Ten seconds, no way back

What instant payments do to fraud, and who ends up with the bill

2026

At a glance

Since 9 October 2025 every euro credit transfer has to arrive within ten seconds, day and night, and afterwards it cannot be pulled back. Strong authentication has worked: the fraud it is designed for stays under control. The fraud that remains goes along the only route authentication cannot close off, namely the payer, and in 2024 users bore roughly 85% of the losses on fraudulent credit transfers in the European Economic Area. Europe answered with a warning screen you are allowed to ignore. The United Kingdom pulled a different lever and put the bill with the banks, after which the losses concerned fell by roughly 21%.

This report is about those two answers, about what the figures say about them, and about what changes when a loss becomes a liability instead of a cost.

85%

of the losses on fraudulent credit transfers in the EEA were borne in 2024 by the user, not by the bank. Joint report EBA and ECB, 15 December 2025

Foreword

Payment fraud is usually presented as an arms race between criminals and detection software. That picture is attractive and largely misleading. The most important variable in the European fraud question of the past two years is not technology. It is the question of who pays when it goes wrong.

For this report it looked at the primary sources: the regulation that made instant payments mandatory, the joint fraud figures of the European Banking Authority and the European Central Bank, the British regulator that was the first in the world to make reimbursement compulsory and had an independent evaluation carried out on it, and the compromise texts of the new European payments legislation.

What emerges is a natural experiment. Two jurisdictions with comparable infrastructure chose a different instrument for the same problem. One of the two has a measured result. The report describes what that result is, and why the two figures circulating about it can be true at the same time.

Venture Campus

01 The payment became instant

Regulation (EU) 2024/886 of 13 March 2024, the instant payments regulation, did something the market itself had not done in twenty years: it made the instant euro credit transfer mandatory instead of optional. From 9 January 2025 every payment service provider in the euro area had to be able to receive them. From 9 October 2025 it also had to be able to send them, at a price that may not be higher than that of an ordinary credit transfer. Outside the euro area 9 July 2027 applies.

Ten seconds, twenty-four hours a day, seven days a week. That sounds like an improvement of the user experience and it is in reality a rebuild of the foundation. Sanctions screening that used to run in an overnight batch now has to happen within those ten seconds, whereby the regulation replaces the screening of every transaction with periodic checking of the customer records against the sanctions lists. Liquidity management no longer has a closing time. Fraud detection gets no time to think.

And then the point that often stays undiscussed. Instant means irrevocable. With an ordinary credit transfer there was time between the instruction and the settlement, and into that time a phone call, a block, a recall sometimes fitted. That time is gone. The money is in the recipient's account before the victim has finished their second thought, and from there it is through a chain of mule accounts within a few minutes.

At the same time payment institutions and electronic money institutions gained direct access from October 2025 to the systems of the Eurosystem, among them TIPS for the settlement of instant payments. The field has therefore become faster and broader at once: more parties on the rails, less time to think, and no button to undo anything.

Source: Regulation (EU) 2024/886 of 13 March 2024 on instant credit transfers in euro · European Central Bank, access of non-bank payment service providers to TARGET services, from October 2025

02 What the figures say

On 15 December 2025 the European Banking Authority and the European Central Bank published the 2025 edition of their joint report on payment fraud, based on the data providers report half-yearly to their national supervisors. The total value of fraudulent payments in the European Economic Area came out at 4.2 billion euros in 2024, against 3.5 billion in 2023. A rise of 17%.

The breakdown is where it becomes interesting. Credit transfers accounted for 2.2 billion euros, 16% more than the year before. Card payments with cards issued in the EU or EEA accounted for 1.329 billion, 29% more. The supervisors establish that strong customer authentication remains effective against the fraud types it was devised for and that were dominant when PSD2 entered into force, certainly with cards. But new forms are coming up, and the report names the most important one: the manipulation of the payer.

> Strong authentication works against the fraud it is designed for. The fraud that remains goes through the customer.

Then the figure that gives this report its title. On credit transfers the payment service users bore roughly 85% of the total fraud losses in 2024. Not the bank, not the scheme, not the merchant. The person who was defrauded. The reason is legally simple: they authorised the payment themselves, and in the system of PSD2 an authorised payment is not an unlawful transaction but a mistake by the customer.

Note also what the figure does not say. As a share of traffic, fraud on credit transfers is negligible: in the earlier measurement it concerned 0.001% of the value and 0.003% of the number. The problem is not an epidemic in the statistics. The problem is that the amount grows, that it is high per case, and that it comes down almost entirely on the party least able to withstand it.

Source: European Banking Authority and European Central Bank, joint report on payment fraud, 2025 edition, published on 15 December 2025 · ECB and EBA, joint report on payment fraud, 1 August 2024, for the fraud rates per instrument · Directive (EU) 2015/2366 (PSD2), article 96(6)

03 The payer is not a leak but a route

What exactly happened when authentication began to squeeze card fraud is best documented in the United Kingdom. On 11 June 2026 UK Finance published its annual fraud figures for 2025: 1.28 billion pounds stolen, 4% more than the year before. Within that, unauthorised fraud, above all card fraud, fell by 5% to 703.4 million pounds, while the number of cases rose by 11% to 3.81 million. Many more victims, smaller amounts each, a lower total bill.

Authorised push payment fraud went the other way: 576.4 million pounds, 19% more, across 248,070 cases. Investment fraud was the largest item at 221.5 million pounds and rose by 40%. Romance fraud rose by 23% to 39.2 million. Impersonation fraud, where someone poses as the bank or the police and presses for a transfer to a safe account, fell by 12%. The two categories move in opposite directions, and that is no coincidence.

The origin is as clear as it is uncomfortable for the sector that gets the bill. Sixty-six per cent of the cases of push payment fraud started online, accounting for 32% of the losses. Seventeen per cent started via telecommunications, and those cases are more expensive: they represent 28% of the losses. The fraud arises on an advertisement, a marketplace, a messaging app or a telephone conversation. The payment is the last chapter, not the first.

That explains why detection alone does not suffice. A bank sees a transfer from a customer to an account in the name of a real person, authorised with a real fingerprint, on a real device, after a real conversation the bank never heard. There is technically nothing wrong with that transaction. Everything that is wrong about it happened outside the field of view of the payer and of the bank, and ends within ten seconds in an account where nothing can be done about it any more.

Source: UK Finance, Annual Fraud Report 2026, published on 11 June 2026, with figures for 2025 · European Banking Authority and European Central Bank, joint report on payment fraud, 15 December 2025

04 The European answer is a warning

The instant payments regulation contains the European answer to this fraud, and it is a check of the name. The Verification of Payee, VoP for short, compares the name of the beneficiary with the IBAN the payer has typed in. The provider of the beneficiary answers immediately, the provider of the payer passes the answer on, and the service is free. It has applied since 9 October 2025 to all providers in the euro area, banks as well as payment institutions and electronic money institutions, and not only to instant payments but to all SEPA credit transfers. The accompanying rulebook of the European Payments Council entered into force on 5 October 2025.

The outcome is returned in four flavours, and the way they are designed says everything about the chosen philosophy. See the table below. The core is in the last column: with every outcome the payment may go ahead. VoP blocks nothing. Business users may even refuse the service, with the possibility of opting back in later.

And there sits the legal sting. When the payer confirms a transfer after their provider has warned them that the unique identifier does not match, they bear the loss when the money ends up with the wrong party. The warning is therefore not only an aid for the customer. It is also a piece of evidence. The screen you show at the moment of confirming is from that instant the document with which it is later established who knew what.

For anyone working in the sector that is a design brief with a different gravity than usual. The wording of the warning, the distinction between close match and no match, the question of whether someone can get through the screen with one tap, whether or not the displayed text is logged: those are no longer questions of conversion rate. They are questions of liability, and they are decided within ten seconds.

Outcome	What it means	What happens
Match	Name and IBAN correspond	The payment goes ahead
Close match	Name differs slightly	The payer sees the registered name and decides
No match	Name and IBAN do not correspond	The payment can go ahead; the payer bears the risk
Other	Verification not possible	The payment can go ahead without confirmation

The four outcomes of the Verification of Payee since 9 October 2025

Source: Regulation (EU) 2024/886, provisions on the verification of the payee · European Payments Council, Verification of Payee Scheme Rulebook, in force on 5 October 2025 · European Central Bank, communication on the Verification of Payee Service, 2 August 2024

05 The British experiment

The United Kingdom chose a different lever. Since 7 October 2024 providers are obliged to reimburse victims of authorised push payment fraud, with a liability that is split equally between the sending and the receiving institution. That last part is the innovation that really matters. The receiving bank, which opened the mule account and checked the identity, until then had no financial motive at all to be good at it. From that date it pays half.

The figures on the first year have been published by the Payment Systems Regulator. Of the money victims claimed back, 88% came back, against 66% in the same period of the year before under the voluntary system. Eighty-four per cent of the claims are handled within five days, 97% within thirty-five days. Between October 2024 and June 2025 roughly 126,000 claims were submitted, roughly 15% fewer than in the comparable window before it.

> The largest improvement came from the institutions that had been in the worst shape before.

On 1 July 2026 the independent evaluation appeared, carried out by Frontier Economics on behalf of the regulator. The estimate: the losses within scope, sent via Faster Payments, fell by roughly 21% after the introduction of the reimbursement duty. In money roughly 73 million pounds a year, in cases almost 35,000 fewer. The reimbursement rate across all claims rose from 54% to 65%.

The detail that makes the causality most convincing is in the distribution. The largest improvements came from the institutions that had the worst fraud figures before the rule. Whoever had the most to lose changed the most. That is not the pattern of a technological breakthrough spreading evenly across the market. That is the pattern of an incentive landing where it hurts. The fraud was to an important extent a distribution problem disguised as a detection problem.

Source: Payment Systems Regulator, reimbursement requirement for authorised push payment fraud, in force on 7 October 2024 · Payment Systems Regulator, One year on: Impact of APP reimbursement on victims, October 2025, with the quarterly data from the reimbursement dashboard · Frontier Economics for the Payment Systems Regulator, independent evaluation published on 1 July 2026

06 What Europe now takes over

Europe has read the lesson. On 27 November 2025 the European Parliament and the Council reached a provisional political agreement on the third payment services directive and the new payment services regulation, together the proposal the Commission had tabled in June 2023. On 23 and 24 April 2026 the national representatives confirmed the compromise texts and they were published. Publication in the Official Journal is expected in the course of 2026, with an application period of roughly twenty-one months after that.

The content shifts the liability in three ways. Whoever becomes the victim of impersonation fraud gets reimbursed. A provider that fails to report a discrepancy between name and identifier becomes liable for it: the warning from the previous part gets, in other words, a sanction on not showing it. And scheme operators and technical service providers can be held liable for shortcomings in strong customer authentication, which means that the chain behind the payment comes into view as well.

The fourth provision is the most surprising and has received strikingly little attention in the trade press. An online platform that is informed of fraudulent content and does not remove it can become liable towards the provider that reimbursed the victim. For the first time a money flow then runs from the place where the fraud starts to the place where it is paid. Given the finding that two thirds of this fraud starts online, that is no detail but the logical keystone.

Alongside that a structural distortion disappears. The rules on market conduct move from a directive to a regulation, so without national transposition and without the room to shop between member states that had filled in PSD2 differently. Payment institutions and electronic money institutions merge into one category, whereby existing authorisations are transferred without a new application.

Source: European Parliament and Council of the EU, provisional political agreement on PSD3 and the payment services regulation, 27 November 2025 · Council of the EU, final compromise texts ST-8221-2026-INIT (regulation) and ST-8222-2026-INIT (directive), confirmed on 23 April 2026 · European Commission, proposals COM(2023) 366 and COM(2023) 367, 28 June 2023

07 What it changes

Fraud stops being a cost. It becomes a liability with a legal test, and that changes where it sits on the balance sheet, who reports on it and what a shortcoming is worth. A loss you write off. A liability you have to provide for, insure and account for. For a payment institution with a thin margin per transaction that is the difference between an operational nuisance and an existential item.

The receiving side becomes interesting for the first time. For twenty years the attention lay with the payer: authenticate them, score their behaviour, warn them. Shared liability puts the spotlight on the account the money goes to, and therefore on onboarding, identity checking and the pattern recognition of mule accounts. That is a different discipline from fraud detection on the sending side, with different data and different models, and most institutions never built it seriously because there was never a bill against it.

Everything moreover has to happen within ten seconds. A model that takes a decision in a hundred milliseconds on the basis of data it already has is something fundamentally different from a team that assesses a suspicious transaction before the overnight settlement. The time pressure is not a performance requirement, it is an architecture decision, and it determines which data you can still consult at the moment it matters.

And a gap remains. Reimbursement is national. The British system covers Faster Payments and CHAPS, so domestic traffic. The criminals who commit this fraud are not bound to the same scope as the rule that has to deter them. What a cross-border chain does with an incentive that stops at the national border is not a theoretical question. It is the next chapter.

Source: Frontier Economics for the Payment Systems Regulator, evaluation of 1 July 2026, on the shared liability between sending and receiving institution · Regulation (EU) 2024/886, on the ten-second settlement period and the sanctions screening

08 What does not add up yet

Start with the two figures that appear to contradict each other. Frontier Economics says that the reimbursement duty made the losses concerned fall by roughly 21%. UK Finance says that authorised push payment fraud rose by 19% in 2025 to 576.4 million pounds. Both are correct. The first is a counterfactual estimate on a delimited part of the traffic: how much higher would it have been without the rule. The second is a level across the whole market, including what falls outside the scope. A measure can work while the number rises, and whoever does not make that distinction reads every evaluation wrongly.

Then the user who does not know about the protection. The research of the British regulator shows that 71% of the victims surveyed did not know the protection existed, and that 49% submitted no claim at all. A right that half of the entitled do not exercise is not a right but an average. The measured reimbursement rate of 88% moreover concerns the money that was claimed back, not the money that was lost. Over 2025 as a whole the British banks reimbursed 354.3 million pounds, roughly 61% of the total authorised losses.

> A measure can work while the number rises. Whoever does not make that distinction reads every evaluation wrongly.

The fundamental objection comes from the sector itself, and it is the strongest argument against the lever that demonstrably works. Reimbursement moves money from the bank to the victim. It does not take the money away from the organised crime that already has it. The amount is therefore paid twice and stolen once, and the criminal proceeds stay unchanged. Prevention before the payment remains the only mechanism that makes the crime itself less rewarding, and the evaluation suggests precisely that the liability enforced that prevention, which makes the argument less clear-cut than both camps make it appear.

Finally three loose ends. The platform liability in the new regulation has never been tested, and how it relates to the removal obligations of the digital services regulation has not been written out. The VoP verification warns and then lets you go ahead, which means that its effect depends entirely on behaviour that nobody has measured on a European scale. And there is as yet no European fraud figure covering a period after 9 October 2025. The figures this report rests on are about 2024. The real answer to the question of whether the name check works is in a report that has not been written yet.

Source: Frontier Economics for the Payment Systems Regulator, 1 July 2026 · UK Finance, Annual Fraud Report 2026, 11 June 2026 · Payment Systems Regulator, APP fraud research and reimbursement dashboard, October 2025

About Venture Campus

Venture Campus is a Belgian consultancy for innovation funding. The firm prepares applications, writes them and submits them together with the client to the Flemish, federal and European instruments.

The assessment criteria are sector-neutral. All sectors, products and services qualify. The client brings the technology, the domain and the plan. Venture Campus brings the scheme, its criteria and the evaluator's perspective, applied before submission.

For the kind of work this report describes, real-time detection, shared identity checking between institutions, and decisions within ten seconds, the O&O instrument of VLAIO is usually the appropriate channel: 25 to 45% of the accepted costs for development projects, 25 to 60% for research projects, with a maximum of 3 million euros. VLAIO funds knowledge building and technical risk, not products. The percentages apply on the date on the cover.

On most assignments no cure, no pay applies: you pay when the support has been granted. That does not hold for Strategische Transformatiesteun and it does not describe the fiscal trajectories. The analysis beforehand is free, as is the subsidiescan with six questions. If there is no realistic case, the firm says so.

Venture Campus BV | Schaarbeekstraat 20E bus 11 | 9120 Beveren, Belgium | +32 333 11 333 | venturecampus.com

SOURCES

Regulation (EU) 2024/886 of 13 March 2024 on instant credit transfers in euro · Directive (EU) 2015/2366 (PSD2), article 96(6), and the EBA guidelines on fraud reporting EBA/GL/2018/05 · European Banking Authority and European Central Bank, joint report on payment fraud, 2025 edition, 15 December 2025 · European Central Bank and European Banking Authority, joint report on payment fraud, 1 August 2024 · European Central Bank, communication on the Verification of Payee Service, 2 August 2024 · European Payments Council, Verification of Payee Scheme Rulebook, in force on 5 October 2025 · UK Finance, Annual Fraud Report 2026, 11 June 2026 · Payment Systems Regulator, One year on: Impact of APP reimbursement on victims, October 2025 · Frontier Economics for the Payment Systems Regulator, independent evaluation of the reimbursement duty, 1 July 2026 · European Parliament and Council of the EU, provisional political agreement on PSD3 and the payment services regulation, 27 November 2025 · Council of the EU, compromise texts ST-8221-2026-INIT and ST-8222-2026-INIT, 23 April 2026 · European Commission, proposals COM(2023) 366 and COM(2023) 367, 28 June 2023