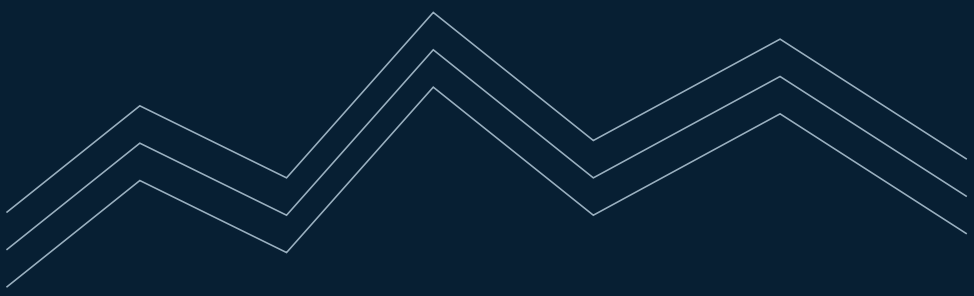
FINTECH AND FINANCIAL CRIME · RESEARCH ANALYSIS

Fintech, EMIs and the Changing Architecture of Money Laundering

Electronic money institutions now provide much of the speed, reach and account-like functionality once associated mainly with banks. Understanding the infrastructure behind a payment is increasingly central to financial-crime investigation.

CARRATU INTERNATIONAL / 23 AUGUST 2026



Fintech has made financial services faster, cheaper and more accessible. The same infrastructure can also be exploited to receive, fragment, convert and transfer criminal proceeds across accounts and jurisdictions.

Electronic Money Institutions - EMIs - are of particular interest because they increasingly provide transactional functionality once associated almost exclusively with banks. The customer experience can look familiar even where the underlying legal, safeguarding and operational structure is different.

What is an Electronic Money Institution?

Electronic money is monetary value stored electronically, issued after funds have been received and used to make payments. An authorised EMI can issue electronic money and may also provide payment services including transfers, cards, foreign exchange and non-bank current-account-style facilities. [3]

An EMI is not necessarily a bank. It does not ordinarily accept deposits and lend those deposits in the conventional banking model. Relevant customer funds are instead subject to safeguarding requirements. Safeguarding is intended to protect customer money if the firm fails; it is not a warranty that every customer, counterparty or transaction is free from financial-crime risk.

A single branded service may involve an authorised EMI, an agent or distributor, a programme manager, a virtual IBAN provider, safeguarding banks, foreign-exchange and payment processors, card schemes and outsourced onboarding technology. This layered structure can create legitimate efficiency, but it can also fragment visibility when responsibilities or data flows are weak.

From payment provider to transactional vehicle

An EMI does not have to be owned or controlled by criminals to be useful to them. It may simply form one link in a longer movement of value.

Receive

Fraud proceeds, money-mule payments or apparently commercial receipts enter an account or virtual account.

Fragment

Funds are split across customers, vIBANs, currencies, cards, wallets or counterparties.

Convert

Value is exchanged between currencies or bridged into merchants, prepaid instruments or cryptoasset services.

Transfer

Funds move rapidly through other providers and jurisdictions, increasing distance from the original offence.

In this setting the account becomes a transactional vehicle: infrastructure through which funds are received, reorganised and moved. Traditional placement, layering and integration stages may overlap because fraud proceeds can enter the financial system electronically and be transferred within hours.

Virtual IBANs and pooled-account structures

Virtual IBANs, or vIBANs, resemble conventional account identifiers but ordinarily route payments to an underlying master account. A provider can therefore give separate payment details to many customers while funds ultimately enter one or a limited number of physical accounts.

This is useful for legitimate reconciliation, but it changes the questions an investigator must ask. The visible payment details may not identify the master account, issuing institution, customer-facing intermediary, party responsible for onboarding or jurisdiction in which the records are maintained.

The National Risk Assessment states that multiple vIBANs may be linked to one payment account and that movements between virtual ledger positions can reduce visibility for underlying banking and custodial partners. It also identifies risks where the institution issuing the underlying IBAN has inadequate visibility of end users. [1]

A platform, a regulated EMI and 60,000 virtual accounts

The 2025 National Risk Assessment describes ongoing HMRC investigations involving an alternative banking platform incorporated in a higher-risk jurisdiction. The platform reportedly provided vIBANs to about 60,000 companies, mainly mini-umbrella companies, through a partnership with a UK-authorised EMI.

No customer due diligence was conducted when customers were onboarded. During the platform's final year of operation, about £2.5 billion was reportedly being laundered annually, with estimated revenue loss exceeding £500 million. The case was described as ongoing. [1]

The example does not show that vIBANs are inherently improper. It shows how a regulated institution can sit within a wider distribution arrangement containing an unregulated or poorly controlled intermediary, deficient onboarding and weak visibility over end users.

Agents, distributors and embedded finance

EMIs frequently scale through agents, distributors, programme managers and embedded-finance partnerships. A customer may believe they are dealing with a standalone financial platform when the regulated service is being provided under another firm's permissions.

Risk increases when the EMI relies excessively on another party's customer checks, transaction data is incomplete or delayed, onboarding standards vary, agents operate outside the original risk appetite, or commercial growth outpaces governance and supervision.

The FCA's 2026 payments priorities require effective governance, systems, controls and appropriately skilled staff to protect financial-system integrity. Its current Approach Document addresses the appointment and oversight of agents and distributors, safeguarding and financial-crime obligations. [2] [3]

Remote onboarding and identity manipulation

Digital onboarding removes geographic friction, but it changes the evidence needed to understand who is behind an account. A technically successful identity-document or facial check does not establish that the business proposition is genuine or that the visible customer is the ultimate controller.

Criminal exploitation may involve stolen or synthetic identities, impersonated directors, companies formed principally to obtain payment facilities, nominees, fabricated websites and invoices, or accounts opened by money mules for an undisclosed controller.

Effective due diligence must therefore consider both identity and commercial coherence: who controls the relationship, what activity should reasonably be expected, and whether the subsequent transactions fit that explanation.

Money mules, velocity and cross-border movement

Money-mule accounts receive and move criminal proceeds, distancing controllers from victims and predicate offences. Some participants are knowing; others are recruited through false employment, investment or relationship propositions. The National Crime Agency describes mule networks as groups of people or accounts used to launder funds while controllers maintain anonymity. [6]

Speed is not itself proof of laundering. Suspicion is more likely to arise from the combination of velocity, customer profile, counterparties, location, devices and the absence of an intelligible economic purpose.

International transfers and currency conversion add further layers. One institution may see the customer, another the settlement account, another the merchant and another the final wallet. Europol has highlighted the way digital payment structures and virtual accounts can make suspicious transactions harder to interpret and trace. [5]

EMIs as cryptoasset on-ramps and off-ramps

EMIs can provide the fiat-money infrastructure connecting ordinary payments with cryptoasset platforms. They may process deposits into exchanges, receive withdrawals, issue cards connected to digital-asset services or provide accounts to crypto-related businesses.

Most of this activity is legitimate. The risk increases when the payment provider, cryptoasset service, customer and ultimate beneficiary sit in different jurisdictions or operate under materially different standards. The National Risk Assessment identifies high risk where UK-incorporated EMI and payment firms provide fiat on-ramps and off-ramps for overseas cryptoasset providers, including those in higher-risk jurisdictions. [1]

Transactional indicators requiring closer examination

Indicator	Question raised
New account, immediate high volume	Does the activity fit the customer's history, staffing, capital and stated purpose?
Many unrelated payers followed by rapid onward transfers	Is the account acting as a pass-through or collection point without an adequate economic explanation?
Repeated currency conversion or cross-border routing	Are the currencies and jurisdictions connected to the trade, supplier or goods?
Shared directors, addresses, devices, domains or beneficiaries	Do apparently separate customers form a centrally controlled network?
Multiple vIBANs feeding a common master account	Who knows the end users, and which institution performed and monitors the due diligence?
Payments cycling through EMIs, wallets, exchanges or prepaid instruments	What commercial purpose explains each movement and conversion?
Activity continuing after the business appears dormant or dissolved	Who is operating the account, and for whose benefit?

No individual indicator proves criminal conduct. The strongest findings usually emerge from combinations and from network analysis rather than an account viewed in isolation.

Why attribution is difficult in layered payment architecture

A payment reference can identify the interface through which money moved without identifying the party that ultimately controlled the customer relationship. A customer-facing brand may sit in front of an authorised EMI, an agent or distributor, a programme manager, a safeguarding bank and a separate settlement chain. Virtual IBANs and pooled accounts can add another layer between the identifier visible to the payer and the underlying account structure.

This creates a recurrent interpretive problem in disputes and financial-crime reviews: the institution named on a statement may have performed only one function in a longer chain. Regulatory responsibility, contractual responsibility, possession of customer data and practical visibility over a transaction may sit with different participants.

The distinction becomes more important where payment infrastructure is embedded into another platform. A merchant, marketplace or fintech product can present a seamless front end while relying on multiple regulated and unregulated service providers behind it. The legal and operational boundaries are therefore part of the factual context; regulated status should not be treated as evidence that every participant in the chain performed the same role or saw the same information.

For expert readers, the point is less that fintech is uniquely opaque than that modern payment architecture distributes functions that traditional banking often concentrated within one institution. That distribution can improve competition and specialisation while making attribution, disclosure and recovery more dependent on understanding which entity performed which role.

Technology is both vulnerability and control

Fintech is also part of the response. Properly implemented systems can identify linked accounts, compare activity against expected behaviour, detect unusual velocity, screen sanctions and adverse information, analyse devices and reveal networks that would be difficult to identify manually.

The weakness arises when automation is treated as a substitute for judgement. A system may confirm that a document passed a technical test without establishing that the business exists, that its controller is genuine or that the transactions make commercial sense.

The European Banking Authority has identified weaknesses in the way money-laundering and terrorist-financing risks are assessed and managed in parts of the EU payment sector, including governance, internal controls and oversight of agents. [4]

Implications for decision-makers

• Separate the customer-facing brand from the authorised institution, intermediary and underlying account structure.

• Treat vIBANs, pooled accounts and embedded-finance arrangements as architectures to be resolved, not as proof of wrongdoing.

• Assess transactions against the customer's expected business, ownership, devices, counterparties and geography.

• Follow the funds beyond the first EMI and record what each participant in the chain can actually see.

Real-world context: regulated status does not eliminate financial-crime risk

The FCA reported in 2025/26 that it imposed requirements on BeAccount Ltd, an authorised electronic money institution, after concluding that the firm could not demonstrate adequate systems to identify, manage and monitor financial-crime risk or compliance with customer due-diligence requirements. The example is useful because authorisation establishes a regulatory status; it does not remove the need to understand how a particular institution operates and is controlled.

Public source: Financial Conduct Authority, Enforcement data 2025/26.

Sources and reading

Sources were accessed and checked for this edition on 23 August 2026. Reported allegations and ongoing proceedings are identified as such in the text.

1. 1**HM Treasury and Home Office.** National Risk Assessment of Money Laundering and Terrorist Financing 2025. 17 July 2025.
2. 2**Financial Conduct Authority.** Regulatory Priorities: Payments. March 2026.
3. 3**Financial Conduct Authority.** Payment Services and Electronic Money - Our Approach, version 8. May 2026.
4. 4**European Banking Authority.** Report on ML/TF Risks Associated with EU Payment Institutions. 16 June 2023.
5. 5**Europol.** The Other Side of the Coin: An Analysis of Financial and Economic Crime. 27 September 2023; page updated 25 November 2025.

6. 6**National Crime Agency.** Money Mules - Do not be used. current guidance accessed 24 July 2026.

Scope note

This article provides general information and analysis. It is not legal, regulatory, financial, compliance or other professional advice. Transaction indicators are not proof of wrongdoing, and public or reported information may be incomplete, delayed, disputed or capable of an innocent explanation.

Carratu International

About the author

Carratu International provides investigation, intelligence and due diligence support to organisations, professional advisers and private clients. Each instruction is scoped around the decision, the evidence available and the need for proportionate, clearly qualified reporting.