

SEPTEMBER 2020

**FEATURE STORY** – PAGE 8

How Axis Bank prevents identity fraud with video-based onboarding

**NEWS & TRENDS** – PAGE 12

5.3 million stolen passwords discovered circulating on dark web marketplaces

**DEEP DIVE** – PAGE 18

How biometrics and AI can curb identity fraud

# PREVENTING FINANCIAL CRIMES

PLAYBOOK

PYMNTS.com

**NICE**·ACTIMIZE



# PREVENTING FINANCIAL CRIMES

PLAYBOOK

## WHAT'S INSIDE

4

A look at recent financial crime developments, including the 184,000 instances of COVID-19-related fraud as of August

## FEATURE STORY

8

An interview with Sameer Shetty, head of digital banking at Axis Bank, on how AI and video onboarding can significantly drive down the rate of identity fraud incidents

## NEWS & TRENDS

12

The latest worldwide financial crime headlines, including details about 5.3 million stolen passwords for sale on dark web marketplaces and 24,182 identity theft complaints so far this year

## DEEP DIVE

18

An in-depth examination of how fraudsters leverage identity fraud to scam banks and their customers as well as an analysis of the technologies being deployed to stop them

## ABOUT

22

Information on PYMNTS.com and NICE Actimize

## ACKNOWLEDGMENT

The Preventing Financial Crimes Playbook is done in collaboration with NICE Actimize, and PYMNTS is grateful for the company's support and insight. [PYMNTS.com](https://pymnts.com) retains full editorial control over the following findings, methodology and data analysis.



**WHAT'S  
INSIDE**

**FINANCIAL CRIME**  
is an unending menace  
for businesses, financial  
institutions (FIs) and  
organizations the world over.

A recent [survey](#) found that 47 percent of companies experienced fraud at least once in the past two years, and a total of \$42 billion was stolen during that period. External cybercriminals and internal perpetrators evenly split the instances of fraud, and 13 percent of organizations that faced fraud said it cost them more than \$50 million.



The ongoing COVID-19 pandemic has exacerbated this problem, with fraudsters exploiting the economic hardships and uncertainty faced by individuals around the world to conduct their schemes. The Federal Trade Commission (FTC) [found](#) 184,000 instances of pandemic-related fraud had occurred in the United States since the end of August, resulting in the theft of more than \$124 million. Fraudsters perpetrating such schemes often target individuals by phone, posing as bank officials, Internal Revenue Service (IRS) agents or public health administrators and asking for personal information or money in exchange for COVID-19 test kits, stimulus checks or work-from-home jobs. This fraud targets all demographics and generations, with U.S. consumers ages 30 to 39 reporting the most incidents but Americans aged 50 to 59 reporting the greatest losses.

These scams may have taken on a new flavor during the pandemic, but they are far from new. Identity fraud has been a constant danger since the invention of banks, with fraudsters posing as other individuals to access their accounts or applying for loans they have no intention of paying back. Such schemes have also taken on new forms in the digital age, with some fraudsters buying stolen identities en masse from dark web marketplaces and others cobbling together pilfered information to forge fictitious identities and conduct synthetic identity fraud.

These financial crime methods are difficult to thwart, but numerous technological innovations can help FIs turn the tide, including biometrics to verify customers at digital entry points and artificial intelligence (AI) to spot suspicious transactions. Identity fraud may never be permanently stopped, but thwarting more attempts could save banks and their customers millions.

## FINANCIAL CRIME DEVELOPMENTS AROUND THE WORLD

Seniors are especially vulnerable to identity theft and fraud, as they are often not as digitally savvy nor as versed in online security best practices as their younger counterparts. A recent [study](#) determined that identity theft against those ages 61 or older rose by 22 percent in 2019, a greater rise than the 18 percent overall increase in such theft that year. There were 223,163 cases of identity fraud across all generations in 2019, with bank and credit card fraud accounting for 42 percent of identity theft cases.

The pandemic is prompting fraudsters to exploit the economic insecurity gripping much of the world. The Financial Crimes Enforcement Network (FinCEN) recently [issued](#) a warning that fraudsters are leveraging various illicit methods, including malware, phishing schemes, extortion and business email compromise (BEC) scams, all with a COVID-19 twist. Some are posing as government officials and asking for personal information for stimulus checks, for example, while others are targeting cryptocurrencies.

Banks are working to curb such fraud by making sizable investments in their security efforts. British FIs, for example, spend [upward](#) of £6.7 billion (\$8.6 billion USD) annually on cybercrime prevention efforts, with much of these funds devoted to cloud-based systems that harness data analytics. They are also leveraging cloud systems to keep up with rules meant to fight organized crime rings, with Thomson Reuters reporting that 2019 saw more than 80,000 regulatory updates around the world.

For more on these stories and other financial crime prevention developments, read the Playbook's News and Trends section (p. 12).

# Executive Insight

***A recent study found that there are more than 5.3 million stolen passwords circulating on dark web marketplaces. What should FIs do to secure their platforms and protect their customers in the wake of harmful data breaches that expose these passwords?***

NICE Actimize continues to see a rise in fraud schemes linked to data breaches. The types of compromised data range from partial information, such as names and birth dates, to wider sets of personally identifiable information, including passwords. This exposed [personally identifiable information] enables fraudsters to impersonate legitimate customers, take over accounts and cause an uptick in synthetic identity fraud.

[Financial services organizations] may need to rely on other data to identify their customers. The first step to detecting ATOs begins at the point of login. A strong, risk-based authentication engine assesses the risk of login and authentication for every monetary and non-monetary transaction, applying stronger authentication for riskier users. This risk-based approach is key to detecting and stopping ATO attacks as well as preventing fraudsters from altering accounts to extend takeover while providing good [customer experiences] for [genuine] clients.

[Financial services organizations] can profile customers in real time using historic transactions, geolocation, device, IP history, behavioral biometrics, authentication patterns and more to avoid relying on [personally identifiable information]. Fraudsters may use stolen data to take over accounts, but they can't successfully mimic customer behavior in a sustained way. Using machine learning and AI, a real-time detection engine will spot behavior anomalies – [enabling financial services organizations] to stop attacks.

**YUVAL MARCO**  
general manager of fraud  
and authentication at [NICE Actimize](#)



### **HOW VIDEO ONBOARDING AND AI FORM A MULTILAYERED IDENTITY FRAUD PREVENTION SYSTEM**

Identity fraud is a constant threat to FIs, especially as the ongoing COVID-19 pandemic brings an unprecedented wave of first-time digital banking users. Identity fraudsters are exploiting this surge to sneak into users' bank accounts, but a combination of video onboarding and AI could be enough to counter their schemes. In this month's Feature Story (p. 8), PYMNTS talked with Sameer Shetty, head of digital banking at Mumbai-based [Axis Bank](#), about how these two technologies combined form a multilayered fraud defense system that can make identity fraud nearly nonexistent.

### **DEEP DIVE: HOW IDENTITY FRAUD THREATENS BANKS**

One of the most well-known fraud methods is identity theft, in which bad actors steal victims' personal information and apply for loans or open accounts in their names. Some fraudsters leverage synthetic identity fraud to the same end, using pieces of data from different consumers to create new identities rather than pilfering or purchasing them wholesale. This month's Deep Dive (p. 18) explores how both of these methods target banks and their customers as well as how technologies like AI and biometrics can counter them.

# 15%

Maximum potential share of total annual lender losses due to synthetic identity fraud



## FIVE FAST FACTS

# 24,182

Number of identity thefts reported to the FTC through early August



# 22%

Increase in identity thefts targeting seniors between 2018 and 2019



# £6.7B

Amount U.K. banks spend annually on cybersecurity measures



# \$16.9B

Total losses due to identity theft in 2019





# FEATURE STORY

e="log"

d" id="log"  
1">

put">

sword" name="pwd"

"2"></td></p>

Submit">

ton">



# How Axis Bank Prevents Identity Fraud With Video-Based Onboarding

**The ongoing COVID-19 pandemic and its associated social distancing and stay-at-home orders have pushed untold services online for easier consumer access, with banking serving as a prime example.**

PYMNTS' recent [Leveraging The Digital Banking Shift Report](#) found that 46 percent of bank customers have used digital banking services more often now than they did before the pandemic began, with 74 percent of recent online users planning to stick with these services once the pandemic has ended.

This surge in digital activity opens vast new opportunities for fraudsters, however. Without in-person interactions with bank staff, account takeovers (ATOs) and

customer impersonations are much easier for fraudsters to accomplish. One of the key ways in which banks can counter this threat is through ironclad authentication processes, according to Sameer Shetty, head of digital banking at the Mumbai, India-based [Axis Bank](#).

"The major cybersecurity issues that will continue to increase as digital becomes more prominent is fraudsters managing to get control of customers' accounts," he said. "We'll see more and more [of this] action as digital [banking] progresses."

Shetty recently offered PYMNTS insights into the financial crime threats that banks like Axis face on a regular basis and how video authentication and AI can significantly reduce the scope of these hazards.

## **FRAUD THREATS TO DIGITAL BANKING**

ATOs are among the biggest threats that digital banking regularly confronts, according to Shetty. These attacks involve hackers gaining access to bank customers' accounts and doing as they please with them, whether transferring funds to hackers' own accounts or pilfering personal data like passwords or Social Security numbers.

"[ATOs mostly] happen through social engineering," he said. "[Fraudsters] will call up customers pretending to be bank employees and ask the customers to share their passwords, debit card details, PINs, et cetera. And then they'll take that [information] and use the accounts."

Another threat is identity fraud, in which bad actors will either steal an individual's identity or forge a new one, and then use it to open new accounts or apply for fraudulent loans they have no intention of paying back. Identity fraud [accounted](#) for \$16.9 billion in losses in 2019, according to a recent study, although it has declined from \$20 billion in 2013.

A major factor in this decline has been the rise of improved authentication and security systems at banks like Axis. Shetty even

stated that Axis has had no digital banking identity fraud incidents, thanks to a multilayered defense system that incorporates video customer authentication and AI.

### **LEVERAGING VIDEO-BASED ONBOARDING, AI TO PREVENT IDENTITY FRAUD**

One of the most important steps in preventing ATOs and identity fraud, according to Shetty, is an ironclad authentication process at the point of entry. Axis Bank harnesses a video-based account opening system that allows customers to open their accounts without visiting a bank branch, a feature that has come in handy, especially as the COVID-19 pandemic makes such visits risky.

"Last quarter, more than 75 percent of our deposits were conducted fully digitally as well as 40 [percent] to 50 percent of our loans and credit cards," said Shetty.

Axis' onboarding system cross-references customers' identifying information with India's national identification number system, the world's largest biometric identity program. Axis verifies that the numbers customers present are the same as what they have in the national database to confirm their identities.

"It's like the Social Security number in the U.S.," Shetty explained. "Customers provide their national identity number and their tax number as well, and then there is a video call. That process takes between seven and 10 minutes, and at the end of this process, they are onboarded onto the bank, and then can open a savings account."

This system is augmented with a facial recognition system that compares the applicant's face with the one on file on government servers. Any mismatch between





the number and the biometric system is a surefire indicator of identity fraud.

“When you’re doing your onboarding, an AI algorithm [conducts] a face match between your real-life face and the picture that has come from the central authority,” Shetty said. “It’s very difficult to do an impersonation unless you can find a way to kind of change the photograph in the central database itself.”

This instant verification system has made synthetic identity fraud nearly impossible as the instant cross-referencing with government databases means that any made-up identification number will be discovered immediately.

This does not mean that just one layer of security is sufficient for fraud prevention,

however. The onboarding system is supplemented by an AI platform that looks for signs of account takeovers, like mismatched location data or unusual transactions.

“Say you are a customer of ours, and you’ve been doing transactions [that] are less than a hundred dollars,” Shetty said. “Suddenly one day you do a transaction worth \$5,000. That transaction will likely get screened by the system, and then somebody will call you to check if ... you have done this.”

Either of these systems individually could have weak points, as fraudsters are constantly innovating and looking for new ways to circumvent crime prevention measures. Banks that deploy multilayered systems in tandem, however, can present such a hard target that fraudsters could steer clear in favor of easier prey altogether.

The background features a complex network of grey lines and black nodes, resembling a molecular or data structure, set against a light grey gradient. A prominent blue banner with a black border is positioned diagonally across the center. The text 'NEWS & TRENDS' is written in white, bold, sans-serif capital letters within this banner.

**NEWS &  
TRENDS**

## Fraudsters step up their game

### 5.3 MILLION PASSWORDS DISCOVERED ON DARK WEB MARKETPLACES

Some fraudsters harvest personal data, while others purchase such information in bulk on dark web marketplaces. British credit marketplace provider ClearScore recently [discovered](#) more than 5.3 million stolen passwords for sale circulating in said marketplaces over the past three months. Passwords for social media services like TikTok were available for as little as £3 (\$4 USD) each, but those for mortgage or banking websites went for up to £280 (\$372.91 USD) apiece.

These passwords had been taken from consumers across the United Kingdom, but ClearScore's study found that the distribution of these thefts has been unequal. Individuals in Birmingham were the most affected, as the average consumer there had nine pieces of data stolen. Liverpoolians had five taken on average.

### SYNTHETIC IDENTITY FRAUD ACCOUNTS FOR UP TO 15 PERCENT OF BANK LOSSES PER YEAR, STUDY FINDS

Some fraudsters eschew stealing or purchasing complete identities in favor of inventing novel ones out of individual details. This practice, synthetic identity fraud, has become much more popular recently, with a recent [study](#) finding that it is responsible for up to 15 percent of U.S. lender losses annually. India also has a significant synthetic identity problem, as the scheme accounts for

18 percent of all detected fraud instances and up to 12 percent of Icredit card fraud losses.

Detecting synthetic identity fraud is notoriously difficult, as victims are unlikely to realize that specific details have been stolen and tip off banks that fraud has occurred. Many FIs either intentionally or unwittingly underreport synthetic identity theft losses by filing them as bad debts, but some banks are turning to data mining and analytics to find small inconsistencies that highlight telltale signs of the malicious activity.



### **IDENTITY THEFT REPORTS SOAR IN 2020, FTC REVEALS**

The global pandemic is prompting continued social distancing and stay-at-home orders as well as a deep recession, and banks are unfortunately also coping with an increase in fraud attempts. The FTC has [reported](#) 24,182 identity theft complaints this year as of Aug. 6, for example. The monthly number of thefts peaked in May at 7,800 and has since declined, but more than 4,800 instances still occurred in July.

Many complaints are related to the stimulus checks the IRS has sent out this year, with scammers posing as victims' banks or the IRS itself and asking for their personal data to process said checks. The thieves then use the stolen information to access victims' bank accounts or sell it to other cybercriminals on the dark web.

### **STUDY SHOWS THAT SENIORS FACED 22 PERCENT INCREASE IN IDENTITY THEFT IN 2019**

Identity theft rates may be setting records this year, but the phenomenon is far from new. A recent examination of the Cifas National Fraud Database [found](#) that identity theft rose 18 percent overall in 2019 from the previous year, while consumers ages 61 and older faced an increase of 22 percent. This age group also experienced the highest rate of card theft, and these trends could be attributed to a less thorough understanding of best security practices than younger generations. Older individuals also typically have better credit scores, making them more desirable targets for fraudsters looking to take out loans in their names.



Identity theft rose  
**18 percent overall**  
in 2019 from the  
previous year.

There were 223,163 identity fraud cases across all generations last year, an increase of 32 percent over the previous five years. Bank and credit cards accounted for 42 percent of all cases, followed by bank account theft at 22 percent and fraudulent loans at 10 percent.

### **FINCEN WARNS AGAINST PANDEMIC-RELATED SCAMS**

The ongoing COVID-19 pandemic has dramatically boosted digital banking usage, but this shift is also opening the door for fraud. FinCEN recently [warned](#) that fraudsters are leveraging pandemic-related uncertainty to deploy various schemes, including malware, phishing, extortion and BEC scams. Many of these schemes target cryptocurrencies, according to FinCEN, with fraudsters posing as teleworking companies and fake mobile apps to bilk consumers of their digital funds.

FinCEN told banks and customers to watch out for signs that any given digital interaction with a stranger could be fraudulent. Blurry pictures, mismatched identity information and the refusal to provide alternative forms of identification, for example, could indicate that a supposed customer is a fraudster.

## FIs improve their fraud-fighting mechanisms

### UK BANKS SPENDING £6.7 BILLION ANNUALLY TO FIGHT CYBERCRIME

Banks are devoting vast sums to defeating identity theft and other financial crimes, with a [study](#) from the U.K.'s Financial Conduct Authority (FCA) finding that British FIs spend upward of £6.7 billion (\$8.6 billion USD) annually on cybercrime prevention. Much of the funding is being devoted to cloud-based systems that harness data analytics, allowing banks to monitor transactions for fraud, review suspicious activity and apply extra screening procedures when deemed necessary. These systems are especially useful as the country enters into another economic recession due to the pandemic — bank revenues are expected to decline and force back-end operations to gain efficiency.

Banks are also deploying cloud technology to meet regulatory requirements meant to fight organized financial crime, with Thomson Reuters reporting that 2019 alone saw more than 80,000 regulatory updates around the world. Banks must stay on top of these crime-fighting regulations, as FIs could face hefty fines in addition to increased cyber risks if they let their crime prevention measures come up short.



### BBVA TRAINS STAFF IN CYBERCRIME PREVENTION TACTICS

Advanced technology is critical to financial crime prevention, but educating customers and staff on fraud prevention best practices is just as important. Financial institution BBVA recently [began](#) a focused training effort to this end, training approximately 2,000 staff members in financial crime prevention techniques that included insight into how hackers operate, tools to optimize security software and drills on conducting business during a cyberattack. BBVA partnered with Amazon Web Services for one lesson that included a set of 200 virtual security challenges.

The cybersecurity seminar was also made available to the public with the intention of educating other banks and individuals on proper cybersecurity protocols. BBVA estimates that up to 14,230 individuals participated in workshops and discussion groups as part of the program.

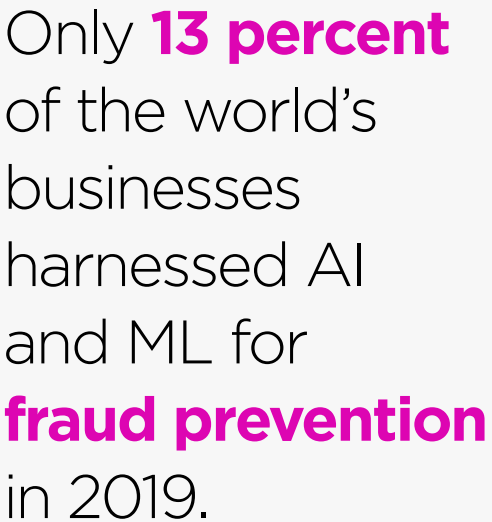
**CUSTOMERS PREFER SLOWER BUT MORE SECURE ACCOUNT SIGN-UP PROCESSES, STUDY FINDS**

Banks face a constant struggle in balancing security and convenience, as potential customers are prone to abandoning sign-ups if they find them too friction-laden. A recent [study](#) found that consumers are willing to undergo slower account creation processes if they are assured of their security, however, with 62 percent of consumers reporting a preference for security over speed. This trend held true across various age groups, genders and industries.

Banks should not swing the pendulum too far toward security, however, as these same customers expressed frustration with poor account opening experiences. Seventy-three percent of consumers said they have grown more intolerant of subpar account opening procedures over time, for example, meaning banks must still walk a fine line between security and convenience.

**ASIA-PACIFIC BANKS STEP UP THEIR USE OF AI FOR FINANCIAL CRIME PREVENTION**

One crucial tool in the fight against financial fraud is AI, which can analyze thousands of transactions in the time it takes a human analyst to assess only a handful. FIs across the Asia-Pacific (APAC) region are leveraging AI for fraud prevention, with governments and FinTechs across the region [promoting](#) its use. Increases in fraud instances are driving this trend, with four out of five APAC banks experiencing rises in fraud losses over the past year and 22 percent predicting that fraud will increase considerably over the next 12 months.



Only **13 percent** of the world's businesses harnessed AI and ML for **fraud prevention** in 2019.

Only 13 percent of the world's businesses harnessed AI and machine learning (ML) for fraud prevention in 2019, according to a recent survey, although one-quarter were planning to adopt such technologies within the next two or three years. Even organizations that are not using AI specifically are stepping up their fraud prevention efforts, with 55 percent of surveyed businesses planning to boost their cybersecurity budgets over the next two years.



## New financial crime-fighting tools and partnerships

### **NICE ACTIMIZE LAUNCHES AI-DRIVEN FRAUD PREVENTION PLATFORM**

Fraud-fighting technology grows more advanced by the day, with tools like AI and ML set to revolutionize how financial crime is detected and stopped. Financial crime solutions provider NICE Actimize recently [unveiled](#) a tool that leverages AI, behavioral analytics and data intelligence to modernize banks' risk management profiles, for example. The platform, Xceed, is deployed on the cloud and geared toward small and mid-sized organizations for which an in-house fraud prevention solution is financially infeasible.

The Xceed platform joins X-Sight, NICE Actimize's financial crime risk management solution, as part of the company's fraud-fighting portfolio. NICE solutions are currently used at more than 25,000 organizations in 150 countries, including 85 of the Fortune 100 companies.

### **CANADIAN BANKS FORM DATA-SHARING ALLIANCE TO FIGHT CYBERCRIME**

Cooperation is also a key fraud-fighting technique, and 31 Canadian banks recently announced the [launch](#) of the Financial Data Exchange (FDX) Canada network. The alliance includes Canada's "Big Five" banks – BMO Bank of Montreal, Canadian Imperial Bank of Commerce, National Bank, Royal Bank of Canada (RBC) and the TD Bank Group – as well as a number of other FIs including Desjardins, Interac and Simplii Financial.

The group plans to share its data via the FDX application programming interface (API), which has already been used by more than 100 firms and 12 million customers in the United States. RBC and Interac plan to serve as FDX Canada's representatives in the greater FDX leadership team, which also includes Bank of America, Charles Schwab and Wells Fargo.





# DEEP DIVE

# How Identity Fraud Targets Banks

**Fraudsters leverage an array of schemes to conduct financial crimes, including digital methods like botnets and brute force hacks as well as old-school approaches like social engineering. One of the most pervasive — affecting customers as much as or more than banks — is identity theft. This tactic can do more than compromise customers' bank accounts: It can also cost them untold hours by forcing them to meticulously change their account passwords and contact customer service departments to have fraudulent charges revoked.**

The damage done to banks as well as the customers they serve has forced FIs and security companies to make curbing identity theft a top priority. Identity theft methods are as numerous as they are diverse, however, ranging from trial-and-error password checks that fraudsters use to test stolen identities purchased in bulk to opening accounts or applying for loans with fictitious identities. The following Deep Dive explores the myriad identity fraud schemes that bad actors harness as well as the technologies that banks are leveraging to keep them at bay.

## **METHODS OF IDENTITY THEFT**

Identity theft is well-known to Americans, who have been educated their entire lives to keep their personal data secure so strangers cannot impersonate them. Data shows that U.S. consumers [made](#) approximately 651,000 identity theft complaints in 2019, including instances of credit card fraud, mobile phone account fraud, impersonations for personal loans and a host of other scams. The rate of identity theft fell by 24 percent from 2015 to 2017 but skyrocketed 46 percent from 2018 and 2019. Fraudsters used these stolen credentials to [pilfer](#) \$16.9 billion last year, up 15 percent from 2018 totals.

Consumers often think of identity theft as involving fraudsters hacking directly into customers' accounts, but most bad actors do not acquire stolen identities themselves. They instead buy them in bulk from dark web marketplaces, where stolen credentials can be sold for as little as \$15 apiece. A recent [study](#) found that there are more than 15 billion such credentials available on the dark web and that 5 billion have never been used and are considered much more valuable. Unique bank credentials, for example, can be sold for as much as \$500 each.

The identities circulating among these dark web marketplaces are often acquired from large-scale data breaches, which can leak hundreds of millions of credentials. Many individuals use the same username and password combinations for multiple accounts, meaning their bank accounts could be put at risk due to breaches at completely unrelated companies.

## SYNTHETIC IDENTITY FRAUD

Some identity fraudsters utilize fabricated synthetic identities instead of leveraging customers' credentials wholesale to open accounts or pose as them. These synthetic identities often incorporate disparate elements of real identities to look more realistic, such as using a valid Social Security number and address but repurposing details from different victims. Banks hit by synthetic identity application fraud often have no victims to notify them that fraudulent applications were made in their names, making this fraud type difficult to notice until it is too late.

One 2016 [study](#) found that identity theft resulted in up to 20 percent of all credit losses, for a total of \$6 billion. The Federal Reserve has also [pinpointed](#) synthetic identity fraud as the fastest-growing financial crime, with industry watchdogs estimating that it costs banks and other FIs \$6 billion



annually. Boston-based Aite Group asserts that each instance of synthetic identity fraud costs lenders between \$10,000 and \$15,000, and Brian Vitale, Notre Dame Federal Credit Union's chief risk and compliance officer, said it cost the credit union roughly \$200,000.

Banks and other FIs are deploying numerous tools to keep identity fraud at bay, but individual users can also employ proper password hygiene to take their security into their own hands.

### IDENTITY THEFT PREVENTION METHODS

One of the most promising technologies in the identity fraud fight is AI, which can be [taught](#) to look for minor inconsistencies in customer identities to see if they are stolen or fraudulent. AI-based systems can even scan physical identity documents like driver's licenses or Social Security cards to ensure their authenticity faster and much more accurately than human analysts can. Biometric tools — especially those with liveness detection, which cannot be fooled by a static picture — can also hinder identity fraudsters.

Many of these identity theft prevention methods have seen success. Synthetic fraud, for example, [rose](#) only from \$1.01 billion in Q2 2018 to \$1.02 billion in Q2 2019. This is its slowest growth in years and marks a sharp contrast from Q2 2016, when it skyrocketed to \$854.4 million from \$524.5 million in Q2 2015 — a 62.9 percent jump. The decline in growth is largely attributed to the rising prevalence of identity databases, which track whether identities have previously been used to commit fraud.



Bank customers can also take the initiative to protect their identities from theft. Many leaked credentials are used for services from which they did not originate, meaning that utilizing different passwords for different accounts can limit the damage done if an individual's password is breached. Two-factor authentication is also effective because fraudsters cannot access customer accounts with stolen passwords alone.

Curbing identity fraud's rise will require the marriage of advanced technologies with due diligence from customers. It may never be stopped entirely, but even stalling it could save millions of dollars and untold hours.

# ABOUT

## **PYMNTS.com**

PYMNTS.com is where the best minds and the best content meet on the web to learn about “What’s Next” in payments and commerce. Our interactive platform is reinventing the way companies in payments share relevant information about the initiatives that make news and shape the future of this dynamic sector. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovations at the cutting edge of this new world.



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 consumer and investor 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.

Copyright © 2020 Actimize Ltd. All rights reserved. No legal or accounting advice is provided hereunder and any discussion of regulatory compliance is purely illustrative. Stay current with NICE Actimize webinars at [actimize.nice.com/events](https://actimize.nice.com/events).

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe to this report, please email us at [feedback@pymnts.com](mailto:feedback@pymnts.com).

# PREVENTING FINANCIAL CRIMES PLAYBOOK

## DISCLAIMER

The Preventing Financial Crimes Playbook may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATION'S ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.

Components of the content original to and the compilation produced by PYMNTS.COM is the property of PYMNTS.COM and cannot be reproduced without its prior written permission.