2026 TREND- The Rise of Network Signals to Fight Fraud and Scams

Expanding Network Risk Signals March Forward in 2026

The Author

Since 2005, Ken has been in Online Security. He was a Director at MUFG Union Bank, retiring in early 2019. He helped shape the initial responses to the U.S. 2005 and 2011 FFIEC Regulatory Guidance to improve online security for US Banks. He is an early adopter and has selected and implemented a number of online security products. Ken was an advisor to the RSA eFraud Global Forum and a Program Committee member for the annual San Francisco RSA Conference. He is currently on The Knoble Scam Committee. He has published many white papers—on the need to focus on online customer safety, on online authentication and on how to select a multi-factor authentication solution. Most recently, his white papers and blogs have been on consumer financial scams. These recent white papers and blogs focus on controls to reduce scams and what countries are doing about scam reimbursement. He also was the editor for the complete list of definitions of financial scams, published by The Knoble in 2022. In 2019, he received the Legends of Fraud Award at the 3rd annual FraudCON conference in Israel. He is currently consulting to banks and to online security vendors.

Outline

Background

In the fight against fraud and consumer scams, nothing is more important than sharing fraud and scam data to fight what is a brutal transnational organized crime attack against the financial institutions (FIs) and their customers around the world. Yet, sharing of fraud and scam data proves to be difficult to execute because of privacy laws and the often times lack of explicit authorization. As a result, many FIs do not participate in fraud and scam data sharing. To help understate the worldwide state of fraud and scams data sharing, there is a 2025 report, Fraud and Scam Data Sharing Around the World, that covers the current state. There is also a 2025 blog on ideas for sharing data in the US, Why U.S. Banks Must Embrace Fraud Data Sharing.

Several countries in Southeast Asia are starting to mandate that banks share fraud and scam data. The UK has had several data sharing efforts for decades, including strong network signals from the Faster Payments systems operator Pay.UK. But even in the UK there is a demand for more organized fraud and scam data sharing.

But now, from financial institutions and payment systems operators, we are seeing a movement slowly taking shape to have effective data sharing. This report is focused specifically on what payment systems operators are doing to provide network risk signals today and what could be possible in the future that can make a real difference in this fight.

Introduction

This Report is about a focus on fraud and data sharing by payment system operators (PSOs). The network signals that PSOs can collect are potentially some of the strongest signals for FIs sending payments.

One major change that will make these network signals so much more important is the launch of the ISO 20022 global messaging standard that increases the amount of data in a payment message by almost ten times. Many of the newer faster payment systems started with this standard. This messaging information goes from the sending bank, through the payment systems operator process to the receiving bank. The added data in the payment message can be very valuable for fraud and scam detection. As examples, the sending bank can include transaction risk scores, free form message information/red flags and other metadata such as the time when the payment was initiated. With the payment systems operator having this new rich data set, the network risk signals can be even more robust than before. Realistically, we are a few years out before we see the benefits of the ISO 20022 standard for fraud and scam detection. Many payment systems are still transitioning to the ISO 20022 payment standard.

This report was conceived based on an idea from an over 40-year-old book called Discovering the Future-the Business of Paradigms by Joel Arthur Barker. This book lists one question that can invoke significant change. The question is " What is impossible to do today, which if it could be done would fundamentally change your business?". The author Joel Barker says "What is defined as 'impossible' today is impossible only in the context of present paradigms."

To understand the importance of this question, one has to only look at Generative AI Large Language Models. As recent as early 2025, it was impossible to create really good graphics and videos from LLMs. The graphics were weak, inconsistent and full of typos. Videos were not available. Yet, six months later, with Gemini 3, Sora, Nano Banana and NotebookLM, we see fabulous graphics and videos that can be meaningfully applied to business presentations and reports (and even used in this report). The paradigm changed that fast.

Another point Joel Barker makes is that often the person creating new rules to change the 'impossible' is an outsider. As an example, for fraud and scam solutions, the breakthrough ideas can very well come from players not in the current fraud and scam space. Remember that.

In this report we will discuss

1. What some PSOs are doing to share network signals.
2. What some PSOs are planning to do to make more network signals available

We will also talk about an exciting new concept for sharing network signals. It will involve an outsider. The 'outsider' will describe how a technology called Fully Homomorphic Encryption

(FHE) can change the thinking of FIs and payment system operators into why today data sharing is not as impossible as it sounds and how some of the current barriers to sharing data and risk signals can be removed . Another outsider we will talk about are international telco carriers who have monetized existing telco data into valuable fraud risk signals that help FIs prevent fraud and scam losses..

Report on Network Signal Growth and Projections

Current Network Signal Capabilities

UK

Probably the most advanced payment operator network signaling is with Pay.UK's Faster Payment System. Pay.UK is the payment systems operator for Faster Payments, Bacs and ICS. Mastercard Vocalink provides the payment infrastructure and processes the payments for Pay.UK financial institution members. Since 2018, Vocalink has provided network signals around money mules with the Mule Insight Tactical Solution-MITS (now transitioned to the Mastercard TRACE solution). When a member bank discovers a fraud or scam transaction, they initiate an API call to Vocalink to find the possible money mule path of the funds. According to Mastercard, "the technology enables suspicious payments to be tracked as they move between bank and building society accounts, regardless of whether the payment amount is split between multiple accounts, or those accounts belong to the same or different financial institutions."

In the past few years Mastercard has increased the network risk signal offerings with Consumer Fraud Risk (CFR) and A2A Protect. These additional products, accessed by banks with an API call at the start of a payment transaction, produce risk assessments on both the sending bank account and the receiving bank account.

These network risk signals that Mastercard Vocalink offer have fees in addition to the payment operator processing service fees.

The Philippines

Since 2019, Mastercard's Vocalink has worked with BancNet, the domestic payment switch operator, to provide real time payments infrastructure for InstaPay. In 2025, BancNet added the Mastercard TRACE network money mule risk signals service. Trace is used "to identify and prevent money laundering and financial crime. Powered by timely and large-scale payments data from multiple financial institutions, TRACE provides holistic intelligence beyond an individual financial institution's siloed view, enabling tracing of financial crime across a payments network."

US

In the US, the Early Warning Zelle payment service offers network signals to its members. At the December 2025 Global Anti-Scam Alliance Conference in Washington DC, Early Warning Chief Fraud Risk Office Ben Chance described how Zelle provides sending banks risk signals, called Risk Insights, about the receiving bank beneficiary account. In some cases, Chance said the network may know more about the risk of the receiving bank account than the receiving

bank itself. In addition, Risk Insights is described as: "the sending financial institution can assess information about the recipient's token behavior in the Zelle Network."

EU

In 2025, EBA Clearing introduced the Fraud Pattern and Anomaly Detection (FPAD) solution for SEPA payments. According to NetGuardians, "FPAD enhances the fraud detection controls in place. This is a Network view of data that provides risk insights on beneficiaries and fraud patterns. FPAD leverages the billions of transactions processed through EBA CLEARING's systems to generate a unique network view that characterises payment behaviours and account relationships. By retrieving transactions and building statistical profiles, FPAD creates a dynamic representation of how accounts interact, enabling sophisticated risk assessments." FPADs is accessed via an API call.

JPM Chase Bank

JPM Chase is not a payment network operator. But they have over 15 billion J.P. Morgan Payments transaction records. And they let their customers access this data to obtain a risk assessment on receiving bank accounts. They introduced a service in 2025, called the Account Confidence Score (ACS). "ACS evaluates accounts across multiple dimensions, including age, recency, location, payment history, known fraud, payment frequency and linkages."

Chase introduced a second product, called Kinexys Liink, in 2020. One of the purposes of Liinx is that it "allows for the validation of account information prior to initiating a payment." Liinx has over 400 financial institutions as members. Liinx partners with Nium Verify to "deliver global, real-time insights into the account beneficiaries across over 50 markets, including a number of Southeast Asian countries." In April 2025, Liinx added NACHA's Phixius to its partnership group. "Phixius will serve as Kinexys Liink's key U.S. payment information network Responder, enabling near real-time validation of domestic bank account data". Phixius is a secure, peer-to-peer payment information network in the US. Liinx "facilitates secure and private information and capability exchange between dozens of sophisticated global institutions and vendors."

Trustpair

There is another network type solution, outside of payment system operators, that is worth talking about. Trustpair help businesses validate beneficiary accounts at the time of enrollment. They cover 190 countries. They validate three components of the beneficiary accounts:

1. does the bank account exist at a real bank?
2. Is the account active?
3. Is the account legitimately owned by the person or business claiming it?

Trustpair uses automated tools to complete this validation, including using over 1000 banking data sources, for the majority of the validation. For a small percentage of more difficult validations, Trustpair has a proven manual set of steps to confirm account ownership.

Planned Network Signals

Canada

Payments Canada has been building its real-time payments system, called Real-Time Rail (RTR). It plans to include network risk signals about the receiving bank when RTR launches. This is called Central Fraud Analytics. According to Payments Canada, "Central Fraud Analytics assesses the likelihood that a payment is fraudulent before it is entered into the RTR system. A numerical score is generated for each payment message, based on inputs such as account history, transaction characteristics and cross-references with the Central Risk List. Participants are required to receive and assess this score before allowing a transaction to proceed and must report the outcome to Payments Canada. These outcomes help refine and improve the scoring model over time." This will include a risk score. Plus, participants will be required to submit confirmed fraud to Payments Canada.

US

The Clearing House

In 2025, The Clearing House (TCH) announced a pilot to provide network signals to participants using TCH's Real-Time Payments (RTP). In January 2026, The TCH described the proposed new service, Network-Level Risk Insights: "through an API, institutions can access attributes regarding a Receiver's account that may highlight unusual account behavior or prior fraud indicators, enabling more informed payment decisions." It also includes "a secure Case Management System allowing participants to alert one another of fraud claims and coordinate investigations, accelerating responses to emerging fraud trends and the ability to report fraud activity."

This pilot moved to production in January 2026.

The Federal Reserve

In 2025, FedNow started a pilot involving network signals for FedNow instant payments. FedNow describes the pilot as follows: "A pilot program is currently underway for an upcoming network intelligence tool that will allow financial institutions sending transactions over the FedNow Service to do a 'pre-check' on receiver accounts before making a payment" The sending bank would use an API to request this information.

Proposed Network Signals Consortiums

Payment system network signals are some of the best signals to detect fraud and scams. Yet, as we have seen these signals are few and far between. Too many payment system operators fail to use AI and machine learning models to mine their data to obtain these amazing signals. These network signals are pure gold. Just look how effective Mastercard Vocalink has been with network signals with the UK's Faster Payments and more recently in the Philippines. Thousands of money mules have been detected. Yes, there are a few operators providing these signals to their members. But not enough. In this section, we will discuss the "what is impossible" question by asking why can't we get a number of payment operators to allow financial institutions to use one bi-synchronous API to query multiple network operators simultaneously to obtain risk information about beneficiary accounts at receiving banks? Think of how we could limit risks on payment transactions. And what if the payment operators were in different countries—a form of cross-border regional co-operation?

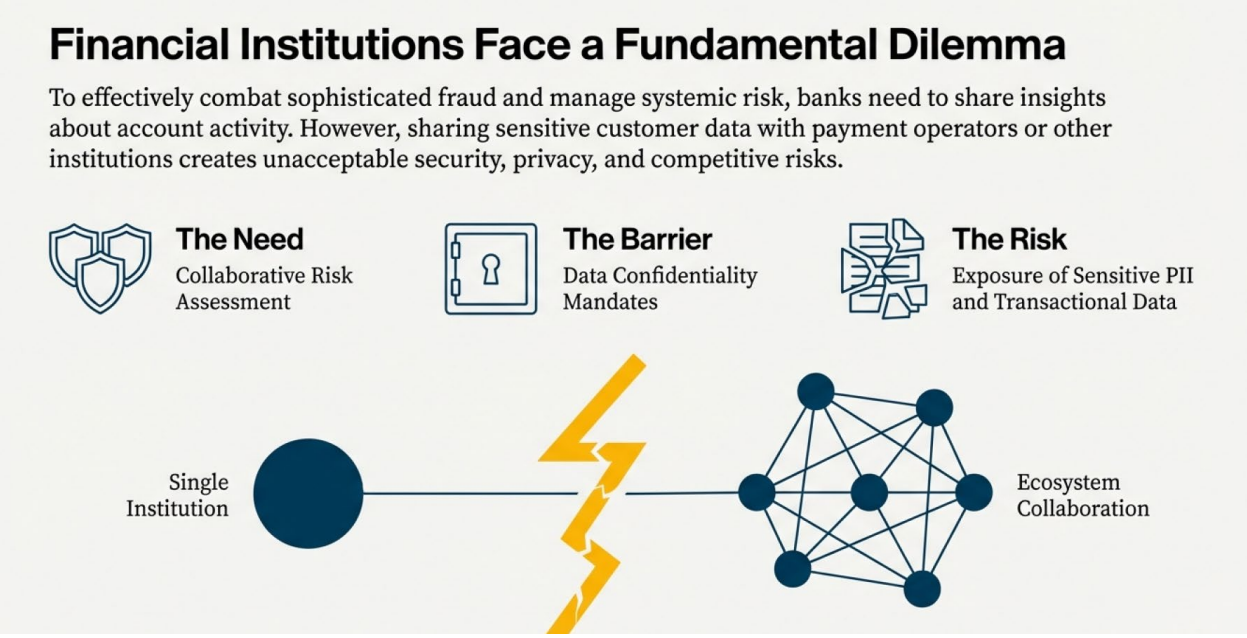
What is being proposed is technically possible. But right away there will be several key objections from payment operators and possibly regulators:

1. Our payment data cannot leave our country.
2. We have to respect the privacy of this data.
3. As a payment operator, I simply pass the payment information. I do not view it.
4. As a payment operator, I do not have permission from my members to share payment data, especially to non-members.

5. We only have permission to create network signals for faster payments (new product). Older payment types (e.g. wires) would require agreements to be modified.
6. We cannot afford a data breach of our operator payment data.
7. We need to be selective about the risk information we provide to non-members (maybe not risk scores on receiving bank accounts but risk attributes only, such as age of account or transaction velocity against the account)

Figure 1 shows some of the constraints that banks and network operators may have in sharing data.

Figure 1. Constraints to Sharing Financial Data



These issues are all valid concerns. But the good news is that many of these types of concerns, especially around the data sharing, have been previously addressed in non-financial areas. One of the best solution components to help with many of these concerns may be the use of Fully Homomorphic Encryption (FHE). As we have seen in true innovation, the best ideas come from other business sectors. In this case, for years governments have had sensitive data that must be shared in an extremely limited way. By using FHE, the source data is protected, while sharing takes place. One consideration to be aware of is that using strong encryption while processing data can increase the processing response time.

Before we continue, here are a few brief points on the benefits of Fully Homomorphic Encryption, a privacy enhancing technology, quoted directly from a Professor Serious blog:

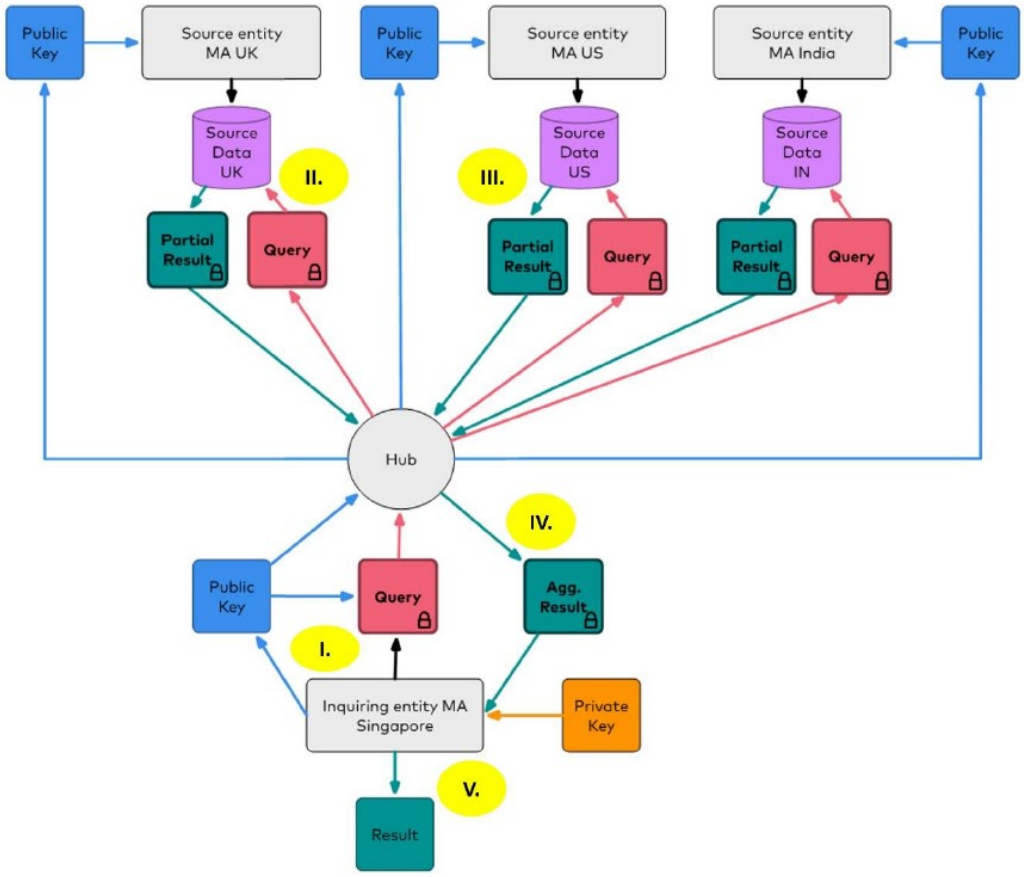
- Privacy-Enhancing Technologies (PETs) comprise methods, tools, and architectures that allow data to be used, shared, analyzed or learnt from, without exposing the underlying information, which may be sensitive.
- PETs enable data use with, at the same time, privacy assurance (achieved by technical means). PETs rest upon the counter-intuitive idea that you can analyze data whilst limiting the access to that data.
- The benefits of PETs are that they: allow systems to avoid holding, or exposing, 'raw' personal data; enable data collaboration across multiple organizations that cannot or should not share datasets.

For more interesting examples of using PET technologies, review the Financial Crime TechSprint from the UK's Financial Conduct Authority and read how to monetise data using PET technologies by Enveil CEO Ellison Anne Williams. This is an important read for payment systems operators. A key quote by CEO Ellison:

> "While Data at Rest and Data in Transit are commonly protected using standard data and transport encryption, the Data in Use segment is frequently overlooked by many organizations. Protecting data while it's being used is especially of critical importance when it comes to leveraging data for monetization purposes."

Let's look at an example of what the Singapore Monetary Authority of Singapore (MAS) and the Infocom Media Development Authority (IMDA) are trying to do in a proof of concept (POC) involving a number of entities across several countries. The project goal was to share financial crime intelligence across international borders – specifically between Singapore, the United States, India and the United Kingdom – while complying with a number of prevailing regulations in each country. See Figure 2 for the scope of the MAS/IMDA project.

Figure 2. Scope of MAS/IMDA Data Sharing Project



This POC was looking for risk information on receiving bank accounts (such as does receiving bank account exist in any country and is the Account Open date for this account within a particular number of days), similar to risk signals payment systems operator data can generate.

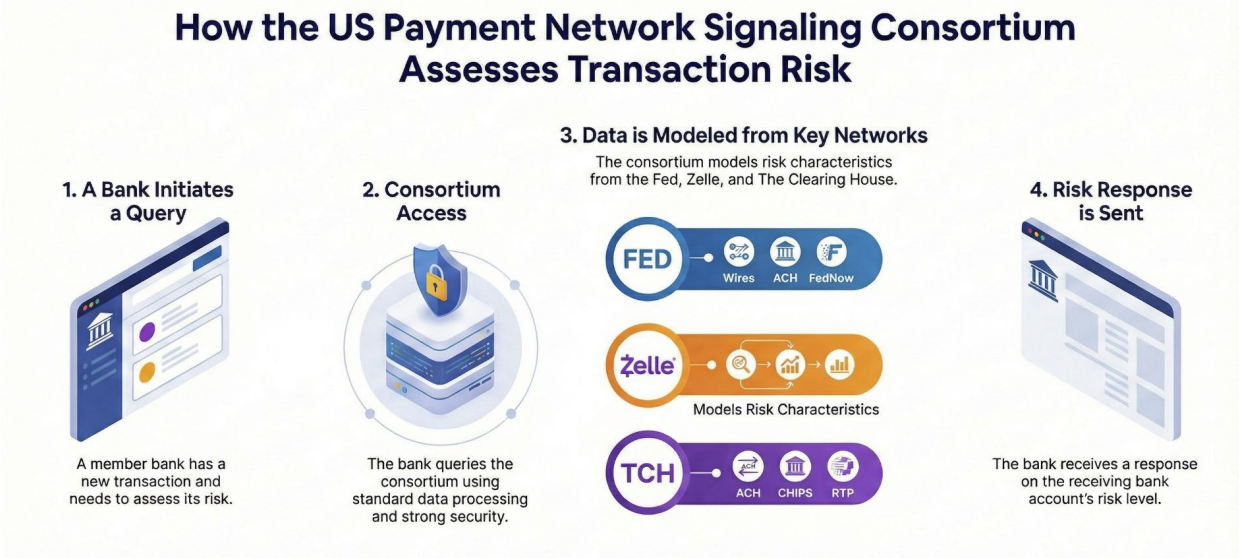
The POC concluded that FHE holds promise in this multi-country, multi-data base environment complying with the associated country regulations around privacy and data sharing.

Examples of Powerful Network Signaling Consortiums

One of the best examples of network signal sharing would be if US financial institutions could share network signals from the three primary US payment systems operators, the Federal Reserve (FED), TCH and Zelle. The good news is that both Zelle and TCH are owned by US banks. So, for the greater good of protecting the US financial ecosystem and its customers, everyone should be in favor of this. This would work by any US financial institution being allowed, under strong security, to use an API to request and access risk signals on receiving bank accounts. Figure 3 shows the simple approach of the payment systems operators providing risk signals,

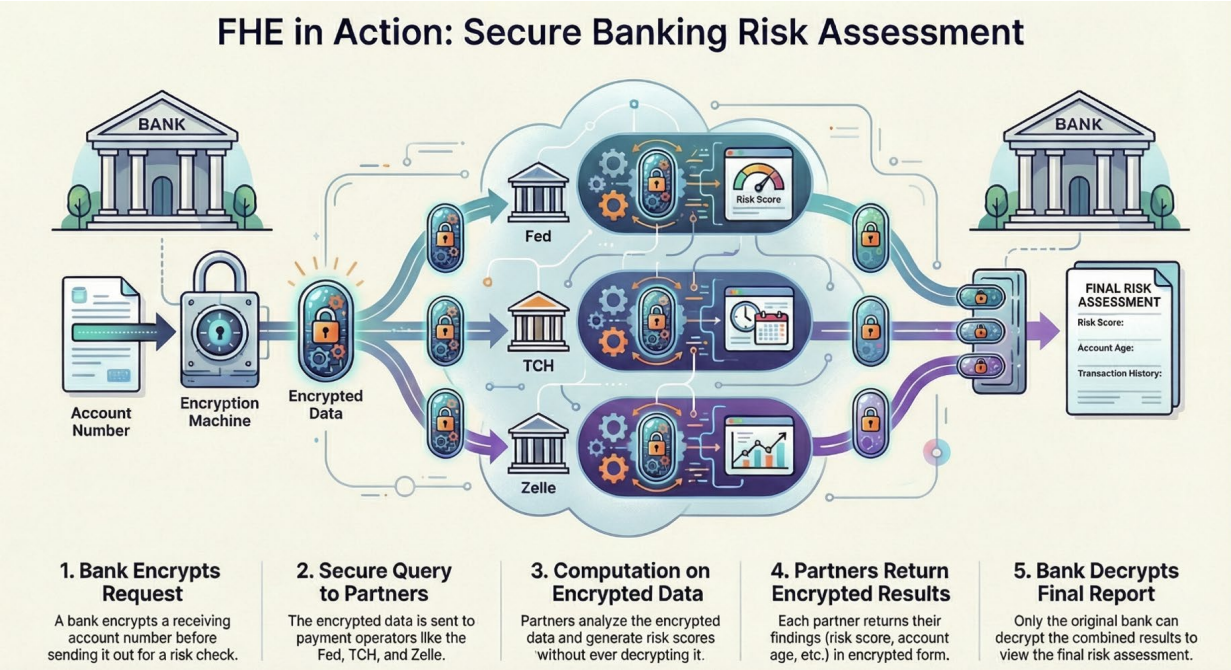
where strong encryption may not be required. Note: although Zelle is not technically a payment system operator (it clears via the FED and TCH), it does have important network risk signals. Also, in the Zelle network the transactions work with tokens for the sending and receiving account. Therefore, as a caution, the network data itself may not be able to identify the receiving bank account.

Figure 3. Simple Payment Network Sharing with US Payment Operators



On the other hand, because of the data constraints previously listed, there may be a need for Fully Homomorphic Encryption, Figure 4 shows the more complicated, but proven, method for the network signal sharing using FHE.

Figure 4. Complex Payment Network Sharing with US Payment Operators



In both of these examples the central hub only does orchestration. The payment system operator data always stays local.

This network signal data sharing could even be expanded to include consortium data available within financial institutions and vendor systems. We already see JPM Chase having special receiving bank network risk signal sharing with its customers. For a fee, why not make this available to other financial institutions to help in the fight against fraud and scams.

Just imagine how powerful this could be to help identify money mule accounts. Money mule accounts are the fuel that allows fraud and scams. And it doesn't stop at the border of one country. Think of the tens of billions of dollars lost in business email compromises where much of the money goes overseas. Think of the hundreds of billions of dollars lost in consumer scam annually. We just don't have our A-team defense in place. Instead, we have so many excuses about why we cannot share fraud and scam data, regulations that prohibit data sharing or make it ambiguous. But if we can share data from payment systems operators, can we finally move forward? And to be fair, many of the payment system operators need to start building payment modeling across all of their payment transaction types to be able to generate network signals. This is especially true for wires and ACH transactions in the US not having network risk signals. Most of the network signal transaction modeling so far has been done for faster payments/Instant Payments transactions.

So, this proposal is clearly a multi-year effort by payment systems operators. The good news is that several vendors, including Mastercard, and Feedzai, are developing solutions involving

analytic models and operating platforms to support these proposals. Watch for Enveil with its Fully Homomorphic Encryption to help in this space.

A moonshot proposal would be what is shown in Figure 5. What if we could have a consortium involving payment system operators from the US, Canadian, UK and the European Union Payment Operators (six payment system operators total). And a financial institution from any of these countries could access this consortium to obtain risk information on receiving banks.

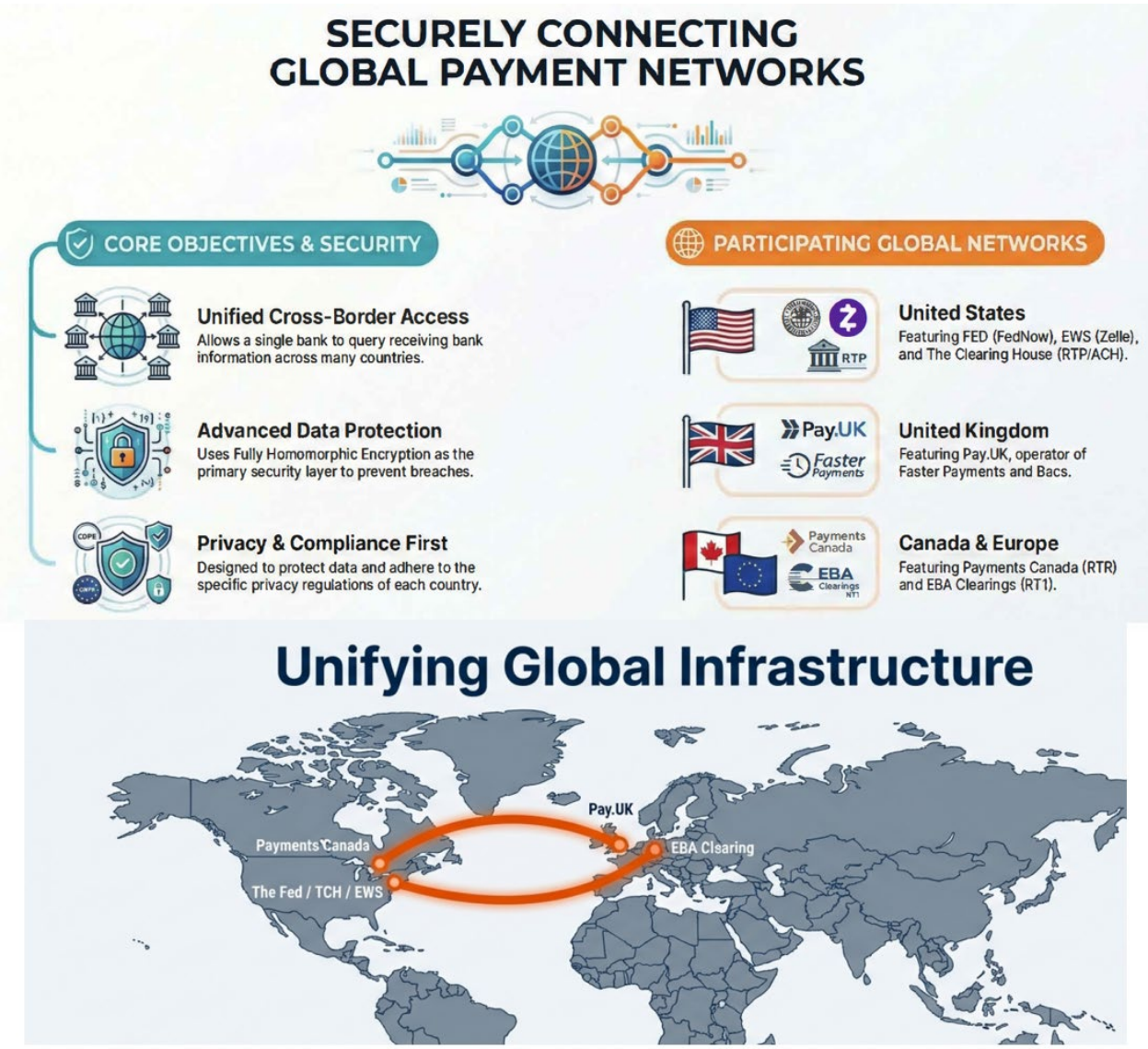
This is not so far-fetched when you consider what Singapore is exploring for ASEAN countries. Yes, that project is more about data sharing for money mule accounts. But it might not take much to also include payment operators in its consortium. The ASEAN countries, especially Singapore, are much more organized about fighting fraud and scams than countries in the Western world.

To demonstrate the drive for new payment flows in Southeast Asia, The Bank for International Settlements (BIS) in January 2026 just announced Project Nexus. "Project Nexus is poised to revolutionise the global payments landscape by seamlessly connecting Instant Payment Systems (IPSs) across 6 countries (The Philippines, Malaysia, Indonesia, India, Singapore, Thailand), significantly enhancing transaction speed, lowering costs, and boosting cross-border connectivity." This will go live in 2026. The article went on to say: "While Nexus has started in ASEAN, it has a global ambition—as it will be able to link up very easily and speedily with other economies."

Project Nexus is part of the BIS international cross-border payment initiative. A natural next step for these ASEAN countries, including India, would be to share the six countries payment systems operator network risk signals.

Now, these much larger consortiums of several payment operators involving multiple countries could very well require Fully Homomorphic Encryption because of the multitude of regulations around customer data privacy and data sharing as well as probable requirements that data not leave the respective countries. This is shown in Figure 5.

Figure 5 Payment System Operator Consortium involving US, Canadian, UK and the European Union Payment Operators



One additional thought on these consortiums involves the potential fees the consortium members can earn. A significant analogy to payment operators earning fees for fraud and scam risk signals is what has happened with international telco carriers. Back around the mid-2010s, the US carriers started to offer mobile risk score to US banks (at the request of US banks). The uptake was initially slow, but then has exploded in the past few years. In fact, today many international carriers offer an array of risk score signals productized by the GSMA, the Global trade association for international carriers, and GSMA currently list several dozen Camara API

risk signal options. Telcos now consider risk signal revenue as a noticeable portion of their revenue.

Another example of monetizing data comes from JPM Chase with it previously discussed Kinexys Liinx service. JPM Chase talks about "Collective intelligence is possible when a network of participants shares information in a secure and controlled manner, allowing it to be used and interpreted outside of its organization of origin…. Not only can companies monetize their data assets, but the shared information can drive better decision-making, innovation and benefit entire industries, creating a whole that is more than the sum of its parts."

Summary

The purpose of these proposals for network signal data sharing is to have the best defense against the large transnational organized crime groups and nation-states bent on destroying financial institutions and their customers. **We need to think of this as a war and have the best financial institution defense tools in place, possibly even with government providing supporting legislation.** We see ASEAN countries serious about this fight and adding legislative support for all kinds of data sharing. So, governments can change the playing field! Yes, what is being proposed here might be viewed as impossible and maybe just Don Quixote tilting at windmills. But just maybe it is finally time to do the impossible to make the fight against fraud and scams more favorable to the financial institutions and their customers. Why can't Don Quixote join this fight? (Figure 5)

Figure 5. Don Quixote Joining the Fraud and Scam Fight

With this report, we have shown examples of network signals, mainly for newer faster payments, that exist today. We have shown pilots and proofs of concepts for new network signaling. Finally, we have shown that it is possible to have a payment system operator consortium that could involve payment operator data from multiple countries. We have to stop bringing a knife to a gun fight.

The concept of sharing network data signals among network system operators is something that cannot be done quickly. Afterall, at minimum, the payment systems operators are limited by the current legal agreements between the operators and their members, often restricting the

use of the payment data. But as we see the innovation from BIS on cross border instant payments in 2026, we should start to see more openness to share network signals.

Recently UK's the Royal United Services Institute's (RUSI} Future of Financial Intelligence Sharing (FFIS) recommended that "*economic crime security by design* should be integrated at the design stage within the payments reform policy-development process" for payments. What better way to do this than by using the network risk signals from payment processors.

What is being proposed here will be dismissed by many as just not the way we do business. Some may ask if the author has been out of the business too long? Actually, that may be what is takes. Get out of your normal well-trodden path and look at what is going on around the world. Is there anything more relevant that GenAI and that 'little' gaming chip company, now the most valuable company in the world, that are showing the existing blue-chip players how the game will be played today and in the future. The world is being turned upside down today. But, not in the fraud and scam prevention space. Isn't it time?

Next Steps

If fraud fighters agree that a consortium of network risk signals from multiple payment operators is valuable, they need to have discussions with their payment counterparts within their banks. After all, the payment managers are the ones that sit on the payment operator boards and make decisions about new services. To get older payment transactions, such as wires and ACH, included in network signals will probably require rewriting existing agreements to allow the use of the payment transaction data for the creation of network signals that might be sold to entities that are not part of the payment system (e.g. I am doing a FedWire and want to get a risk score from TCH or Payments Canada).

Watch for near-term change from Singapore and South East Asia. They have some of the most need for cross-border payments and network risk signals.