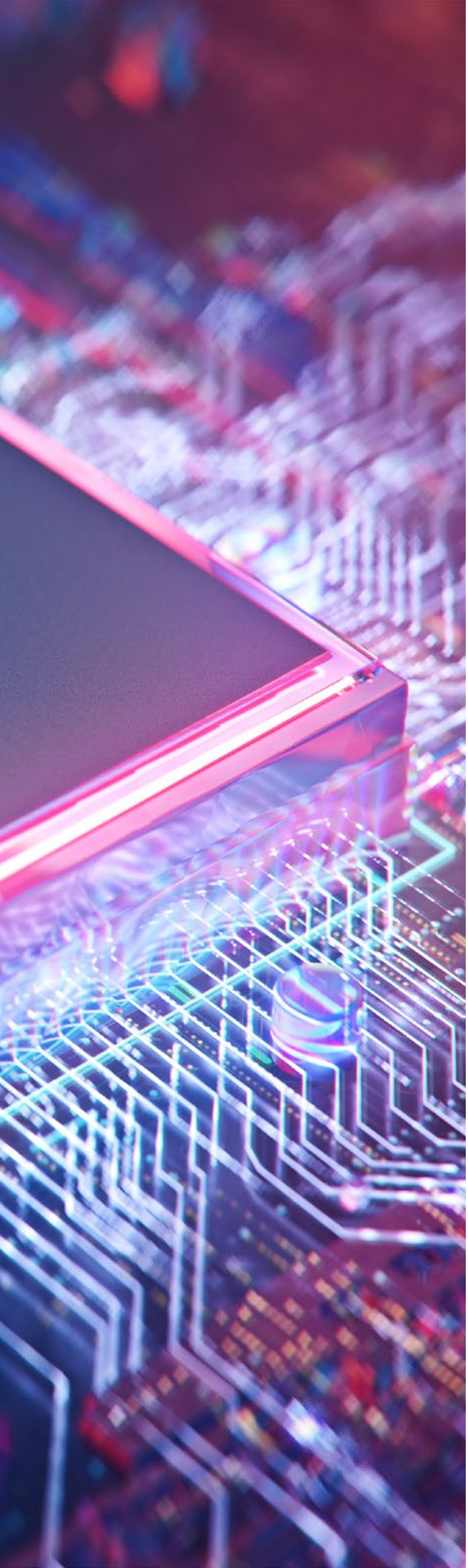
AUGUST 2020



# PREVENTING FINANCIAL CRIMES PLAYBOOK

PYMNTS.com | NICE · ACTIMIZE



PYMNTS.com | NICE · ACTIMIZE

# PREVENTING FINANCIAL CRIMES PLAYBOOK




**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 retains full editorial control over the following findings, methodology and data analysis.

# WHAT'S INSIDE

**Fighting financial crime is a never-ending battle for banks, credit unions and other financial institutions (FIs).**

They collectively stop upwards of $22.3 billion in fraud attempts in a given year, but the struggle to prevent fraud may at some points feel quixotic, as attempt volumes continue to grow no matter what FIs do to curb it. Sixty-one percent of banks report that the volume of fraud is increasing over time, 59 percent report that the total value of fraud attempts is increasing and 41 percent say that the average value of any given fraud attempt is on the rise.

Fraudsters deploy a diverse array of methods to stage their crimes, including identity theft, account takeovers (ATOs) and brute-force attacks. Fraud affected 1.7 million Americans in 2019, according to the Federal Trade Commission, with 23 percent of victims losing a total of $1.9 billion. These losses mark an increase of $293 million from 2018, indicating that not only are fraudsters improving their techniques and expanding their range of schemes but that cybersecurity efforts on the part of banks and consumers have not stemmed the tide.

Part of the difficulty in combating fraud is that fraudsters now have more resources than ever with which to conduct their attacks, thanks to massive data breaches that have spilled untold terabytes of customers' personal data — including usernames, passwords, account numbers and payment card information — onto dark web marketplaces for bad actors to leverage. Marriott International's data breach in December 2018 leaked 500 million customer records, whereas Facebook inadvertently exposed 50 million accounts and Equifax exposed 148 million consumers' records.

FIs are turning to advanced technology to arm themselves against fraudsters' seemingly endless supply of stolen data. Some of the most promising solutions come in the form of artificial intelligence (AI) and machine learning (ML), which can analyze thousands of ongoing transactions and applications every second and pinpoint telltale signs of fraud, like uncharacteristically large transactions or login attempts from multiple devices in different regions. Banks have reported increased fraud detection rates of up to 50 percent through the use of these technologies, but the tools are still used by only a minority of FIs around the world.

AI and ML developers will have to look at how these technologies can be made more accessible if they want more banks to protect themselves against financial crime. The number of avenues that fraudsters leverage to conduct their schemes are only growing, and the sum of fraud-fighting technologies need to expand as well if banks are to have any hope of defeating their hacker foes.

## FINANCIAL CRIME DEVELOPMENTS AROUND THE WORLD

Banks are working to improve their financial crime prevention efforts, but their customers can help by increasing their awareness of common fraud techniques. A recent study of

2,000 bank customers found that four in five individuals could not consistently differentiate real messages from their banks versus fake ones from fraudsters, leaving them vulnerable to phishing or other methods. The phony messages included trademark signs of deception that bank customers should recognize, including spelling mistakes and requests for personal information that a legitimate FI would never ask for.

Other fraudsters avoid direct interaction with their victims in favor of purchasing stolen credentials from other fraudsters online. A recent study from security firm Digital Shadows found that there are more than 15 billion such user credentials circulating on the dark web — an increase of 300 percent since 2018 — and that 5 billion are unique. These credentials consist of bank account numbers, username-password combinations and other valuable information that could be exploited for financial crimes.

These leaked credentials are primarily used for identity theft, which a recent study found increased by 15 percent between 2018 and 2019. Losses caused by identity theft totaled $16.9 billion after reaching a five-year low in 2018, with this increase attributed to a rise in ATOs. Just 12 percent of financial fraud was the result of ATOs in 2015, but ATOs accounted for 53 percent in 2019.

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

# Executive Insight

***Passwords are a particularly weak security measure, with one out ofevery 142 users choosing "123456" as their password. What kinds of security measures can FIs deploy to secure their customers' accounts from fraudsters?***

"We are starting to see the need for fusion between 'cyber' and 'fraud.' By bringing elements of each discipline together as part of a holistic response tocustomer security and fraud prevention, we can see important improvementsin detection and prevention.

This work needs to start with password policies and user education. [As] an organization, ensure you have sensible password strategies in place to 'hygiene' out the most common passwords (e.g., '123456').

Next, integrate your authentication and fraud profiling together, scoring enrollments and logins as well as payments. By feeding in all the relevant events, normal customer patterns and profiles can be built. This allows for more friction weighted to the risk of the event at hand, and MFA [(multifactorauthentication)] can be directly linked to the level of risk, increasing security while allowing genuine customers through.

Once that's complete, enrich your fraud profiling system with data and intelligence, including credentials from internal and external sources.

Employing these actions can help drive a more holistic approach to fighting credential stuffing. This means that credentials and customer logins are blocked where required, but genuine customers can go about their business."

**YUVAL MARCO**

general manager of fraud and authentication at NICE Actimize

### HOW AI AND ML CAN DETECT FINANCIAL CRIME AMIDST MILLIONS OF TRANSACTIONS

The sheer quantity of financial crime attempts makes fraud extremely difficult for FIs to fight — bad actors deploy schemes as diverse as they are numerous. Manual transaction review teams and static rules can become overwhelmed or inadvertently alienate legitimate customers through false positives, but automated systems like AI and ML could give banks the edge they need to stop fraud in a seamless manner. In this month's Feature Story (p. 8), Beate Zwijnenberg, chief information security officer for ING Group, discusses how these systems help form multilayered fraud prevention systems by detecting anomalous transactions that could indicate financial crime.

### DEEP DIVE: HOW HARNESSING AI AND ML BOOSTS FIs' FRAUD PREVENTION EFFORTS

Banks deploy a wide range of fraud prevention protocols to protect themselves and their customers, but many of these existing efforts are largely ineffective. Solutions based on human analysis can have false positive rates of more than 90 percent, frustrating legitimate customers and even jeopardizing their loyalty. Solutions that harness AI and ML, however, could both accelerate these efforts and reduce friction for customers. This month's Deep Dive (p. 19) explores the advantages that AI and ML systems bring to fraud prevention and the obstacles hindering more banks from leveraging these solutions.

# FIVE FAST FACTS

**$1.9B**

Total consumer losses to fraud in 2019

**5B**

Number of unique leaked credentials circulating on dark web marketplaces

**134%**

Increase in new account fraud since the onset of the COVID-19 pandemic

**15%**

Increase in financial losses from identity theft in 2019

**60%**

Portion of businesses that said their fraud risk had somewhat increased due workers going remote

# FEATURE STORY

# ING On Its Multilayered Approach To Fraud Prevention

**The financial sector is a prime target for cyberattacks, with FIs around the world defending against breaches and spending up to $3,000 per employee annually on cybersecurity measures.**

These defenses take a variety of forms, including transaction review teams, static rules-based verification measures and biometric authentication processes. Banks are constantly looking for new ways to ensure this annual security budget is spent more efficiently, devoting resources toward ever-more-advanced fraud prevention.

Some of the most promising of these innovations involve AI and ML, analyzing thousands of transactions in real time to look for any anomaly that could be a sign of fraud. One bank harnessing AI and ML in its cybersecurity measures is Amsterdam-based ING Group, which has €887 billion ($1.05 trillion USD) in assets in need of protection.

"The real-time aspect of online fraud means that you need to intervene immediately, because otherwise the money is transferred and it's gone for good," said Beate Zwijnenberg, ING's chief information security officer. "So the real-time element [of AI] is quite important."

PYMNTS talked with Zwijnenberg in a recent interview about the financial crime that threatens digital banking systems and how AI and ML form an integral part of multilayered fraud defense systems that can drastically reduce this threat.

## THE SCOPE OF THE FINANCIAL CRIME THREAT

The objective of financial crime — illicitly obtain money — has remained unchanged since the days of Al Capone and Jesse James, but the methods used to turn a profit have become significantly more sophisticated than tommy guns and safecrackers. All fraudsters desire profit, but some aim for a payday not by stealing cash from the bank itself but by harvesting customer data, either

using it to siphon funds from individual bank accounts or selling the data online to other fraudsters.

"Fraudsters are after the data or the money, but until recently, the techniques had not changed," said Zwijnenberg. "If you have a traditional bank branch, they try to get into the safe and physically get the money out, and for digital banks, it's not much different. It is only the modus operandi that has changed."

Digital methods like phishing and malware are the most common tools of the trade for fraudsters, according to Zwijnenberg. Cybercriminals often combine the two in large-scale schemes, harvesting customer data through phishing scams and then leveraging malware to test their stolen credentials in a range of online services in the hopes that their victims use the same usernames and passwords elsewhere.

Fraudsters' targets have also evolved. Their typical victims used to consist of retail banking customers and everyday consumers, but corporate accounts have been targeted much more frequently in recent years, Zwijnenberg said. The same fraud tactics that victimize consumers often work just as well on corporate customers.

"Criminals are investing in business cases as well, [changing] from the retail side to wholesale banking and applying techniques to different customers," she said. "Phishing scams are the ones we see fairly often in business banking and wholesale banking, as well as identity theft."

The ongoing COVID-19 pandemic has amplified all of these strategies. Fraudsters' methods have remained largely the same, Zwijnenberg said, but they have increased in volume and have often used COVID-19-related angles to exploit bank customers' anxieties and insecurities regarding their personal safety and the precariousness of their financial situations.

"We've seen similar types of phishing and scams, but with the [COVID-19] theme," she said. "They'll say your banking card has expired and you need to log in because [the pandemic] has resulted in additional security

measures, for instance. We also see a lot of scams [involving] people trying to sell you masks, and of course they will never deliver."

Fighting this kind of fraud comes down to the use of advanced technologies such as AI and ML. These systems do not operate alone, however, working in tandem with static rules and human analysts in multilayered defense mechanisms.

## HOW AI AND ML HELP FIGHT FRAUD

The best fraud prevention measures, according to Zwijnenberg, are those that harness multiple layers of protection, starting with user authentication and including systems that analyze transactions to detect signs of fraud. AI plays an important part in this system but is not the be-all and end-all.

"You need a layered approach, making sure that you have multiple controls and invest in multiple areas," she explained. "You make sure that you invest in multiple domains at customer authentication, for instance, and you also make sure that you have the right detection and response capabilities in place. You need to get all the data and profile the customer based on that, and you have to make sure that you detect anomalies if needed."

AI and ML's crucial advantage, Zwijnenberg said, is in the sheer quantity of data they can comb through to find anomalous transactions and other signs of fraud. Digital banking's surge in popularity during the pandemic has generated terabytes of new data from customer transactions that would be impossible for a human employee to analyze and too complicated to manage with static rules alone.

"You cannot say it's always better to have an AI or ML model in place, because sometimes there's a very simple static rule that works perfectly well," Zwijnenberg said. "The huge advantage of applying machine learning is that the amount of data is becoming bigger and bigger over time. You need to find the needle in the haystack, and you benefit from applying AI and machine learning to make sure that you really only look into the specific areas that call for it."

Banks are not on their own in this fight, however. It is important for them to collaborate with other banks to share intelligence and technology, because although they may be competing with one another for customers, fraudsters threaten the entire industry.

"You cannot fight this war alone," Zwijnenberg noted. "It doesn't make a lot of sense to compete [with] each other in this area. It's better to work together and to see what we can learn from each other to make sure that we maintain customer trust, because that is what banking is all about."

A breach of customer faith can do more damage to an FI than any fraudster, as the decline in business from customer flight can result in more lost revenue than an individual heist. Maintaining customers' trust requires letting them know that their data and funds will be kept safe, and AI and ML are key tools in banks' arsenals to ensure this security.


NEWS &
TRENDS

# Cybersecurity trends

### MOST POPULAR PASSWORD IN THE WORLD IS '123456,' STUDY FINDS

Cybersecurity is more crucial than ever in the banking world because hackers are always devising new ways to break into customers' bank accounts, but it appears that a substantial fraction of these customers do not take their security as seriously as they should. A recent analysis of breached credentials by a computer engineering student in Turkey found that for one out of every 142 passwords, a user chose "123456," accounting for seven million out of the more than one billion passwords analyzed. This password is remarkably weak, as it is short, easy to guess and contains no special characters or capitalization.

The student found that there were only 169 million unique passwords out of the billion-plus leaked credentials he studied, and the top 10 most common accounted for 6.6 percent of the total. Only 12 percent of the passwords used special characters, 29 percent used only letters and 13 percent used only numbers. The average password length was 9.48 characters.

### SURVEY FINDS THAT FOUR IN FIVE INDIVIDUALS ARE TRICKED BY FRAUDULENT BANK MESSAGES

One particularly popular fraud technique consists of bad actors impersonating consumers' banks and sending them texts or emails asking for sensitive information like account numbers or passwords. A recent study of 2,000 bank customers found that four out of five consumers could not correctly identify fake messages when presented with a series of both phony and legitimate messages. Only 18 percent of customers correctly identified every fake message they were sent. The messages contained telltale signs of fraudulence, including spelling mistakes, links to nonbank websites and requests for personal information that a legitimate FI would never ask for.

The study found that customers between the ages of 18 and 24 performed the worst on the test, with only 9 percent of these individuals getting a perfect score. Less than a

third of this age group admitted placing an emphasis on fraud protection when choosing an FI.

### DARK WEB MARKETPLACES ARE FOUND TO CONTAIN MORE THAN 5 BILLION UNIQUE CREDENTIALS

Some fraudsters stage their schemes not by soliciting personal information from victims directly but by purchasing their credentials on dark web marketplaces. Security firm Digital Shadows recently published a study showing there were more than 5 billion unique username-password combinations circulating on the dark web. The firm found over 15 billion credentials total, including bank account numbers and other valuable information that could be used for financial crimes. The 5 billion unique combinations present a much higher risk, however, as they have not yet been used by bad actors and are likelier to slip through security monitoring.

The number of stolen credentials available on the dark web has increased by 300 percent since 2018, according to the study. The collected credentials stem from almost 100,000 different data breaches, and the average prices for each range from $15 to $71. Bank credentials are among the most valuable, as some sell for more than $500.

### IDENTITY THEFT FRAUD LOSSES HIT $16.9 BILLION LAST YEAR

These stolen credentials are often used to carry out financial crimes targeting victims' bank accounts, and this type of fraud increased by 15 percent from 2018 to 2019, according to a recent study. Total losses hit $16.9 billion last year after reaching a five-year

The number of stolen credentials available on the dark web has **increased by 300 percent since 2018.**

low in 2018. American Banker attributed the 2019 spike in fraud to an increase in ATOs, in which fraudsters hijack accounts entirely and prevent legitimate users from accessing their funds. Only 12 percent of financial fraud instances were due to ATOs in 2015, but 2019 saw this rate climb to 53 percent.

Security experts said that knowledge-based authentication, consisting of passwords or security questions, is ineffective at preventing this type of fraud, as this data can more easily be leaked in data breaches. Behavioral analysis systems that monitor and study users' typical patterns are gaining steam, though, as they can identify abnormal behavior and flag transactions or logins as fraudulent.

# COVID-19 and financial crime

### FINANCIAL CRIME ATTEMPTS RISE DURING COVID-19 PANDEMIC

The COVID-19 pandemic has been devastating to most of the world, yet it has afforded a wide range of new opportunities to fraudsters looking to take advantage of bank customers' economic insecurities. Digital identity verification provider Socure recently released a report that said a variety of different fraud techniques have been on the rise during the pandemic. New account fraud attempts, in which bad actors try to open bank accounts under false identities, have increased by 134 percent since the outbreak was declared a pandemic in March, while fraudulent credit card applications increased by 93 percent between March 24 and April 23.

Not even government attempts at economic relief were safe, with the Paycheck Protection Program (PPP) leading to a 65 percent increase in fraud targeting small to mid-sized business (SMB) loan applications. Challenger banks fell victim alongside their traditional bank cousins, experiencing a 200 percent increase in demand deposit account (DDA) fraud between March and June 2020.

### REMOTE WORKING INCREASES FINANCIAL CRIME RISK, STUDY FINDS

One of the most wide-ranging effects of the pandemic is the sheer number of office workers who are now working from home. More than one-quarter of all businesses in a recent survey reported having 100 percent of their staff working remotely, and 86 percent had half their staff out of the office. This shift is effective at preventing disease transmission but has also increased the risk of financial crime. Sixty percent of the businesses surveyed said that fraud threats have increased at least somewhat due to working from home, and 27 percent said such risks had increased considerably.

The heightened risk is due to the higher number of sensitive documents and files being transmitted online and outside the company firewall, where they can be intercepted by fraudsters. Businesses also fear incursions on Zoom or Skype meetings, where fraudsters can be privy to sensitive information and use it to harm the company. Security experts recommend regular software updates, two-factor authentication and proper password management to help reduce these risks.

# Fraud-fighting initiatives

### US SECRET SERVICE COMBINES ELECTRONIC AND FINANCIAL CRIME UNITS INTO SINGLE TASK FORCE

One of the primary government agencies charged with preventing financial crimes is the U.S. Secret Service (USSS), which was originally created to fight counterfeit money production before it became famous for protecting presidents. The agency's financial crime prevention portfolio has extended into the digital age, with the USSS recently announcing that it would combine its electronic fraud and financial crime units into a one entity that will focus on preventing electronic fraud schemes like ransomware attacks and business email compromises. The new unit, known as the Secret Service Cyber Fraud Task Force, was formed in part from the massive increase in financial crime attempts erupting during the COVID-19 pandemic.

Lawmakers are in favor of revitalizing the USSS's financial crime prevention duties by moving it back under the jurisdiction of the Department of the Treasury, its original home until it was shifted to the Department of Homeland Security (DHS) following the Sept. 11 attacks. Proponents of this idea said that DHS's other security-related expenses prevent the USSS from getting the resources it needs to fight financial crime and that the department would be better empowered within the Treasury.

Two-thirds of British banks are now leveraging some form of machine learning to detect fraud and money laundering, with most firms using it for at **least two different functions.**

### FEDERAL RESERVE ISSUES REPORT ABOUT SYNTHETIC IDENTITY FRAUD AND HOW TO DETECT IT

The Federal Reserve is also taking steps to fight financial crime with a recently published report titled "Mitigating Synthetic Identity Fraud in the U.S. Payment System." The study details a multilayered strategy to fight synthetic identity fraud, a method by which fraudsters concoct a fake identity out of whole cloth rather than steal another individual's. Synthetic identities make up 0.3 to 0.6 percent of new accounts, according to software company SentiLink, but certain FIs could have up to 2.7 percent of new accounts held by such identities. Their effect on FIs is outsized, as synthetic identities are responsible for 20 percent of all loan portfolio losses.

Fraud experts recommend that banks look beyond surface-level authentication measures like name, date of birth, address and Social Security number to fight financial fraud. The Fed's report instead recommends the use of AI and ML to detect synthetic identities, noting that such technologies can also reduce detection times and labor costs.

### COLORADO MAN PLEADS GUILTY TO DEFRAUDING FEDERAL BANKS OF NEARLY $32 MILLION

Fraudsters can rack up immense sums if left unchecked, especially if they originate from sources that banks would typically trust. A man from Boulder, Colorado, recently pleaded guilty to selling 144 fraudulent residential mortgage loans to a bank in Texas for a total value of $31.9 million, using stolen identities from customers of the businesses he owned. The customers had used the defendant's companies to conduct real estate transactions, in the process giving him enough information to make fraudulent mortgage applications. The fraudster asked these customers for permission to apply for mortgages on their behalf and then lied to them that the application was rejected when in fact it was approved, and the fraudster simply kept the money.

This fraud process also involved forged signatures, altered credit reports and fake title documents. The defendant was charged by the U.S. Attorney's Office with federal bank fraud and aggravated identity theft, having undergone investigation by several federal agencies including the FBI, the Federal Deposit Insurance Corporation and the Department of Housing and Urban Development.

## New financial crime prevention solutions

### TWO-THIRDS OF UK BANKS HARNESS MACHINE LEARNING FOR FRAUD PREVENTION

Other fraud-fighting prevention solutions use technologies like AI and ML to detect and flag financial crime attempts, and these methods are now more popular than ever. A survey of 500 United Kingdom-based FIs found that two-thirds of British banks are now leveraging some form of ML to detect fraud and money laundering, with most firms using it for at least two different functions, such as customer service or risk management. Other financial services markets, like those of consumer finance and insurance, are using AI to detect the fraud that plagues their industries as well.

AI systems can analyze vast quantities of data in a fraction of the time it takes human analysts to do the same, and AI systems can also provide a more holistic view of fraud trends rather than analyzing each transaction in a vacuum. A smart system can see which transactions are abnormally large compared to the customer's average and flag them as potentially fraudulent, for example.

### SEVERAL UK BANKS TO REQUIRE EXACT NAME MATCHES FOR FRAUD PREVENTION

Customer authentication is key for preventing bad actors from gaining access to customer accounts, with banks almost always requiring a password to verify their customers' identities. Another method gaining popularity is requiring recipient names to

be an exact match for the account number in payment transfers, which banks previously did not take into consideration. Users wishing to pay someone else had to get only the account number correct and could put anything they wanted into the name field, but now an alert will pop up to the payer if the payee's name does not match the account name. This could potentially thwart fraudsters asking victims to pay them under the pretense that they are paying someone else, as bad actors often pose as trusted authorities while providing their own account numbers for payment.

The requirement for an exact name match means that entering "Dan Smith" will not work if the name on the recipient's account is "Daniel Smith," for example. Users can override the name match requirement if they wish, but the alert should serve as a warning that something is potentially amiss if they are sending money to a stranger.


DEEP
DIVE

# How AI and ML Improve Fraud Detection Rates And Reduce **False Positives**

**Financial crime and other forms of digital fraud are a pressing concern for banks, credit unions and other FIs, with fraudsters stealing $2.8 billion from bank accounts in 2018. Banks are devoting time, money and effort to prevent this type of fraud, which stopped $22.3 billion in fraudulent transactions during the same year. They could head off even more, however, by reexamining their often inefficient and intrusive fraud prevention procedures.**

Most banks rely on teams of human analysts to examine transactions for potential financial crime, but these teams encounter numerous issues. Forty-five percent of banks say their investigations take too long to complete, and 40 percent say the investigations result in a high number of false positives, which occur when legitimate transactions that have been mistakenly flagged as fraudulent. Banks can even have false positive rates of more than 90 percent, resulting in unpleasant experiences for customers as they are forced to resubmit their transactions.

FIs are exploring many avenues to overcome these stumbling blocks, but few are as promising as AI and ML. The following Deep Dive explores the fraud-fighting benefits of these systems as well as the challenges that many banks face in implementing them.

## THE PROS – AND CONS – OF ARTIFICIAL INTELLIGENCE

Detection systems driven by AI offer a number of fraud prevention benefits, as they can analyze transactions holistically, comparing each data point within a transaction to every other data point in fractions of a second. These systems can also compare each

transaction against every other transaction banks have ever processed to determine its likelihood of being fraudulent based on variables a human analyst might never notice, such as attempts to log in to the same account with different usernames and passwords over the course of several months or uncharacteristically large transactions.

Banks are deploying AI-based systems in record numbers, with more than $217 billion spent on AI's applications for middle-office use cases like fraud prevention and risk assessment. These investments are paying off, according to fraud prevention specialists, as 80 percent of experts say AI reduces payments fraud and 63.6 percent of FIs cite AI as a valuable tool for halting fraud before it succeeds. These systems are commonplace at large FIs that have more than $100 billion in assets — 72.7 percent of which leverage AI — but only 5.5 percent of all FIs reportedly have an AI-based system in place.

The most obvious explanation for this gap is AI systems' expense, but there are a number of other concerns that keep FIs from jumping aboard the AI bandwagon. AI systems often do not operate in real time, with 45.6 percent of FI fraud specialists citing this as a concern — a significant obstacle for payments that need to be processed instantly. A lack of transparency is a problem as well, according to 42.8 percent of specialists: A human analyst could definitely provide justification for rejection of any given transaction, as opposed to many AI systems, whose reasonings may much more nebulous.

## SUPERVISED AND UNSUPERVISED MACHINE LEARNING

Some of these concerns can be addressed by ML, a more advanced form of AI that can learn from its own analyses instead of operating based on unchanging protocols. ML systems take past transactions into account and apply these rules to future analyses to detect financial crime, making them gradually more adept at fighting fraud over time. This means that banks' investment in the technology will increase in value as ML tools become more familiar with FI systems and the techniques that fraudsters use to crack them.

ML largely comes in two different flavors: supervised and unsupervised. Supervised ML requires predetermined parameters — a supervised ML system could be given a profile of digital fraud and search a database to find transactions that match this profile, for example. Unsupervised ML, meanwhile, does not require set outcomes and relies on its own ruling to detect patterns and anomalies. Unsupervised ML is thus superior to the supervised variety at combing through much larger data sets and is also better suited to finding innovative fraud techniques that have not yet been encountered.

Financial crime attempts against banks will likely never cease completely, but the addition of AI and ML to FIs' fraud-fighting arsenal could go a long way toward making these attempts less likely to succeed.

# ABOUT

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.



Stay current with NICE Actimize webinars at 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.

# PREVENTING FINANCIAL CRIMES PLAYBOOK