Fighting the Fraudsters

As bank fraud becomes increasingly sophisticated, compliance is the strategy of choice to beat it. Leading the way is the Society for Worldwide Interbank Financial Telecommunication or SWIFT, one of the world's leading providers of compliance services.

Bank fraud is changing. It was not long ago that the greatest threat to bank security was to its customers. Individual accounts were the targets and customers had to be protected from hackers getting hold of security information that could, in theory, allow a criminal network to clear out an account. The biggest threat now however is to banks themselves and fraudulent payments made between banks on the networks that connect them.

The way a bank moves its money is now under the spotlight along with the innovative tools for financial transactions across the financial system that customers demand. In emerging economies especially, integrating hundreds of thousands of previously underbanked clients into online networks through mobile payments, digital wallets, cryptocurrencies, crowdfunding and alternative lending is providing a revolution in convenience. And a goldmine for criminals.

The downside is that new technology also opens up new channels for cyberattacks. A new, more highly organised and more professional criminal class has become active in the past few years, either working alone or in conjunction with insiders. The most publicized incidents have happened at traditional banks.

In February 2016, the Bank of Bangladesh, the central bank of Bangladesh, suffered 35 near-simultaneous fraudulent transactions issued by security hackers via the SWIFT network. They withdrew nearly $1bn from the Federal Reserve Bank of New York account belonging to the Bank of Bangladesh. Five of the 35 instructions were successful and moved $101M. It was only a

misspelling on one of the instructions that raised suspicions at the US bank. It responded by blocking the remaining 30 transactions which were worth $850M. Only part of the $101M was recovered.

Tony Wicks, head of anti money-laundering at SWIFT, says "That was a watershed moment, a very large wake up call. It made people recognise fraudsters were no longer attacking the edges of the banking system, but were making attacks directly on the heart of the system itself. What we saw were cyber hackers actually getting inside the institution. It is certainly a sea change in the modus operandi of the fraudsters."

According to SWIFT, cyber attackers are innovative and work with subtlety and sophistication. They cover their tracks and exploit the fact that payments move faster than ever. Thanks to the speed and finality of the settlement, wire payment frauds are particularly attractive and have risen dramatically, from 14% in 2014 to 48% in 2018.

"Fraudsters will follow the money, they will move to make money in the most cost effective areas, they are running and operating very much as a business. They are choosing to target areas and systems where they don't believe that there are controls in place, something that Swift has worked hard in terms of raising the bar in its community." adds Wicks.

One of the challenges for SWIFT is how to address the rapid increase in transaction speeds in an industry that needs to make high volumes of cross border transactions safely. To address this, SWIFT created a protocol called Global Payments Innovation (GPI) in 2017 which increased the speed, transparency and tracking of cross-border payments. It drew together over 120 key transaction banks from more than 200 countries and territories around the world, and because SWIFT is where the critical mass of cross-border payments happen, its global payments innovation has been hailed as one of the biggest advancements in international payments in several decades.

"What we're seeing in the payments industry, in fact across the entirety of financial services, is that the world is speeding up. Everything is moving

towards real-time. In the cross-border setting, it would take multiple days to settle a transaction, with SWIFT GPI, we now settle 40% of all transactions within 5 minutes, and now over 50% of messages across Swift are GPI-enabled." says Wicks.

A second strategy launched in October 2018 is SWIFT Payment Controls, an in-network solution to combat fraudulent payments and to help strengthen customers' existing security. The service boosts GPI and screens transactions in-flight, flagging, holding or rejecting them based on risk policies designed to spot unusual intermediaries and out-of-hours or non-typical activity.

But security systems run by SWIFT must evolve with the threat, and the danger of complacency remains ever-present. A cyber attack in India in August 2018 illustrated just how resourceful and imaginative criminals are when designing a heist. Cosmos Bank in India was attacked in a $13.4 theft in two phases over a single weekend. The first was an international effort - after a highly sophisticated malware attack disabled part of the bank's defences, money mules in 28 different countries, all extracting cash from their local ATMs with 450 cloned bank cards. According to estimates, 15,000 transactions were carried out over a seven-hour period. The second phase took place the following Monday, when a SWIFT transaction saw Cosmos move $1.93m to an account at a bank in Hong Kong.

The most powerful tool available to banking networks is strong compliance, ensuring banks adhere closely to the security protocols of the regulatory bodies that invest in the fight against cybercrime, money laundering and adherence to sanctions. In many ways, security is a governance issue because for many financial institutions, it still remains an information technology issue with organisational silos addressing only a part of the threat rather than a C-suite priority with an overview.

For Tony Wicks, that is changing and there is a growing convergence between the different functions within a financial organisation. "Historically you'd have your security team, you'd have your regulatory team, looking at

compliance, you'd have other types of risk mitigation in relation to suppliers and your counterparts. It's all about an organisation having a complete view of risk. Ultimately, you're a connected network of institutions and it is that connected network that is the strength and also the weakness".