NICE Actimize

Insights Article

The Rise of Fraud Threats and the Implications of Canadian Payments Modernization: How Soon is Now?

While it's true that Canadian payments modernization will harness the agility of technology to transform the efficiency and speed of the nation's payments and settlement system, the reality is that such progress will bring with it an increase in fraud threats. And with the digital acceleration due to the effects of COVID-19, we are seeing both Canadian consumers and businesses quickly adopting digital methods to spend, send and receive money. In fact, a record-setting 61.3 million Interac e-Transfer transactions took place in April 2020 – with firsttime Interac e-Transfer users increased by 43 percent since mid-March 2020. Another day, another welcomed step in the evolution of banking as we know it and another need for Financial Institutions (FIs) to take a serious look at how to address these threats to safeguard themselves, businesses and consumers.

Setting the stage

Real-time payments systems and schemes are often based on ISO20022 and are proliferating across the globe. Canada is now joining this group of countries, with an ambitious modernization plan across its payments systems that is beginning to gain traction.

There are three main parts to payments modernization:

- A replacement for the Large Value Transfer System (LVTS), called Lynx, which will provide Real-Time Gross Settlement (RTGS)
- Updates to the existing clearing and settlement system (ACSS) along with a replacement system, Settlement Optimization Engine (SOE)
- A brand-new payment rail, for now called Real-Time Rail (RTR)

The RTR, where the key fraud issues will originate, may have the biggest impact on consumer and business payments and have large impacts for fraud. In practical terms, the RTR means that consumers and businesses will have access to real-time payments directly from their online or mobile banking service. This approach builds on the current E-Transfer service, which in some circumstances can be real time. Although E-Transfer currently makes up only one percent of payments, it is extremely fast growing, as it grew at an average annual rate of 45 percent5% volume and value over the last five years, according to the 2018 Payments Canada Trends Report.

The biggest fraud threat will come from the take up of real-time payments itself. Once the RTR is in place (scheduled for 2022 post lynx including ISO20022), there will be a significant move by consumers for many of the current batch (EFT) payments to move to the RTR, as well as organic growth and supplanting cash. Therefore, large volumes of payments will move from revocable to irrevocable, with significant impact for fraud.

Embedded within the RTR will be the ability to provide alias/proxy services, allowing payments to be made without account details, perhaps with just a phone number or an email address. RTR payments will be irrevocable payments, unlike Electronic Funds Transfers (EFTs) that make up the bulk of online payments, offering benefits to both sending and receiving parties.

From a fraud point of view, these inherent characteristics will produce various impacts. The inbuilt support for alias to account details, when combined with real time, creates a potent fraud vector that has been exploited in the case of Zelle in the U.S. The richer messaging formats and support for services, such as request for payment, offer clear benefits, but can clearly be exploited by fraudsters, especially in the case of social engineering.

Just as genuine customers will take to real-time payments, it's almost inevitable that fraudsters will increase their attacks on the RTR as they have in other markets. The combination of these two factors makes for a landscape where it's hard to spot the fraud without impacting lots of genuine customers, either in terms of fraud, greater friction or delayed or declined payments.

One prime example of this occurred in the UK where there was a 132 percent increase in online banking fraud in the year faster payments was introduced (2007 vs 2008). This has since increased to £152 million, according to UK Finance's Fraud the Facts 2019, with preventions of £317 million.

As the banks have invested more in prevention, fraudsters switched to targeting customers with increasingly sophisticated social engineering scams, both to gain credentials and get customer to move the money themselves. In the UK, £455 million of authorized push payments fraud, predominantly social engineering, that may or may not have been refunded by banks was lost in 2019.

Mitigating the threats

The RTR is a significant development for Canada's payment systems, and how swiftly real-time payments take off once this approach is in place may come as a surprise to some. The UK example shows, as does Zelle in the U.S., that there is often a large increase in the use of real-time payments once the capability is live. This is not only in the early stages, but also even in a mature infrastructure, as new use cases come about, along with migration from cash and cheques, and cannibalization of existing batch payments and those of an RTGS.

For example, the faster payments service (UK) saw 81 million more payments in 2019 than 2018, a 32 percent increase, more than 10 years after launch. Payment value also increased to £1.7 trillion from £1.4 trillion. This is in part due to an increase in the scheme limit migrating more corporate payments from slower batch payments (BACS) or more expensive RTGS payments (CHAPS). Q1 2019 is showing similar increases over 2018. This epitomizes the ageold adage, "If you build it, they will come."

Canada may see very fast growth as online and mobile banking usage has increased massively in recent years and EFT usage in Canada is high (65 percent of remote payments volumes1) and ripe for migration to the RTR.

From a fraud point of view, the key impacts of the RTR will be a fast and hard attack by fraudsters via the exploitation of silos between rails and channels; a quick increase in both volume and value following the migration of customers to faster payments which, in turn, will significantly affect alert volumes and false positives and lead to an increase in operations head count and negative customer experiences; and greater interest from the regulator due to the migration to social engineering and authorized fraud.

Devising a strategy

There are several key areas on which Canadian banks must focus to protect their customers and themselves:

1. Banks need to profile all the transactions, both payment and non-monetary along with the extra information that goes with the payment on the ISO message, that may have invoice details.
2. Banks must build out a 24/7 fraud operations area, staffed with the right number of people at the right time. This is especially important since Canada's time zones cover 4.5 hours and different fraud typologies happen at different times of day, e.g. social engineering takes place during the day. To cope with increasing alert volumes, improve efficiency by using 4 intelligent routing, smart automation and visual storytelling.

3. Banks must enrich transaction data with additional information such as device and behavioral biometric data. This can then be utilized by applying advanced analytics to create models to detect both account takeover frauds and social engineering/authorized fraud to protect customers and the bank.
4. Multi-factor authentication (though preferably not SMS as this has lots of issues such as SIM Swap to contend with) built in conjunction with profiling, can bring security with the right amount of friction.
5. Banks must ensure that their system has the performance to cope with higher volumes of payments as real-time payments take off fast.

Moving to real-time payments brings evolving fraud challenges to go along with new business opportunities, payments innovation and improvements in efficiency. However, by making the right investments early on in terms of fraud-focused technology, Canadian banks can make the most of these opportunities, keep losses down and only introduce a modest amount of friction to their customers.

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance.

The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

www.niceactimize.com