NOCTULA RISK INTELLIGENCE

RESEARCH & INTELLIGENCE WEEKLY REPORT

# Verifying the Payee
# Does the Name Match the Account?

*Verification of Payee, Confirmation of Payee and the limits of name checks against mule accounts*

**Doğancan İpek**

November 2026

**KEY TAKEAWAYS**

- **The mandate is in force.** Since 9 October 2025, euro-area payment service providers (PSPs) must offer payers a free check of the payee name against the IBAN before a SEPA credit transfer is sent (Regulation (EU) 2024/886). Non-euro Member States follow on 9 July 2027.
- **It is close to, but not the same as, the UK model.** Both return match, close match or no match. They differ in legal basis, in who operates the scheme, and in how liability is allocated when a check is skipped or fails.
- **Published outcome data are thin.** We found scheme-participation figures from the European Payments Council and match rates from one vendor, but no published estimate of the effect on fraud losses in either the EU or the UK.
- **A name check does not detect a mule account.** A mule usually holds an account in the mule's own, correct name. The check addresses misdirected payments and payee impersonation, a narrower problem than the push-payment fraud described in Week 2.
- **Name checks and reported-account lists answer different questions.** Several jurisdictions outside Europe publish or allow public queries of reported accounts; European law makes that difficult. The gap is a policy choice with costs on both sides.

## SUMMARY

This report is a narrative review. It describes the EU Verification of Payee (VoP) requirement, compares it with the UK Confirmation of Payee (CoP) service, collects the first available data on its operation, and sets out what a payee-name check can and cannot detect. It then contrasts the European position on public listing of reported accounts with practice in several Asian jurisdictions. It reports no original data.

*Keywords: Verification of Payee; Confirmation of Payee; Instant Payments Regulation; IBAN; authorised push payment fraud; money mules; reported-account databases.*

## DISCLOSURE

Noctula Risk develops AI-powered financial crime prevention technology. This report was written independently of product considerations. Figures that originate with vendors are identified as such in the text and in the exhibits.

## 1. INTRODUCTION

Week 2 followed the proceeds of authorised push payment (APP) fraud to the accounts that receive them. Its main finding was that the receiving account is usually a real account held in a real name, and that the cost of such fraud is gradually being moved onto the institutions that hold it. A natural next question is what a sending institution can check before it releases a payment at all.

The most visible answer in European payments is the payee-name check. A payer enters a name and an IBAN; before the payment is authorised, the payee's PSP compares the two and the payer's PSP reports the result. The UK has run a version of this since 2020 as Confirmation of Payee. The euro area has had a legal obligation to offer it since October 2025. This report asks what the two regimes have in common, what early evidence exists on their operation, and where the check stops being informative.

## 2. SCOPE, METHOD AND LIMITATIONS OF THE EVIDENCE

Sources were chosen for relevance to payee verification and to public listing of reported accounts: the Official Journal text of Regulation (EU) 2024/886, publications of the European Payments Council (EPC) and the UK Payment Systems Regulator (PSR), trade and vendor commentary on early EU operation, and the public pages of the services discussed in Section 7. Online sources were retrieved in November 2026.

Four limits apply. First, outcome data are sparse. The EPC figures describe scheme participation, not fraud outcomes, and the match rates available come from a single vendor. Second, we found no study that estimates the effect of VoP or CoP on APP fraud losses; any such effect is confounded in the UK by the reimbursement rules that took effect in October 2024. Third, the review of non-European services relies on the services' own descriptions and on press coverage, not on an independent test of their accuracy. Fourth, the legal points in Section 7 are the author's reading and not legal advice; national law was not reviewed.

## 3. THE EU REGIME

Regulation (EU) 2024/886 amended the SEPA Regulation (260/2012) and other instruments to require instant credit transfers in euro and to add safeguards. The payee-name check is in Article 5c. The payee's PSP verifies the name against the IBAN and returns one of three outcomes (match, near match, no match); the payer's PSP notifies the payer of the result and, under Article 5c(7), of the consequences of proceeding despite a mismatch. The service must be free of charge (Article 5b(2)) and applies to SEPA credit transfers generally. Euro-area PSPs were required to comply by 9 October 2025 and PSPs in non-euro Member States by 9 July 2027 (Article 5c(9)).

Three design features matter for what follows. The recitals allow, for legal persons, identifiers other than the name, such as a fiscal number, the European Unique Identifier or an LEI, and acknowledge that habitual and formal names differ (recitals 20 to 22). Large payers that send bulk files may opt out of or into the check by agreement (recital 24). And the technical scheme is not set in the Regulation: it is delegated to the EPC scheme (recital 23), whose rulebook took effect on 5 October 2025 after the Directory Service went live on 2 September 2025.

Liability is addressed in Article 5c(8). A PSP that complied with the obligation is not liable for a payment that went to the wrong account because of an incorrect unique identifier. If the payer's PSP did not comply, it must refund the payer without delay. If the payee's PSP failed to perform the check correctly, it compensates the payer's PSP. Any further loss is left to contract and national law. The provision allocates liability for a failed check; it does not make anyone liable for a fraud that the check did not catch.

## 4. COMPARISON WITH THE UK

Confirmation of Payee began under PSR Specific Direction 10 in 2019, which applied to the six largest banking groups and brought about 90 per cent of Faster Payments and CHAPS volume into scope by March 2020. Specific Direction 17 extended the requirement to about 400 further firms in two stages (31 October 2023 and 31 October 2024). The PSR reports coverage above 99 per cent of Faster Payments and CHAPS volume, more than 320 participating organisations and over two million checks a day (PSR, 2025a, 2025b). Pay.UK operates the service; the PSR regulates it. Exhibit 1 sets the two regimes side by side.

**Exhibit 1. EU Verification of Payee and UK Confirmation of Payee**

| Dimension | EU VoP | UK CoP | Source |
|---|---|---|---|
| Legal basis | Regulation (EU) 2024/886, Art. 5c, applying directly in each Member State | PSR Specific Directions 10 and 17 (regulatory directions to named PSPs) | Regulation; PSR |
| Operator | EPC scheme and rulebook; Directory Service and routing and verification mechanisms (RVMs) | Pay.UK service; PSR supervises compliance | EPC; PSR |
| Outcomes | Match, near match, no match; the scheme adds a "not able to perform" outcome for technical failure | Match, close match, no match | Regulation; EPC; PSR |
| Rails covered | SEPA credit transfers, instant and standard | Faster Payments and CHAPS | Regulation; PSR |
| Non-name identifiers | Fiscal number, EUID or LEI may be used for legal persons (recitals 20 to 22) | Account-type selection (personal or business) and name | Regulation; PSR |
| Cost to payer | Free of charge (Art. 5b(2)) | No payer charge found in the PSR materials reviewed | Regulation; PSR |

| Dimension | EU VoP | UK CoP | Source |
|---|---|---|---|
| Liability for a failed check | Art. 5c(8): refund by a non-compliant payer PSP; compensation by a non-compliant payee PSP | CoP sets no liability rule; APP reimbursement is a separate regime (from 7 Oct 2024) | Regulation; PSR |
| Compliance date | Euro area 9 Oct 2025; non-euro 9 Jul 2027 | 2020 (first group); remaining firms by 31 Oct 2024 | Regulation; PSR |

*Full references at the end of the report.*

Two differences deserve emphasis. The EU obligation sits in primary legislation and is uniform across Member States, whereas the UK obligation derives from regulatory directions and a scheme operator. And the EU provision ties the check to a liability rule (Article 5c(8)), which the UK service does not. In the UK, the incentive to participate came from the direction, and the incentive to prevent loss from the later reimbursement regime. Whether either design yields better fraud outcomes is not shown by the evidence reviewed here.

## 5. FIRST DATA FROM THE EU

Operational data on the EU service are limited and mostly describe participation. In November 2025 the EPC reported that 2,785 PSPs had joined the scheme, of which 2,719 were reachable, supported by 58 routing and verification mechanisms across 23 countries, and that its support desk had handled about 1,400 tickets since launch. The EPC expected more than 3,000 PSPs by mid-2027 (EPC, 2025). Vendor commentary puts the number of PSPs offering SEPA credit transfers at about 3,700 (nocash.ro, 2026), which would imply that coverage, not accuracy, is the first constraint on usefulness; we could not confirm that denominator independently.

The only match-rate data found come from SurePay, a vendor that supplies the service to banks. As reported in trade press, match rates were around 44 per cent in basic deployments and above 80 per cent in mature markets (nocash.ro, 2026). The same vendor's technical review identifies recurring causes of non-matches: diacritics, name-field limits of 40 or 70 characters at some institutions against 140 in the scheme, vague "not able to perform" responses, and the absence of a standard for bulk checks (MonitorPay, 2025). These are data-quality and implementation problems. They suggest that a no-match in the first year often reflects formatting rather than fraud, which bears on how payers read the warning (Section 6).

**Exhibit 2. Early operational figures, EU VoP and UK CoP**

| Measure | Figure | Period / geography | Source | Caveat |
|---|---|---|---|---|
| PSPs joined scheme | 2,785 (2,719 reachable) | Nov 2025, SEPA | EPC (2025) | Participation, not use or outcome |
| Routing and verification mechanisms | 58 RVMs; 23 countries | Nov 2025 | EPC (2025) | Infrastructure count |
| Support tickets | About 1,400 | Launch to Nov 2025 | EPC (2025) | Indicates implementation load |
| Match rate | About 44% (basic) to above 80% (mature) | 2026, markets served by one vendor | nocash.ro (2026) | Vendor-reported; not independently verified; "basic" not defined |
| UK CoP checks | Over 2 million a day; over 320 organisations | 2025, UK | PSR (2025a) | Volume, not fraud outcome |
| Effect on fraud losses | Not found | EU and UK | None | Evidence gap; confounded by UK reimbursement from Oct 2024 |

*Figures use different bases and are not directly comparable.*

## 6. WHAT A NAME CHECK CAN AND CANNOT DETECT

A payee-name check detects a discrepancy between the name the payer holds and the name registered to the account. It therefore addresses two situations: a mistyped or substituted IBAN, and an impersonation in which a fraudster supplies an account in a different name from the trusted party the payer believes they are paying, as in invoice redirection or a spoofed supplier. For these, the check is a direct control.

It does not address the cases that dominate the Week 2 evidence. We identify five limits.

- **Mule accounts carry correct names.** A money mule opens or lends an account in a real person's own name. A transfer to that account returns a match because the name is correct. A match can therefore raise a payer's confidence in a payment that is fraudulent.
- **The payer is the one who authorises.** In APP fraud the payer has been persuaded that the destination is legitimate. A no-match warning may be overridden by a victim who is being coached, and a match may reassure a victim who should be cautious. The effect on behaviour is an empirical question we could not answer from the sources found.
- **Compromised genuine accounts pass the check.** If the account of a legitimate business is taken over, the name still matches. Detection depends on behavioural signals on the receiving side, not on the name.
- **The scope is SEPA.** The check does not cover payments outside SEPA or crypto-asset off-ramps. Week 2 reported that international APP scams in the UK rose from £21m in 2023 to £60m in 2025 while in-scope domestic losses fell, which is consistent with displacement but is not evidence of it.
- **Implementation affects signal quality.** If a large share of no-matches arise from diacritics or field-length limits (Section 5), payers learn to ignore them, and the warning loses value when a genuine impersonation occurs.

The conclusion is not that name verification is of little use. It is a control against one fraud type, and its limits are the reason receiving-side controls remain necessary. That was the position of Week 2: the receiving account is where laundering can be interrupted.

## 7. PUBLIC LISTING OF REPORTED ACCOUNTS: EUROPE AND ELSEWHERE

A payee-name check asks whether the account belongs to the person named. A reported-account list asks a different question: whether the account has already been reported as used in fraud. For mule accounts, which pass the first test, the second is the more relevant signal. Practice differs sharply between regions.

In Europe, we found no public database that lists reported IBANs by number. The reasons are partly legal and partly practical. An IBAN linked to an individual is personal data; publishing it with an allegation of fraud engages the rules on criminal-offence data (GDPR Article 10) and exposes the publisher to defamation claims, since a report is an allegation and not a finding. The Dutch police offer a per-query check of counterparties and do not publish a downloadable list (Politie, n.d.). Public registers that do publish bank accounts, such as the Polish and Czech VAT registers, record the accounts of registered taxpayers and are not fraud lists. The French AMF and ACPR blacklist covers unauthorised investment websites and does not list IBANs. Sharing between institutions occurs, but within closed, contractually governed arrangements rather than in the open.

Several jurisdictions in South-East Asia operate differently. Exhibit 3 summarises the services we could verify from their own pages or press coverage. Services we could not confirm are omitted.

**Exhibit 3. Public or per-query checks of reported accounts**

| Jurisdiction | Service | Operator | What can be checked | Notes |
|---|---|---|---|---|
| Netherlands | Controleer handelspartij | Police (Politie) | Counterparty details, per query | No downloadable list |
| Malaysia | Semak Mule | Royal Malaysia Police (PDRM CCID) | Bank account, phone number or company, per query | Official, free; "No Record Found" is not a guarantee |
| Indonesia | CekRekening.id | Ministry of Communication and Digital Affairs (Komdigi) | Reporting, searching and whitelisting of bank and e-wallet accounts | Official; reports are verified before listing |
| Thailand | Blacklistseller.com | Community-run | Search by bank account, PromptPay ID, ID number or name | Community reports; no official verification found |
| Thailand | Police online check-and-report site | Police Investigation Bureau | Bank accounts and fake websites | Known from press coverage (Thairath, 2025); not independently tested |

*Retrieved November 2026. The accuracy and coverage of these services were not tested.*

Two points follow. First, the Asian services combine reporting with public or per-query checking, and in the Malaysian and Indonesian cases an official body operates the service, which addresses part of the accuracy and defamation concern by adding verification. Second, quality control differs widely. A community list such as Blacklistseller reflects the reports it receives; an official "no record" result reflects only what has been reported so far. Neither is evidence of an account's integrity.

For Europe the choice is not between publication and silence. A VoP result and a reported-account signal could be combined at the receiving PSP, with the second source held within a regulated information-sharing arrangement. The legal basis for such sharing was not reviewed here and would need examination before a design is proposed.

## 8. RECOMMENDATIONS

### For institutions

1. Treat the VoP outcome as one input to payment risk scoring, not as a decision. A match should not lower the risk score of a payment to a newly opened account or a first-time payee.
2. Record outcomes and overrides. A firm that logs match, near-match and no-match results alongside override rates and later fraud reports can test whether the check changes behaviour in its own customer base.
3. Check the quality of name data (diacritics, field lengths) so that no-match warnings reflect real discrepancies.
4. Write the Article 5c(7) notice so that it explains in plain terms what proceeding after a mismatch means, and test the wording with customers.
5. Pair VoP with receiving-side signals such as account age, rapid inflow and outflow, and counterparty concentration, which are more informative about mules than the name.

### For the sector

1. Publish outcome statistics for the EU service, including match, near-match and no-match shares and override rates, so that independent evaluation is possible.
2. Set a standard for bulk and corporate checks, since the bulk-payer carve-out (recital 24) leaves a large part of supplier-payment fraud outside the control.
3. Clarify the lawful basis for sharing reported-account signals between PSPs, and decide whether any public or per-query element is compatible with data-protection and defamation law.

## 9. CONCLUSION

The EU payee-name check is a meaningful addition to the control set. It makes a UK-style service a legal duty across the euro area and closes off a class of misdirection and impersonation cases. The evidence reviewed does not show that it reduces APP fraud, and the structure of that fraud suggests it will not do so alone. Mule accounts hold correct names, and the check was not designed to see them.

VoP verifies identity at the point of payment; receiving-side monitoring and reported-account signals address behaviour afterwards. Europe has the first by law and the second only in closed form. Whether it should move toward the openness seen in parts of Asia is a question of legal design rather than technology, and it deserves a deliberate answer.

## WHAT TO WATCH

- Publication of EU outcome data from the EPC or supervisors, in particular override rates and the share of no-matches caused by data quality.
- 9 July 2027, when the obligation extends to PSPs in non-euro Member States.
- The first disputes or supervisory actions under Article 5c(8), which will show how liability is applied.
- Any independent evaluation of CoP or VoP effects on fraud, which would fill the main evidence gap identified here.

## REFERENCES


Blacklistseller.com. (n.d.). *Blacklistseller* [Community report search]. https://www.blacklistseller.com/

CekRekening.id. (n.d.). *CekRekening.id* [Service website]. Ministry of Communication and Digital Affairs (Komdigi). https://cekrekening.id/

European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/886 as regards instant credit transfers in euro. *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R0886

European Payments Council. (2025, November 20). *EPC's Verification of Payee scheme: A European success story*. https://www.europeanpaymentscouncil.eu/news-insights/news/epcs-verification-payee-scheme-european-success-story

MonitorPay. (2025). *Why VoP won't stop supplier fraud: The hidden limits of EU payee verification*. https://monitorpay.ai/why-vop-wont-stop-supplier-fraud-the-hidden-limits-of-eu-payee-verification/

nocash.ro. (2026, May 28). *Verification of Payee: Key lessons learned from SurePay, Europe's leading VoP provider*. https://nocash.ro/verification-of-payee-key-lessons-learned-from-surepay-europes-leading-vop-provider/

Payment Systems Regulator. (2025a, November 18). *Fraud prevention is key during International Fraud Awareness Week*. https://www.psr.org.uk/news-and-updates/latest-news/news/fraud-prevention-is-key-during-international-fraud-awareness-week/

Payment Systems Regulator. (2025b). *Confirmation of Payee*. https://www.psr.org.uk/our-work/app-scams/confirmation-of-payee/

Politie. (n.d.). *Controleer handelspartij*. https://www.politie.nl/aangifte-of-melding-doen/controleer-handelspartij.html

Royal Malaysia Police. (n.d.). *Semak Mule* [CCID service portal]. https://semakmule.rmp.gov.my/

Thairath. (2025, December 12). Police Investigation Bureau online check-and-report site for bank accounts and fake websites. *Thairath English*. https://en.thairath.co.th/lifestyle/life/2901485

UK Finance. (2026). *Fraud report 2026*. https://www.ukfinance.org.uk/system/files/2026-06/UK%20Finance%20Fraud%20Report%202026.pdf

*Week 2 sources (FCA; Frontier Economics) are cited as in the Week 2 report.*