SAFWAN ALMODHAYAN



OPINION AND ANALYSIS

Editorial date: November 2, 2026

The Transfer That Ended in the System and Continued in Court

When the Instructions Are Valid but the Will Is Deceived

On March 19, 2018, **Fiona Philipp** returned to a Barclays branch in Britain to transfer **£250,000** to a United Arab Emirates account. The bank did not execute this third transfer because her account had been suspended for review. Days earlier, on March 10 and 13, she and her husband had attended the bank and instructed two international transfers totaling **£700,000** to UAE accounts. No one stole her password and pressed a button in her name. She issued the instructions. What her signature did not reveal was the story that produced them: a fraudster impersonating an official working with the UK Financial Conduct Authority and National Crime Agency persuaded the couple to send most of their life savings. When the deception emerged, the money and its owners stood on opposite sides of certainty.1

On **July 12, 2023**, the UK Supreme Court held that, under the rule litigated there, the bank was not generally required to refuse a clear payment instruction personally issued by a customer merely because its purpose gave reason for suspicion. This did not give the fraudster a right to the money, declare the transfer fair, or say the bank could not stop the third payment. The Court distinguished a bank's **power to decline an instruction in specified circumstances** from a **general legal duty to do so**. It left another issue open for trial: after Philipp discovered the fraud and notified the bank on March 27, did the bank fail to take reasonable steps to recover the money? The Supreme Court did not find that claim proved; it declined to dispose of it summarily before examination.1

One detail says more than many claims about secure applications. Police had supplied the bank with concerning information on March 16; on March 19, Philipp still sought a third transfer. She and her husband did not understand the fraud until late in the month. Recall attempts sent at the end of May failed. These 2018 events concerned conventional international transfers, and **the British reimbursement rules beginning in 2024 cannot be applied retroactively**. Their relevance to instant payment is not the number of seconds involved. It is the exposed question: what happens when a payment order is procedurally authentic but the will producing it has been systematically deceived?1

Settlement Finality Is Not the End of the Dispute

We treat “complete” as an ending. A green mark appears after a transfer, reassuring the sender that the institution performed the instruction. That may be right in accounting terms while the contractual problem is only beginning. A payment system does not determine the truth of every relationship between payer and payee: whether someone promised an apartment they do not own, offered a fictional investment, impersonated an official, or sold goods that exist. A standard payment message has no field capable of deciding every such question, and real-time infrastructure does not become a judge disguised as a server.

“Final” must therefore be unpacked. **Principle 8 of the CPMI–IOSCO Principles for Financial Market Infrastructures**, issued in 2012, requires a clearing and settlement system to define the point at which obligations become final and the point after which a participant cannot revoke an unsettled order. The purpose is not moral absolution for merchants. Participants need to know which inter-institutional obligations are discharged so later action rests on a financial state that is not indefinitely pending. **Settlement finality among participants** is not **immunity from a civil claim**, or the loss of a victim's right to pursue value through another legal route.2

This engineering point requires rigor. If every goods dispute or doubt about a buyer's story could erase settled payments on which later transactions relied, participants would not know what could be treated as complete. Finality does not prevent another transaction from returning value. That later event might be a voluntary refund, compensation paid by a responsible institution, enforcement of a judgment against a recipient, or a recovery process under network rules. Each is a **new financial event** with its own basis, scope, and authority—not magical deletion of the first transfer.

Everyday language can blur the distinction; product design cannot. A **refund** may mean the merchant voluntarily returns the price. A card **chargeback** is a procedure under network rules among issuer, acquirer, and merchant. **Recovery** from a fraudulent account may depend on finding funds still within a cooperating institution's control. **Mandatory reimbursement** may require an institution to pay a victim from its resources even if the fraudster's proceeds are

not fully recovered. Visa itself says chargeback is not a general legal right with a guaranteed outcome, but a network procedure; other claims, including some UK credit-card obligations, have a different legal basis.3

Britain Redistributes the Cost of Fraud

From **October 7, 2024**, payment firms covered by UK Payment Systems Regulator rules were required to reimburse victims of specified **authorised push payment fraud** across defined UK systems, particularly **Faster Payments** and **CHAPS**, subject to eligibility. The regime covers individuals, qualifying microenterprises, and qualifying charities. The regulatory limit is **£85,000 per covered claim**, with an excess of no more than £100 in some cases. Decisions should ordinarily be made within five business days, with controlled extensions for additional information and an ultimate 35-business-day limit. This is not a promise to repay every disputed transfer and does not automatically cover international payments or every dispute with an honest seller.4

Economically, the basic rule divides reimbursement **50% between the sending and receiving firms**. The sender's bank first hears its customer's complaint, but the criminal's receiving account may be at another institution. Placing all loss on the sender could leave the institution that monitors beneficiary behavior without an economic cost for poor controls. Placing it all on the recipient could weaken the sender bank's incentive to detect behavioral signals known only to it. Britain did not discover a natural law of equal responsibility. It chose **an incentive-and-cost allocation rule** between institutions positioned differently to prevent fraud. The ratio can be criticized without ignoring the logic that turns the receiving firm from a conduit into a party with potential loss.5

For illustration, suppose a victim is deceived into sending **1,000 monetary units**. A recovery attempt finds **300** that can be returned. A hypothetical reimbursement rule grants another **600** from payment firms, leaving the victim with **100** of loss. The victim receives 900, but the fraudster did not necessarily return it all: 300 came back from transferred value and 600 shifted loss onto firms. If the firms split the 600, each records 300; it is not added again to victim loss. **Reimbursed money is not always recovered money**. Confusing them hides the difference between reducing criminal proceeds and changing who bears them.

Evaluation should therefore ask not only how many pounds victims received, but how much was removed from the fraud path before dissipation, how much banks paid from their own budgets, how much remained with victims, and what investigation, freezing, appeal, and review cost. An institution can improve customer satisfaction by financing losses after they occur while the source of harm continues efficiently.

In July 2026 the PSR published an independent **Frontier Economics** evaluation estimating that Faster Payments APP-fraud losses within the analysis fell about **21%**, equivalent to roughly **£73 million annually**, with about **35,000 fewer fraud incidents** under the model. It estimated additional prevention, claims-processing, and compliance costs to firms of **£44–56 million annually**. The estimated short-term net benefit was positive, while long-term competition, innovation, and market behavior remained less certain. These are **policy-evaluation estimates**, not a randomized experiment yielding a universal law.6

Broader reports meanwhile recorded increases in some total UK fraud losses for 2025. The responsible response is not to assume someone lied. The evaluation measures a defined fraud segment on a specified system, orders events by **transaction date**, and estimates a counterfactual policy effect. Broader reports include transactions outside protection and may order statistics by **claim-closure date**. Mixing domestic and international transfers, covered and uncovered fraud, recorded loss and paid reimbursement produces arithmetically exact but scientifically broken conclusions. The PSR dashboard for October 2024–March 2026 reports about **£316 million reimbursed**, roughly **88%** under its definition of eligible covered claims, with exclusions and methodological cautions. It does not mean 88% of every UK fraud victim's money was recovered.7

Brazil Follows the Money After It Moves

Brazil took a different route in its instant-payment system **Pix**. Rather than begin only with how two banks share the crime's outcome, the institutional design asked: **where did the money go after the first account?** Fraudsters may split value and move it rapidly. The Banco Central do Brasil developed the **Mecanismo Especial de Devolução**, or MED, and in 2025–2026 added capabilities for tracing successive value paths, sharing notifications among institutions, and examining balances that might be suspended and returned when suspicion and decision requirements are met.8

The official **DICT** API specification shows the difference between publicity and engineering. A recovery request passes named states: **CREATED**, **TRACKED** when a transfer-path graph is formed, **AWAITING_ANALYSIS**, **ANALYSED**, **REFUNDING**, and **COMPLETED** or **CANCELLED**. It describes automated ordering of candidate paths for balance suspension and notifications requiring recipient institutions to analyze suspect operations. It even defines an error when the original payment has not settled: recovery concerns money that **has already moved**, not a trick portraying the old payment as nonexistent.9

Tracing is not complete justice. Fraud proceeds may reach an innocent person paid for a legitimate service. Multiple sources may mingle in one account, creating allocation problems among claimants. Reports may arrive after the account empties, and suspicion must be balanced against an innocent holder's right to use funds. Brazilian rules therefore require

notification and analysis. Central-bank material states that MED **does not always guarantee recovery** and is not for an ordinary commercial dispute with an honest seller or a simple beneficiary-selection error. Official guidance permits a request within **80 days**, but economic time is harsher: the later the signal, the less likely a recoverable balance remains.8

Britain and Brazil intervene at different points. Britain reallocates **who pays the crime's cost** when loss settles or recovery fails. Brazil strengthens **pursuit of transferred value** before it disappears through layers of accounts. Neither school eliminates the other's limits. Firms can reimburse a victim while a fraudster remains rich if nothing is recovered; a tracing system can map every path without finding balance or lawful grounds for return. Success depends on what each party can prove and enforce without making an innocent person pay for suspected error.

Prevention Before Payment—and Its Limits

Europe addressed part of the risk **before send is pressed**. Regulation **(EU) 2024/886** introduced requirements for **verification of payee**, with related euro-area operating rules beginning in October 2025. The firm checks whether the entered name corresponds to the owner of the destination account. This small step reflects a different logic: slow identity verification rather than settlement as a whole. Yet the named owner may be exactly who the payer intended and still be a fraudster who fabricated an urgent story. Name matching tests beneficiary identity; **it does not test the truth of the story that made someone want to pay**.10

Financial interfaces must distinguish credential theft in which a criminal issues the payment, deception in which the customer presses the button, a legitimate trade followed by a delivery or quality dispute, and a transfer to a mistyped account. “Dispute” is no more diagnostically sufficient than “pain.” The route depends on **who issued the instruction, how it arose, the dispute type, network, law, and time**. In the United States, CFPB interpretation of **Regulation E** illustrates one distinction: if a fraudster obtains access credentials through deception and then initiates an electronic transfer, the transaction may be **unauthorized** even though the account holder disclosed credentials after being tricked. That need not be the same as a customer personally issuing an instruction because of a false story. Similar fraud labels do not make US and UK protections identical.11

Who Has the Least-Cost Means of Prevention?

The more useful economic question is: **which party can reduce the probability of loss at least cost?** The sender's bank knows normal customer behavior and documented signs of panic or urgency. The recipient's bank knows account age, incoming patterns, rapid outflows, and suspicious relations among connected accounts. An advertising or messaging platform may

see where the fraudulent story began, which neither bank sees. A victim has information but may be deliberately deceived; their preventive capacity is not equal to that of an institution observing millions of transactions. Responsibility allocation is market design, not a customer-service footnote.

Expected social cost includes not only direct loss but fraud probability, irrecoverable value, prevention and investigation resources, and the cost imposed when legitimate transfers are falsely blocked. Mandatory human review above a threshold may prevent crime while delaying a merchant's supplier payment or urgent family support. Broad reimbursement liability may encourage firms to refuse new customers or cross-border activity they cannot easily model. A low fraud rate achieved by making innocent use of money harder is not an unqualified success.

Fairness may itself be distributed unequally. An educated victim with time and records may construct a precise claim and appeal. An older person, second-language speaker, or someone who lost control of a phone may repeat the story across five screens and a call before being told they failed to take care. UK rules give special treatment to vulnerability and constrain the gross-negligence exception. Recovery systems should measure not only classification accuracy but claim abandonment, time without funds, and the share of decisions changed after independent appeal. Two legal rights are unequal if one is practically available only to someone able to spend a week explaining the deception.[4]

sarie and Beneficiary-Name Verification

Saudi Arabia launched **sarie**, its instant-payments system, in **2021**, with features including immediate beneficiary-name verification and identifiers other than IBAN. Prevention tools therefore already exist in the customer interface. But UK reimbursement limits and Brazilian Pix procedures cannot be imported and declared automatic Saudi rights. Local research should map each payment route under its rules: finality, reporting, freezing and recovery pathways, institutional powers, case classifications, and actual outcomes when a customer is persuaded to send money rather than an account being hacked.[1][2]

The Post-Settlement Obligations Atlas

I propose a **Post-Settlement Obligations Atlas** as a research concept, not an existing bank product or approved legal standard. It keeps five files separate: a **payment record** showing network and execution time; an **instruction-origin file** distinguishing the customer, stolen authority, or another mandate; a **value path** recording lawfully traceable balances and later transfers; a **legal-basis file** identifying recovery, reimbursement, or dispute rights and exclusions; and an **outcome budget** separating value recovered from a recipient,

compensation borne by institutions, and loss remaining with the victim. “Complaint closed” must never equal “the victim received their right.” Closure may follow an appealable refusal, partial compensation, full return, or insufficient evidence. Combining them hides different rights statistically.

Testing requires lawfully authorized, de-identified data and independent legal review. Four paths can be compared: an instruction stolen by a fraudster, one issued by a deceived customer, a mistyped beneficiary, and a legitimate commercial dispute. Measures include correct routing, false freezes of innocent funds, help time, claimant and institutional cost, detection of recurrent fraud-linked accounts, and net value actually recovered from offenders. Cross-market comparison must not combine different victim definitions, payment scopes, or accounting dates and announce victory from incompatible numbers.

A banker may ask whether wider post-payment recovery undermines the finality built to protect the system. The objection conflates two rights. Settlement finality stops interparticipant obligations becoming promises erased whenever someone disputes the original payment's purpose. Compensation or value return under published rules, independent adjudication, and controlled procedure creates a new enforceable obligation without pretending the first payment never happened. Either can be badly designed: finality used to conceal fraud evades responsibility; recovery without examination can confiscate innocent rights. Their apparent tension does not remove the need for both.

In Fiona Philipp's story, what is hardest to grasp is not that the first two transfers were executed, but that she returned seeking a third after warnings began to appear. Customer “will” is not a mechanical button isolated from the world, and protecting it cannot be reduced to identifying who touched the keyboard. Yet a bank cannot become guardian of every risky wish, and a court cannot transform every regretted action into fraud. Clear rules must preserve a person's authority to act and the right not to be abandoned when deception emerges.

The 2023 judgment could be remembered as a dry result: no general duty to stop the authorized transfers in those circumstances. It kept the post-notification recovery question alive. Later systems show that settlement can finish while the search for value and responsibility for loss remain open, without using finality of the first as an excuse to close the second. After discovering fraud, a person needs not another screen describing bank speed, but a path explaining **who can do what, when, on what evidence, and at whose cost**. A system may truthfully record completion in seconds and still leave the hardest part of the transaction outside its definition of success.

References

1. UK Supreme Court, Philipp v Barclays Bank UK PLC [2023] UKSC 25, July 12, 2023. The Court left a potential post-notification recovery claim unresolved.
2. BIS and CPMI–IOSCO, Principles for Financial Market Infrastructures, Principle 8: settlement finality, April 2012.
3. Visa UK, Chargeback: Debit & Credit Card Purchase Disputes.
4. UK Payment Systems Regulator, APP fraud reimbursement protections, effective October 7, 2024.
5. UK Payment Systems Regulator, PS23/3: Fighting authorised push payment fraud, 2023.
6. Frontier Economics, Payment scam policies reduce fraud and improve consumer protection; PSR, Payment fraud falls by £73m following PSR reimbursement scheme, July 2026.
7. UK Payment Systems Regulator, APP scams reimbursement dashboard for Q1 2026, updated July 30, 2026.
8. Banco Central do Brasil, Segurança no Pix; Mecanismo Especial de Devolução explanation, updated September 18, 2026.
9. Banco Central do Brasil, DICT API, MED 2.0 status specifications.
10. European Union, Regulation (EU) 2024/886; European Payments Council, Verification of Payee scheme rulebook now into force, October 2025.
11. US Consumer Financial Protection Bureau, Electronic Fund Transfers FAQs.
12. Saudi Central Bank, Launch of the sarie instant-payments system, February 20, 2021; sarie features.