FINTECH AND FINANCIAL CRIME / RESEARCH ANALYSIS

Fintech, EMIs and the Changing Architecture of Money Laundering

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

RESEARCH & ANALYSIS / JULY 2026

BY VCI / 17 JULY 2026 / 16 MINUTE READ

Verify Carratu International Ltd / Company No. 17327582

carratu.co.uk / ICO Registration: ZC202007

Fintech, EMIs and the Changing Architecture of Money Laundering

£2.06tn	£1.1tn	High	c.60,000
combined annual payment value reported by regulated EMIs and payment firms in 2023 [1]	annual payment value reported by regulated EMIs alone in 2023 [1]	UK money-laundering risk rating for the regulated EMI and payment sector [1]	companies provided with vIBANs in the HMRC case study described in the NRA [1]

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 the transactional functionality once associated almost exclusively with banks. They can issue electronic money and may provide transfers, cards, foreign exchange and non-bank current-account-style facilities. The customer experience can look familiar even where the underlying legal, safeguarding and operational structure is very different. [3]

The risk is not that fintech is inherently criminal. It is that speed, remote access, cross-border reach and layered delivery arrangements can allow criminal activity to hide among very large volumes of legitimate commerce.

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 EMI is not necessarily a bank and does not ordinarily accept deposits and lend them 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 each customer, counterparty or transaction is free from financial-crime risk. [3]

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. These layers can create legitimate efficiency. They can also fragment practical visibility when responsibilities, data flows or controls 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. In this setting the account becomes a transactional vehicle: infrastructure through which funds are received, reorganised, converted and moved.

Receive Fraud proceeds, mule payments or apparently commercial receipts	Fragment Split funds across customers, vIBANs, currencies or counterparties	Convert Exchange currencies or bridge into cards, wallets and crypto services	Transfer Move rapidly through other providers, jurisdictions or merchant accounts	Obscure Increase distance between the original offence and final controller

Traditional descriptions divide money laundering into placement, layering and integration. Digital payment activity often compresses those stages. Proceeds of fraud may enter the financial system electronically and be divided, converted and transferred within hours without criminals handling physical cash.

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 small number of physical accounts.

This can simplify reconciliation for legitimate businesses. It can also make an investigation more difficult. The payment details visible on an invoice or statement may not reveal the master account, the issuing institution, the customer-facing intermediary, the jurisdiction in which records are maintained or the party that performed the customer due diligence.

The 2025 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 UK case study

> HMRC investigations described in the National Risk Assessment concerned 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 UK-authorised EMI. No customer due diligence was conducted at onboarding. During its final year, 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 intrinsically improper. It shows how a regulated institution can sit within a wider chain containing an unregulated or poorly controlled distributor, 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.

- The EMI relies excessively on another party's identity and customer checks.
- The contractual allocation of responsibilities is clearer than the operational reality.
- Monitoring data is incomplete, delayed or split between different technology systems.
- Agents operate from jurisdictions or customer segments outside the EMI's original risk appetite.
- Commercial growth outpaces governance, staffing and the ability to supervise the distribution chain.

The FCA's current payments priorities require firms to protect financial-system integrity through effective governance, systems, controls and appropriately skilled staff. Its Approach Document also addresses 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 also changes the evidence needed to understand who is behind an account. A technically successful document or facial check does not establish that the commercial proposition is genuine or that the person operating the account is the ultimate controller.

- stolen, altered or synthetically assembled identities;
- impersonated directors and beneficial owners;
- companies incorporated principally to obtain payment facilities;
- nominees, false websites, invoices and trading histories;
- accounts opened by money mules for an undisclosed controller.

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 organised to launder funds while controllers maintain anonymity. [6]

Speed is not itself evidence of laundering. Digital businesses can legitimately process high volumes. Suspicion is more likely to arise from the combination of velocity, customer profile, counterparties, location, device data and the absence of an intelligible economic purpose.

International transfers and currency conversion can add layers between the source and destination of funds. One institution may see the customer, another the settlement account, another the merchant and another the final wallet. Europol has highlighted the way modern digital payment structures and virtual accounts can complicate the interpretation and tracing of transactions. [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 control standards. The UK National Risk Assessment identifies a 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

Account behaviour A newly opened account immediately receives substantial funds; turnover is high while the balance remains low.	Payment pattern Many unrelated incoming payments are followed by rapid onward transfers or repeated currency conversion.
Customer coherence Volumes, counterparties or geographies do not fit the stated trade, staffing or financial record.	Shared infrastructure Several customers share directors, addresses, telephone numbers, devices, IP data, domains or beneficiaries.
vIBAN structure Multiple virtual accounts feed a common master account or beneficiary without a clear commercial explanation.	Cross-border exposure Funds repeatedly pass through jurisdictions unrelated to the customer, supplier, goods or documented purpose.
Digital-asset bridge Payments cycle between EMIs, wallets, exchanges or prepaid instruments with limited economic rationale.	Lifecycle anomaly Material activity continues after the business appears dormant, dissolved or no longer operational.

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

Investigating an EMI-linked payment

An effective enquiry separates the customer-facing brand from the regulated, banking and technical relationships underneath it. The following sequence is designed to clarify the payment architecture before conclusions are drawn.

	Identify the regulated entity Verify the EMI or payment institution actually providing the regulated service, its permissions and any restrictions.
	Resolve the distribution chain Establish whether an agent, distributor, programme manager or embedded-finance platform introduced or serviced the customer.
	Define the account structure Determine whether the payment details relate to a conventional account, vIBAN, pooled account or another payment reference.
	Identify the underlying banks Establish which institutions safeguard or settle the funds and what visibility each participant is likely to possess.
	Map ownership and control Examine directors, beneficial owners, connected entities, nominees and the people who actually operated the account.
	Test the economic rationale Compare volumes, currencies, counterparties and jurisdictions with the customer's stated trade and commercial footprint.
	Follow the payment path Trace beyond the first provider into other EMIs, banks, merchants, wallets, cryptoasset services and corporate entities.

Where litigation, fraud recovery or regulatory reporting may follow, payment records, statements, invoices, corporate records and electronic evidence should be preserved promptly. Care is also required not to prejudice an investigation or breach restrictions associated with suspicious-activity reporting.

Technology is both vulnerability and control

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

The weakness arises when automated compliance 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 its transactions make commercial sense. The EBA has identified weaknesses in the way money-laundering and terrorist-financing risks are assessed and managed in parts of the EU payments sector, including governance and oversight of agents. [4]

The investigative conclusion

Electronic Money Institutions are now part of the mainstream financial system. Their speed, accessibility and international functionality provide significant benefits. Those same features also make them relevant transactional vehicles within some fraud and laundering structures.

A regulatory authorisation should therefore be treated as the beginning of an enquiry, not its conclusion. Understanding an EMI-linked transaction requires examination of the institution, customer, distribution chain, virtual-account architecture, underlying banks, counterparties and ultimate destination of the funds.

In an increasingly fragmented financial system, following the money means understanding the infrastructure through which it travels.

Sources and reading

Sources were accessed and checked for this edition on 24 July 2026. The HMRC vIBAN example is described by the National Risk Assessment as an ongoing case and is presented here on that basis.

1. HM Treasury and Home Office. National Risk Assessment of Money Laundering and Terrorist Financing 2025. 17 July 2025.

2. Financial Conduct Authority. Regulatory Priorities: Payments. March 2026.

3. Financial Conduct Authority. Payment Services and Electronic Money - Our Approach, version 8. May 2026.

4. European Banking Authority. Report on ML/TF Risks Associated with EU Payment Institutions. 16 June 2023.

5. Europol. The Other Side of the Coin: An Analysis of Financial and Economic Crime. 27 September 2023; page updated 25 November 2025.

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

Scope note

This publication 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.

About VCI

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

carratu.co.uk · info@carratu.co.uk