana/el-numero-de-operaciones-de-pago-con-instrumentos-distintos-del-efectivo-aumento-un-85-en-el-primer-semester-de-2025-respecto-al-mismo-periodo-de-2024.html>

[52] <https://www.bde.es/wbe/es/noticias-eventos/actualidad-banco-espana/notas-banco-espana/el-numero-de-operaciones-de-pago-con-instrumentos-distintos-del-efectivo->

aumento-un-108-en-el-segundo-semester-de-2025-respecto-al-mismo-periodo-de-2024.html
<https://www.bde.es/wbe/es/noticias-eventos/actualidad-banco-espana/notas-banco-espana/el-numero-de-operaciones-de-pago-con-instrumentos-distintos-del-efectivo-aumento-un-108-en-el-segundo-semester-de-2025-respecto-al-mismo-periodo-de-2024.html>

[55] https://www.bis.org/statistics/payment_stats/commentary2402.htm
https://www.bis.org/statistics/payment_stats/commentary2402.htm

[57] <https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/>
<https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/>

[60] <https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/>
<https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/>

[61] <https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/>
<https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/>

[62] <https://www.consumerfinance.gov/data-research/research-reports/consumer-use-of-buy-now-pay-later-and-other-unsecured-debt/>
<https://www.consumerfinance.gov/data-research/research-reports/consumer-use-of-buy-now-pay-later-and-other-unsecured-debt/>

[63] <https://www.consumerfinance.gov/archive/newsroom/cfpb-research-reveals-heavy-buy-now-pay-later-use-among-borrowers-with-high-credit-balances-and-multiple-pay-in-four-loans/>
<https://www.consumerfinance.gov/archive/newsroom/cfpb-research-reveals-heavy-buy-now-pay-later-use-among-borrowers-with-high-credit-balances-and-multiple-pay-in-four-loans/>

[67] <https://www.eba.europa.eu/publications-and-media/press-releases/eba-amends-its-guidelines-ict-and-security-risk-management-measures-context-dora-application>
<https://www.eba.europa.eu/publications-and-media/press-releases/eba-amends-its-guidelines-ict-and-security-risk-management-measures-context-dora-application>

[70] <https://www.europol.europa.eu/media-press/newsroom/news/crypto-investment-fraud-ring-dismantled-in-spain-after-defrauding-5-000-victims-worldwide>
<https://www.europol.europa.eu/media-press/newsroom/news/crypto-investment-fraud-ring-dismantled-in-spain-after-defrauding-5-000-victims-worldwide>

[71] <https://www.ic3.gov/PSA/2025/PSA250226>
<https://www.ic3.gov/PSA/2025/PSA250226>

[74] <https://www.gsma.com/newsroom/press-release/spanish-mobile-industry-to-launch-online-anti-fraud-and-identity-services-through-gsma-open-gateway-initiative/>
<https://www.gsma.com/newsroom/press-release/spanish-mobile-industry-to-launch-online-anti-fraud-and-identity-services-through-gsma-open-gateway-initiative/>

[77] <https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-financial-crime-operation-makes-record-5-500-arrests-seizures-worth-over-USD-400-million>
<https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-financial-crime-operation-makes-record-5-500-arrests-seizures-worth-over-USD-400-million>

[78] <https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat>
<https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat>

[79] <https://www.mastercard.com/news/europe/en/newsroom/press-releases/en/2025/mastercard-introduces-first-ever-threat-intelligence-solution-to-combat-payment-fraud-at-scale/>
<https://www.mastercard.com/news/europe/en/newsroom/press-releases/en/2025/mastercard-introduces-first-ever-threat-intelligence-solution-to-combat-payment-fraud-at-scale/>

[80] <https://eur-lex.europa.eu/eli/dir/2023/2225/oj/eng>
<https://eur-lex.europa.eu/eli/dir/2023/2225/oj/eng>

[82] <https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.20661.html>
<https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.20661.html>

[83] <https://investor.visa.com/news/news-details/2024/Visa-Issues-10-Billionth-Token-Generating-40-Billion-in-Incremental-E-commerce-Globally/default.aspx>
<https://investor.visa.com/news/news-details/2024/Visa-Issues-10-Billionth-Token-Generating-40-Billion-in-Incremental-E-commerce-Globally/default.aspx>

[85] <https://corporate.visa.com/en/sites/visa-perspectives/security-trust/visa-announces-latest-vsd-milestone.html>
<https://corporate.visa.com/en/sites/visa-perspectives/security-trust/visa-announces-latest-vsd-milestone.html>