Fraud Threats and Impacts … and What to Do about It

From 2016 to 2017, account takeover fraud increased by 120%, topping $5.1 billion, according to Javelin Research.[1] Thanks to data breaches that add to the staggering amount of personally identifiable information (PII) available on the dark web, it's easier than ever for fraudsters to commit account origination and account takeover fraud.

Banks and credit unions are rightfully concerned, with more than half of senior executives saying that preventing or mitigating fraud is somewhat or a much higher priority than other major initiatives. More than half of 506 senior-level executives surveyed from banks, credit unions, and non-bank lenders say their financial institution is more vulnerable to fraud compared to 12 months ago, according to a 2018 research study sponsored by Neustar and conducted by American Banker and SourceMedia Research.

Investigating and resolving fraud is expensive and time-consuming. Nine in 10 survey respondents say it takes at least one day — and often many days — to investigate a fraud incident. Less than a quarter (23%) report they are able to resolve a fraud incident in less than one day.

Fraud is everyone's problem. While risk management is an obvious stakeholder in fraud prevention and detection, executives in areas including compliance, operations, IT, audit and management have reported being involved in their institution's fraud reduction initiatives.

[1] https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin

Fraud Happens Everywhere

Banks and credit unions have ramped up security in online and mobile channels but often leave the phone channel vulnerable. When asked what the highest threat entry points are for account origination and account takeover fraud, survey respondents list online and mobile.

However, any entry point — including the branch — is vulnerable to fraud. Fraud often originates in one channel and is carried out in another. For example, fraudsters use social engineering to trick call center representatives into divulging account information they then use to open accounts online.

Something You Know and Have — Might Be in the Wrong Hands

The good news is that most banks and credit unions understand that a single tool for fraud detection and mitigation is not 100% effective, so they're relying on a variety of tools. The most prevalent identity solution is multifactor authentication, used by 62% of survey respondents. Also widely used is internal data, with 42% of respondents seeking to verify that the phone number the customer is calling from matches the number in the bank or credit union's customer relationship management (CRM) system. And even though many customers loathe answering knowledge-based authentication (KBA) questions, 41% of banks and credit unions continue to rely on KBA.

Multifactor authentication that combines something the customer knows with something the customer has — typically an SMS text sent to the mobile phone – is widely used but is problematic. Fraudsters might have access to the customer's PII and they can easily spoof a phone.

Banks and credit unions are rightfully worried, with more than two-thirds of survey respondents saying they are somewhat or very concerned about fraud from spoofing.

In one fraud scheme, fraudsters call customers with a spoofed 800 number from a legitimate financial institution, claiming there is suspicious activity on the account. The customer checks the 800 number online, verifies it's the correct number for the financial institution, and divulges their user ID and password.

With just a few credentials, fraudsters can also hijack a customer's phone using SIM swap, call forwarding and porting. Fraudsters use these tactics for both inbound and outbound calls. They will call the bank or credit union pretending to be the customer or they will pretend to be the customer if the bank or credit union either calls or sends a one-time passcode (OTP) via SMS text to verify a transaction.

It's Only a Few Bad Apples

One way to tackle fraud is to make every customer jump through extra hoops to prove they are who they say they are. But since the vast majority of customers are legitimate, adding more processes and authentication methods can make good customers feel like they are being treated as criminals. Not exactly a recipe for a great customer experience. Banks and credit unions recognize the challenge, with 22% of banks and 32% of credit unions saying that reducing friction is a very high priority.

Some data — like the ANI — is easy for fraudsters to replicate or steal. But there are "unstealable" device behaviors that fraudsters can't access. Phone type is an example: a phone is either a mobile device, or a VoIP phone. Activity is another: either the phone has been used or it hasn't. A fraudster can't purchase a new TracPhone and then fake the phone having been activated 18 months ago.

The mobile network operator (MNO) tracks whether a phone has been SIM-swapped or if call forwarding has been turned on, offering yet another way to determine the risk of a device.

A Layered Approach to Fraud

Banks and credit unions can't rely on only a few pieces of data to identify fraudsters. A transaction from a prepaid phone doesn't necessarily indicate fraud. But combining phone type with activity — a prepaid phone used for 12 months is less risky than a brand new prepaid phone — and whether the device is linked to an email account that can be authoritatively linked to an identity, dramatically increases confidence that it's a legitimate customer.

Layer that device intelligence with online and offline data such as IP address, cookies and social security number, and banks and credit unions can identify good customers and stop fraudsters.

The data must come from authoritative sources. For example, an email address linked to several legitimate subscriptions or accounts is much more authoritative than a recently created email account. Tracking pixels on account opening forms can help identify an applicant's device using browser, cookies and IP addresses.

Fraudsters can easily call into the call center with a spoofed phone number, and using social engineering, pretend that they are the consumer.

Where to Get Device Data Fraudsters Can't

With more than 90% of caller ID data and updated device data on more than 500 million phones through relationships with MNOs, Neustar is able to gather a wide variety of device data. This includes if a SIM card is still tied to a customer's phone, if a phone number has been forwarded, or if phone porting has occurred.

As banks and credit unions put fraud barriers in place, fraudsters work hard to navigate around them. Banks and credit unions must close the gaps created when fraudsters figure out how to defeat anti-fraud technologies. Combining online and offline data with "unstealable" device data elements allows banks and credit unions to confidently let the good customers in and keep the fraudsters out.

Account takeover fraud is lucrative for criminals, so it won't be going away anytime in the near future. If anything, expect the incidence of this damaging type of fraud to increase.

LEARN MORE

Neustar's authoritative consumer identity intelligence enables financial institutions to reduce compliance risk, improve customer experience and increase revenue across the enterprise.

For more information, contact us at **1-855-898-0036** or email **risk@team.neustar**.

SS-FRC-149035-10.23.2018