kinexys
by J.P.Morgan

Tackling fraudulent activity in cross-border payments

Cross-border payments are becoming ever more important for economies around the world, driven by growth in international tourism, e-commerce and remittances. These transactions are an important way for governments to secure foreign currency reserves, and for business and workers to operate in a globalized economy. Yet, actually executing a cross border - transaction remains notoriously complex and inefficient. The fragmented nature of the payments system, along with the rapidly expanding volumes, has made this area especially prone to fraudulent activity.

Contactless criminals

Cyber-criminal groups specifically target cross-border transactions because the process is opaque and convoluted, with little standardization. It is estimated that there are 26,000 global rules that affect cross-border payments.[1] There is no single regulatory body as each country's banking system has its own regulations and security policies. Consequently, organized criminals can target vulnerabilities at certain banks in certain countries and use them to access wider networks. They can then re-route transactions to different beneficiaries, spread around the world, confident that there will be little chance of recovering the funds. In one example, hackers sent fraudulent payment instructions from a compromised account at Bangladesh Bank that was linked to the Federal Reserve Bank of New York. Around $100mn was stolen, the majority of which has still not been retrieved.[2]

Although cyber heists may grab the headlines, more common routes of attack are to send fake invoices or set-up false supplier accounts. According to PYMTs.com, the majority of payment fraud attempts target AP operations.[3] Cross-border payments are also a key facilitator in the endless global churn of money laundering. Shell companies can be set-up in jurisdictions with low regulatory oversight, making it hard to check the legitimacy of the entity. Funds can be received and sent on with a minimal threat of discovery. Conversely, legitimate company accounts may be taken over and used as proxies by criminal gangs.

1 Tipalti. 'The Total Guide to Cross-Border Payments.' Available: https://tipalti.com/cross-border-payments-guide/. Accessed April 2021.

[2] Wall Street Journal, March 2016. '*Crime Scene: Who Stole $100 Million From Bangladesh's Account at the New York Fed?*' Available at: https://www.wsj.com/articles/crime-scene-who-stole-100-million-from-bangladeshs-account-at-the-new-york-fed 1458052955. Accessed April 2021.

[3] PYMTS.com, April 2020. '*AP Automation Combats COVID Scams*.' Available at: https://www.pymnts.com/news/security-and risk/2020/ap-automation-combats-covid-scams/. Accessed April 2021.

kinexys
by J.P.Morgan

A comprehensive threat

As well as the damage to wider society, payment-related fraud also has major ramifications for both banks and their clients. Not only is there the loss of money – which often can only be recovered through insurance claims or drawn-out legal proceedings between different entities – there is also the potential loss of sensitive data which can then compromise other areas of the impacted bank. A major breach may also result in significant reputational damage. Meanwhile, if a bank is deemed to have been negligent regarding anti-money laundering (AML) requirements or terrorist financing regulations, then they could face significant fines. In 2020, over $10bn in penalties were issued by regulators for non compliance in these areas.[4]

The customer pays the bill

But ultimately it is the customers that have to foot the bill, whether that is a corporate client, a small business or a worker sending money home to their family in a different country. The need to constantly verify transactions, check beneficiaries and ensure compliance is the reason that cross-border payments are so slow. According to the Bank for International Settlements, it can take up to seven days to complete a transaction.[5] Around 2-5% of cross border B2B transactions are checked or subjected to additional investigations.[6] Considering the huge volume of transactions, this quickly adds up, with the costs are generally passed on to the consumer. This is why cross-border transfers can cost up to 10% of the total transaction. The average cost for sending remittances remains 6.8% on a global basis, still above the G20 commitment to reduce fees to 5%.[7]

Liink – Transforming how information moves

J.P. Morgan's Liink is a peer-to peer, permission-based blockchain network. One of the reasons that blockchain is creating such excitement among financial service firms is because it has the potential to reduce fraud in cross-border payments. In a traditional payments model, each bank has its own separate ledger, with little sharing of information. If a hacker can access this, then they are able to alter information and make fraudulent transactions. As the other counterparties in the transaction do not have access to the originating bank's ledger, the fraud can go undetected. Importantly, once information has been added to the ledger, it is immutable and cannot be altered. In this scenario it becomes almost impossible to tamper with a supplier invoice or change beneficiary details. With the Bangladesh Bank example, the criminals initially made

[4] FStech.co.uk, November 2020. 'Regulators issued $10 bn in AML fines in 2020.' Available at: https://www.fstech.co.uk/fst/Regulators_Issue_10bn_AML_Fines_2020_Fenergo.php#:~:text=Regulators%20issued%20more% 20than%20%2410,according%20to%20research%20from%20Fenergo. Accessed April 2021.

[5] BIS, March 2020. '*Innovations in payments*.' Available at: https://www.bis.org/publ/qtrpdf/r_qt2003f.htm. April 2021.

[6] PYMNTS.com, July 2020. 'Deep Dive: How Overlapping Regulations And Fraud Risks Complicate SMBs' B2B Cross-Border Payments.' Available at: https://www.pymnts.com/smarter-payments/2020/regulations-fraud-b2b-payments/. Accessed April 2021.

[7] BIS, March 2020. '*Innovations in payments*.' Available at: https://www.bis.org/publ/qtrpdf/r_qt2003f.htm. April 2020.

transfer requests for almost $900mn. They were only stopped when a spelling mistake was spotted in a payment message, but not before sizable transfers had already been completed.[8] With blockchain this fraud would be nearly impossible. Due to cryptographic hash techniques, even the minutest change in information would be instantly flagged, invalidating the payment.

Validate account information globally with speed, simplicity, and security.

JP Morgan's Confirm application, which runs on the Liink network, adds another layer of security. It allows payees to quickly and simply validate account information before an international payment is sent, something that Sushil Raja, global head of Liink describes as "holy grail" for banks. It does this by sending out a payment inquiry to participating banks on the Liink network, which then validates whether the information is accurate. Instead of having to validate information through manual methods such as emails or telephone calls to the corresponding parties, it can be done in seconds. As participants will know before conducting a transaction if the beneficiary details match the owner of the account, it greatly reduces the possibility of fraud or a transaction being returned due to incorrect information. Because Confirm operates in near real-time it also has the potential to significantly cut processing times. JP Morgan estimates that it could cut delays by 3-4 days[9].

Closing the gaps

Because the Liink network is designed to facilitate the quick and secure sharing of information, the unique structure actually incentivizes the sharing of data, as information requestors will pay a fee for what they receive. The key is scale. The more banks that join the network, the more information can be shared, and the harder it is for fraudsters and other bad actors to exploit the gaps in the system. Today, over 400 institutions have signed letters of intent to join the network, and that number continues to grow. Together they are helping to create a financial system that is faster, cheaper and safer, for all parties involved.

[8] Reuters, March 2016. '*How a hacker's typo helped stop a billion dollar bank heist.*' Available at: https://www.reuters.com/article/us-usa-fed-bangladesh-typo-insight-idUSKCN0WC0TC. Accessed April 2021.

[9] JPMC Internal Study, 2020

kinexys
by J.P.Morgan