Challenges and Opportunities in Fraud and AML

NICE Actimize

With COVID-19 and the recent CARES Act, fraud and AML teams need to quickly address the rapidly evolving financial crime landscape. As financial criminals become savvier, it's critical to adapt quickly and accurately to stay ahead of the perpetrators. To help you navigate these new dynamics, NICE Actimize recently partnered with other leading industry experts on a four-part webinar series. The following blog offers highlights and insights from the "Challenges and Opportunities in Fraud and AML" webinar.

This webinar session featured insights from Aite Group and NICE Actimize.

Customer Habits in Changing Times

In highlighting the macro trends related to the COVID-19 pandemic, the best place to start is the impact that it has already made – and that it will continue to make – on the habits surrounding how consumers and businesses interact. Of course, the trend toward digital was very well established even before the pandemic and the shelter-in-place orders were issued.

For example, prior to the pandemic the adoption of contactless payment methods faced considerable headwinds primarily in the form of ingrained habits among consumers who prefer to swipe their cards. Until recently, many retailers showed little or no interest in deploying contactless payments, but in the wake of COVID-19, they're now accepting contactless payments to help consumers reduce contact with commonly used services such as PIN pads.

Prepayment and curbside pickup services have enjoyed enormous growth during the lock down for reasons equally obvious to those in support of contactless payment adoption. But while it's nice to avoid the crowds at the store, the shift toward no-touch contactless payments is likely to outlast curbside pickup as people emerge from their isolation.

In addition, it's a safe bet that person-to-person money transfer (using apps such as PayPal, Venmo, Zelle, and Dwolla) will also surge during the pandemic, and it's reasonable to expect a substantial increase in both P2P and contactless payments even beyond the pandemic.

How Will This Impact Fraud?

Fraudsters thrive on fear and confusion. When considering how heavily they rely on tactics like social engineering and victim vulnerabilities, fraud attacks tend to increase as economic conditions deteriorate and the perceived threats to individual economic stability also go up. To this end, the pandemic is a particularly potent mix of environmental conditions for a surge in fraudulent activity.

So how will fraudsters exploit these conditions? The proverbial "canary in the coal mine" in terms of the early signs of financial crime resulting from the pandemic is the corresponding increase in phishing activity, reported by researchers and security professionals – and even our own anecdotal evidence – which took almost no time to emerge.

As legitimate businesses quickly began to deploy widescale communications to assure their customers that they are on top of the pandemic and are taking precautions, fraudsters took advantage as this is precisely the kind of activities on which they thrive.

Another recent target for fraud is the IRS stimulus checks going to consumers who've not previously filed tax returns online, but signed up to get their checks via direct deposit. While there are controls in place to verify the authenticity of enrollees, there's enormous potential for abuse by fraudsters.

Addressing Fraud While Working Remote

While the federal government stimulus program is a very high-profile target, it is by no means the only one. In business settings, scams were successful for fraudsters in the old normal even when face-to-face interactions were common. Today, the potential for scams and nefarious activity is exacerbated by the growing prevalence of remote workforces.

While remote workforces certainly can be managed, fraudsters are continuing to exploit these conditions, adding additional pressure for businesses to manage their remote employee bases.

Fortunately, we're seeing a very high degree of resiliency among Financial Services Organizations (FSOs) as they shift workload from the office into their employee's homes. There's been some challenges on that front, particularly for offshore activities, with both infrastructure and policies that make it more complicated to move people to a work-from-home arrangement with access to high-speed internet and computing technology and equipment. One example is FSOs having to ship equipment to employees' homes, which has delayed getting them up to speed. Given the situation, however, the industry overall has done very well with teams interacting effectively and limiting the disruption from having a widely dispersed workforce.

Industry Challenges

We've also talked with some medium and large FSOs about the challenges they're facing. One of the significant shifts in patterns reported among those we interviewed were "increases in enrollment" fraud attempts. Many of the increases were attributed to mule activity and many others are associated with fraudulent loan applications. A variety of challenges make it difficult to effectively and accurately differentiate between those enrollments that are tied to mules and those tied to first-party fraudsters; however, most respondents believed that the bulk of the increases were due to mules.

While many FSOs have proactive mule interdiction programs, most of them are informal and suffer from a lack of resources and formal procedures. Many are missing the kind of sophisticated analytics and monitoring technologies that are required to perform effective detection and interdiction processes in a consistent manner. It's key for FSOs to consistently and effectively interdict new activity and sustain a means of supplementing their existing controls with more robust mule monitoring and detection capabilities. They will be better equipped to proactively mitigate the reputational and market risks of fostering a mule-friendly environment.

Another financial crime trend that executives are seeing is "card-not-present" (CNP) fraud attacks. As the pandemic accelerated the migration of transactional traffic away from brick and mortar toward e-commerce, CNP fraud attack rates rose. Internal fraud became another concern, though it has not yet revealed any specific indications that it is increasing.

In addition to consumer and retail fraud, the Payment Protection Program, which is designed to provide a direct incentive for small businesses (SMBs) to keep their workers on the payroll, certainly provides ample opportunity and vectors for fraudsters. In fact, many would argue that even in the pre-pandemic state, SMB lending was susceptible to fraudulent behavior.

The chaos and confusion created by the pandemic is exacerbating potential vulnerabilities in the SMB segment to be further exploited by fraudsters. Some key reasons include:

- Virulent nature of fraud, which is growing even more severe
- "Bulls-eye" effect of massive financial distributions and opportunity
- Inferior risk- and self-assessment by lenders
- Nascent nature of the deterrent ecosystem, which is not as sophisticated as the retail environment
- Looking to administer SMB loans at a breakneck pace
- Small Business Administration capacity is overloaded

Expediting KYC Processes

While there was already substantial evidence that small business lending fraud was trending upward prior to the pandemic, these unprecedented conditions have the potential to add considerable fuel to the fire.

As a result, know your customer (KYC) processes are a critical part of evaluating customers to complete the necessary due diligence. Regulators are also stressing the importance of keeping the necessary controls, but obviously taking a risk-based approach in light of the current situation.

To help address critical needs of FSOs in operationalizing programs to support the CARES Act, NICE Actimize launched KYC Xpress. The cloud-based solution expedites operations and procedures with advanced automation – eliminating manual and time-consuming tasks and reducing the time to set up KYC processes by more than 80 percent. Learn more about this solution here.

Stay Vigilant

During these times, vigilance from investigative teams and sound human judgement are key.

In addition, AML-related activities and information sharing that your teams did when they were face-to-face in the office, had to continue even when working remotely – and in most cases, this was executed successfully. And while completely remote workforces may not be as prevalent after the pandemic has run its course, they are definitely here to stay.

While most of the adjustments FSOs made during the pandemic journey were heavily accelerated – and some may roll back to previous practices – FSOs must be positioned to adopt some of the new processes and key learnings that they've implemented and discovered along the way, as the new normal continues to evolve.

For more specifics and detailed information, access the full series here.