Guidepost

THE DIGITAL PAYMENT CRIME THREAT PORTENDS A FINTECH/REGTECH ALLIANCE

As published in PaymentSource.com, October 4, 2018.

Digital payments remain vulnerable to abuse by financial criminals seeking to make fast payments and undetected payments through the financial system.

There are multiple ways in which digital payments can be used by those laundering money, committing fraud, or financing terrorism. What are some of the risks fintechs should be thinking about, and what are the ways to mitigate them?

Because financial crime risks, properly mitigated, are in fact business opportunities, fintechs that take this seriously can give themselves a competitive advantage over those that have not done so.

Here are some notable examples and typologies we have come across in our own work and research:

Transaction laundering. In transaction laundering, criminals set up an internet store that purports to sell legitimate goods but is in fact laundering funds or selling illicit goods. These fake stores are onboarded by unsuspecting merchant processor systems, which process the transactions in good faith. Recent research by EverCompliant, a cyberintelligence firm, suggests that transaction laundering for the online sales of products and services in the U.S. for all financial services (of which fintech is only a part) reaches over an estimated $200 billion a year, with $6 billion going on illicit goods.

Buyer/seller collusion. As these figures suggest, there is often no underlying trade taking place. In these instances, there is likely to be collusion between the "buyers" and "sellers."

Authorized pushed payment fraud. This crime occurs when fraudsters mislead consumers or businesses through false documentation, or manipulation through social-engineering techniques, into sending a digital payment to an account that appears to be legitimate but is in fact controlled by the fraudster.

Synthetic identify fraud. In "traditional" identity fraud, the criminal steals the credentials of a real individual. In synthetic identity fraud, the criminal starts with some authentic stolen credentials. In the United States, these are often Social Security numbers, especially those from economically "dormant" individuals such as children and senior people, which are then synthesized with fake information on addresses, age, etc., to create a new identity. According to research published in May, synthetic identity fraud resulted in $820 million in credit card losses in 2017, up from $580 million in 2015, with further rises expected in the future.

Terrorist financing. Terrorism experts have suggested for some time that online stores could be used as fronts by terrorist groups, and the March 2018 conviction of a U.S. citizen, Mohamed Elshinawy, has provided an example of this. Elshinawy, a self-professed member of the Islamic State, was believed to have received more than $8,000 from Islamic State facilitators via PayPal, ostensibly for sales of printers through his eBay account. The funds were intended to support operations in the United States, including possible attacks.

These kinds of crimes raise two key financial crime risks for fintechs in the digital payments sector: genuinely knowing your customer (KYC) and identifying unusual patterns in transactions.

Regulation technology, or regtech, is an important means of addressing these issues. There are an increasing range and variety of sophisticated online/virtual document verification firms that can test document validity through a range of techniques, from visual analysis to verifying against publicly available information and "scraping" from social media. Other firms have focused on the second problem, developing transactional monitoring tools, some using machine learning, to seek to identify unusual patterns of transactions.

However, before turning to technology, any firm working in the fintech sector should undertake a customer risk assessment during onboarding. Such an assessment should use factors that are relevant to the customer type and business model, to ensure it assesses credible indicators of risk. An assessment also provides an invaluable future benchmark for whether account and client conduct can be considered "normal," and should be regularly refreshed as the relationship continues.

Moreover, fintech employees themselves need to understand what financial crime might look like "in the moment." Even if regtech tools can identify potential "alerts," these need to be investigated internally before possibly filing a suspicious activity report. When it comes to customer due diligence and KYC, often simple in-house investigatory measures can help. For example, a Google search of the client's payment details or static information, such as an address, might also appear on other sites for other, completely unrelated and possibly questionable businesses.

In terms of transactions, there are common red flags that digital payments fintechs should be aware, including:

Turnover mismatch. At the opening of an account, it is common to ask the client what kind of turnover is likely in the account. Substantial differences in the expected pattern of use are worthy of investigation.

Payments incommensurate with business. Accounts might receive funds that do not appear realistic in light of the goods supposedly being traded. For instance, an online bookstore is likely to receive payments well below the $100 mark, and anything above that level would be anomalous.

Possible payment "structuring." Accounts might receive a large amount of similar-sized funds, possibly in, or close to, round figures. This might be indicative of the "structured" payments of illicit funds in smaller batches, to avoid suspicion.

High/low velocity of payments. Short periods of high-velocity payments, or alternatively long periods of account dormancy, or alternating periods of both, are potentially indicative of an account not being used for the trading of goods, which would be likely to show a more random pattern.

Frequent cross-border transactions. Numerous cross-border payments from different jurisdictions might also be of concern, especially when those jurisdictions, such as known tax havens, might be considered higher risk from a financial-crime perspective.

None of these individual indicators should be sufficient on its own to show an elevated risk. However, in increasing combination, they should be of concern to any digital payment provider. The key question that needs to be asked is whether this makes sense, and if it does not, act accordingly. Combining this information, with that gathered at onboarding and during the life cycle of the customer, is key to helping to establishing and sifting out the potentially unusual from the downright suspicious.

**CO-WRITTEN BY GEMMA ROGERS, CO-FOUNDER, FINTRAIL LTD
GEMMA ROGERS IS THE CO-FOUNDER OF FINTRAIL LTD., A FINANCIAL TECHNOLOGY COMPLIANCE CONSULTING FIRM. SHE HAS A PASSION FOR CHANGING THE TERMS OF DEBATE AROUND FINANCIAL CRIME RISK MANAGEMENT, DEBUNKING THE LETHARGIC TICK-BOX CONCEPTS OF OLD AND FOCUSING ON INTELLIGENT, INCLUSIVE AND BUSINESS-FOCUSED SOLUTIONS. DRAWING ON HER WEALTH OF EXPERIENCE ACROSS DISRUPTIVE SERVICES, INTERNATIONAL BANKING AND THE PUBLIC SECTOR, GEMMA BRINGS CLIENTS DEEP DOMAIN KNOWLEDGE OF FINANCIAL CRIME RISKS, AS WELL AS AN ABILITY TO EXECUTE INTELLIGENT FRAMEWORKS ACROSS BOTH EMERGING PLATFORMS AND ESTABLISHED FINANCIAL SERVICES.

JULIE MYERS WOOD

Chief Executive Officer

As the Chief Executive Officer of Guidepost Solutions, I focus on helping corporations resolve problems with government agencies, and ensure they are proactively addressing compliance requirements. Prior to joining the private sector, I held leadership positions with the U.S. Departments of Homeland Security, Commerce, Treasury and Justice. This includes serving as the Head of Immigration and Customs Enforcement, Homeland Security's largest investigative component, as well as the Assistant Secretary for Export Enforcement and the Chief of Staff for the Criminal Division at the Department of Justice. Throughout my government and private sector career, I have helped develop, implement and execute compliance programs and crisis management plans and responses across a wide range of industries for numerous companies. I am nationally recognized as a speaker for my expertise on compliance, security, immigration and other law enforcement issues and have testified before Congress.