Quick Q&A

ON REAL-TIME PAYMENTS FRAUD

with Saberi Chattopadhyay, Senior Product Manager, and Alak Das, VP Product, Premier, **at NICE Actimize**

Consumers increasingly enjoy the convenience and spontaneity of peer-to-peer (P2P) transactions between bank accounts. But there's a dark side to the relatively new phenomenon of real-time payments via money-transfer platforms like Zelle and Venmo—bad actors.

These bad actors defrauded nearly 18 million U.S. consumers via P2P payment apps and digital wallets in 2020, according to financial services industry consultant Javelin Strategy & Research. And regulators are taking notice. The Consumer Financial Protection Bureau (CFPB) is considering requiring banks and credit unions to compensate more consumers who've been victimized by cybercriminals, according to published reports.

In the meantime, financial services organizations must redouble their efforts to educate their customers, says Saberi Chattopadhyay from NICE Actimize, a cloud-based financial crime and compliance solutions provider for mid-market, regional, community banks, and credit unions as well as tier one financial institutions.

"Customer education is extremely important," Chattopadhyay says. "Regulations can only do so much. Financial institutions can only do so much. AI and machine learning rules can only do so much. Customers need to be informed of the potential situations they might encounter by knowingly or unknowingly authorizing a link or a transaction."

"Because of the increasing sophistication of fraudsters, traditional rules-based policies to identify any red flags or trigger alerts may not be sufficient."

1 Why are customers more vulnerable to fraud when using Zelle and other RTP platforms?

Saberi: First of all, real-time payments like Zelle and Venmo have become very popular in recent years. They have experienced triple-digit percentage volume gains. Some of it can be attributed to the pandemic as people try to avoid cash and use digital transactions. Touchless payments have now become almost second nature. But these payments are vulnerable to fraud because of the instant, real-time and final, irrevocable nature of these transactions. Real-time payments are different from traditional payments that often allow consumers to recall a payment before it is processed. Too many consumers are not fully aware that real-time payments are instantaneous and more vulnerable to fraud. They tend to authorize payments they are not supposed to.

2 Are real-time payments becoming more of a concern for regulators?

Alak: A lot of smaller transactions that are being dispersed through "questionable" entities have become easier to clear. That movement is becoming a major concern to regulators because financial institutions often cannot stop or investigate some of the payments prior to the initiation of the actual transaction or money flow.

3 How can AI help transform customer data into actionable intelligence?

Saberi: Because of the increasing sophistication of fraudsters, traditional rules-based policies to identify any red flags or trigger alerts may not be sufficient. Financial institutions need to get smarter, better and faster with how they can prevent their customers from falling victims to these various financial crimes. And this is where AI and machine learning come into the picture. AI and machine learning do smart segmentation of the customers of a financial institution, using both structured and unstructured data. This holistic segmentation considers all dimensions of a customer profile and provides next-level insights. Let's say a bank secrecy act (BSA) officer is trying to make strategic decisions. These next-level insights using AI and machine learning will help him or her make certain management or other operational decisions. Rules-based AI and machine learning tackles the advanced fraudulent techniques that bad actors are deploying against customers.

4 Are community banks and credit unions particularly vulnerable to money laundering?

Alak: In most cases, community banks, credit unions and smaller financial institutions lack sufficient resources as well as headcount to safeguard against the improvisational sophistication of various techniques used by fraudsters. Their techniques include phishing, social engineering, malware and hacking. One of the most recent techniques we have seen on the rise is known as smishing. It is where a bad actor sends a compelling and convincing text message to trick the targeted recipient. It's designed to look like a continuation of a conversation that someone had in the past. It tricks you into clicking a link which sends the bad actor your private information or downloads malicious programs. Community banks, credit unions or smaller financial institutions sometimes don't have enough manpower to prevent smishing. But just because an institution is small and under-resourced does not exempt it from the requirements of the Anti-Money Laundering Act (AMLA) of 2020. All financial institutions, regardless of size, must comply with those regulations.

*Content sponsored by NICE Actimize. Saberi Chattopadhyay can be reached at **saberi.chattopadhyay@niceactimize.com**. Alak Das can be reached at **alak.das@niceactimize.com**.*

BAI® POWERING SMART DECISIONS.