



JANUARY 2021

Taking the fight to the fraudsters

Fraudsters grow more virulent during the pandemic



BY TERRY BADGER, CFA
tbadger@bai.org

CONTENTS

3

Pandemic-related fraud: A crisis within a crisis

Smaller institutions are struggling to stay ahead of the crooks as COVID-19 scams hit community banks and their customers.

6

Combating fraud from the very start

Banks are addressing account opening weaknesses as criminals exploit pandemic-related security gaps.

9

Profitable defense against financial crime

Using a holistic approach featuring automation and analytics can mitigate risk, deliver a better CX and generate revenue.

12

Small business has a big fraud problem

10 ways to minimize the risk and deal with the outsized impact of schemes and scams.

15

Anti-fraud technology with a human touch

AI and ML solutions are rooting out hidden risks, while enhancing the customer experience.

18

Security without compromise

As ATMs become more sophisticated, so must your security measures to thwart physical and online attacks.

22

Better verification with less friction

Ramping up your authentication standards doesn't have to mean sacrificing customer experience.

Fraudsters are nothing if not resourceful and opportunistic—give them an inch, and they'll take as much as they possibly can. And COVID-19, which has brought severe disruption to workplaces and customers, certainly created many opportunities for them to exploit financial services.

The latest fraud trends report from LexisNexis Risk Solutions found that monthly fraud attempts at financial services firms climbed nearly 20 percent during the period after the arrival of the coronavirus, and that the cost of fraud to the firms increased by roughly 11 percent.

The types of attacks aimed at banks and credit unions have also grown more varied and sophisticated. Some of them take inspiration from the specifics of the COVID-19 environment—examples include calling work-from-home bank employees while posing as company IT representatives, and contacting customers new to digital banking and pretending to be from bank call centers.

This month's BAI Executive Report identifies fraud and cybersecurity challenges faced by financial firms and offers insights on how to address them.

Our lead story by Karen Epper Hoffman digs into the tougher time that smaller financial providers are having with fraud because of their more limited IT departments and smaller capital budgets. She centers her reporting around a family of community banks in the Midwest working to stay ahead of the scam artists plying old and new tricks.

Because customers can be weak spots in a bank's defense, these banks have prioritized efforts to raise awareness of various fraud risks and how to minimize those risks. They are also implementing stronger employee protocols and technology for prevention and detection to further harden their security.

New account opening is a main targets for fraudsters during COVID-19, with cybercriminals using personal information stolen in phishing attacks or data breaches. Remote takeovers of cell phones, used for sending those six-digit codes to confirm identity, have also been reported.

In his article, Howard Altman writes that 85 percent of banks and credit unions experience fraud during the account opening process, but they are fighting back. Responses include increasing their training regimens, which can better prepare bank employees who have been shifted to new roles during the pandemic. BAI's training business has seen nearly a 20 percent jump in the use of its curriculum.

Cheryl Chiodi from ABBYY makes the case for a holistic approach centered on automation and analytics. She contends this can not only provide more-robust risk protection, but also enhance the customer's experience, which can help generate more revenue.

In her article, she defines this holistic strategy as being "a dynamic, continually evolving combination of prevention, detection, analysis and response." And its high-tech structure allows for lessons learned in one place to be shared, enabling the industry to join together to safeguard common interests.

The other articles in this month's Executive Report include:

- » Andy Shank from Harland Clarke on fraud pressures facing small businesses, for whom each dollar lost represents a bigger chunk of revenue. He lists 10 ways to minimize the risk of getting scammed—near the top of the list is hiring well and not skimping on training.
- » Katie Kuehner-Hebert on how banks are working to infuse their anti-fraud technology with customer-friendly features that blend more smoothly into the banking experience. One of the keys, she writes, is to build in more personal characteristics into the security side.
- » Chad Davis from F5 on the fine security line that banks and credit unions walk between protecting customers and frustrating them, but from the verification perspective. He advocates for more modern, technology-based solutions to strike that balance.
- » And Jordan Riek from Cardtronics on what banks and credit unions can do to make their ATMs less vulnerable to attack, both by tech-minded fraudsters and brute-force bad guys using heavy chains and pickup trucks. These days, he writes, ATMs function like miniature branch offices and, security-wise, need to be thought of that way.

With the development of COVID-19 vaccines, we are all optimistic that we may be on the back side of the current pandemic. But there is no accompanying anti-fraud vaccine, so banks and credit unions must be diligent in taking measures to protect themselves from infection by those intending to do them serious harm.

Terry Badger, CFA, is the managing editor at BAI.

Pandemic-related fraud: A crisis within a crisis

BY KAREN EPPER HOFFMAN

Smaller institutions are struggling to stay ahead of the crooks as COVID-19 scams hit community banks and their customers.





When the going gets tough, the tough crooks get going—with more scams, cons and other types of fraud than ever.

Fraud attempts have as much as tripled in the nine months since COVID-19 began, according to financial institutions and federal agencies. A wide variety of new and emerging scams prey on those who have been hit hard financially by the economic effects of the pandemic, as well as on those who want to be charitable in this time of crisis.

[John M. McVoy](#), director of financial crimes risk management and senior vice president for [Heartland Financial](#), says that since March his company has seen increased fraud across the board—“so much so that we’ve had to double our staff associated with fraud mitigation.” Fraudsters are targeting retail customers and businesses with common scams such as email compro-

mise, robocall data collection and phishing, as well as new variants related to the pandemic.

For example, newly remote employees struggling with computing or teleconferencing have been tricked by sly scam-artists posing as their corporate IT department, says McVoy, whose company owns 11 U.S. community banks with combined assets of nearly \$18 billion. Bank customers who turned to online banking platforms when local branches shut their doors were duped by scammers posing as their bank’s customer service representatives.

FRAUDSTERS PREYING ON THE DESPERATE

Another common scam, targeting the recently unemployed, has involved fraudsters posing as employment services and gaining access to account information on the pretense of “taking an application fee for job hunters,” he adds. And this is to say nothing of the more

*People are desperate.
And fraudsters are
sharks seeing blood
in the water.*

JOHN M. MCVOY
HEARTLAND FINANCIAL

sophisticated cyber criminals, who are still plying their trade with the typical phishing, ransomware and other virus schemes—now with a recently widened field of potential victims, thanks to the booming number of people working, shopping, communicating and banking online and via their mobile phones.

“People are desperate,” McVoy says. “And fraudsters are sharks seeing blood in the water.”

[Chris McCulloch](#), corporate security officer and senior vice president for \$5 billion-asset [Enterprise Bank & Trust](#) of Clayton, Missouri, points out that “any time there is a drastic event or change in the economy, people will fall for more scams.” Financial institutions like Enterprise Bank are reporting increases of between



Unfortunately, those hardest hit are often the unemployed or senior citizens.

CHRIS MCCULLOCH
ENTERPRISE BANK & TRUST

they're slicker and more believable, and playing to the fears and needs of the recently homebound populace. "Fraudsters have definitely upped their game. They are getting more sophisticated in their spoofing, and [in some cases] attacking on a larger scale."

Like many banks, Heartland Financial has put together a resources section on its website regarding the recent rise in fraud, and it has sent out emails to customers explaining how to spot and mitigate potential fraud in their personal and professional financial lives. "We've put up information on social media too, and we've put on security-related seminars for our commercial customers," says McVoy, adding that they have also promoted Positive Pay, a business-related fraud prevention system to decrease fraud risk for commercial customers.

Heartland is working with its banks and their vendors on added authentication technologies and protocols for employees and customers alike, as well as improving early detection technologies for the back office. "As the fear is becoming more widespread, there is also a risk of

30 percent and 300 percent in the number of fraud attempts reported by retail and business customers alike.

"Unfortunately, those hardest hit are often the unemployed or senior citizens," McCulloch says, adding that many reports show that the elderly (among those most susceptible to serious illness because of COVID-19) lose on average double the amount that others lose, "so it hits them especially hard."

With more people than ever working from home, electronic fraud has become the most common fraud type, McCulloch says. But, she agrees this recent pandemic-era fraud goes well beyond run-of-the-mill scams to incorporate themes that are particularly painful right now: romance, jobs and politics.

PHISHING EMAILS ARE GETTING SLICKER

Continuing the ongoing trend that began well before 2020, "fraudsters are continually getting better," says McVoy. Phishing emails, for example, used to land in inboxes full of typos and jumbled grammar, so they were easy to spot by bankers and customers. Now,



over-saturating customers with all these concerns and precautions," McVoy cautions.

On a positive note, McVoy observes anecdotally that he does not see fraudsters actually succeeding at a vastly greater rate than before the pandemic. The problem is there are so many more fraud attempts and variants taking place that "it can overwhelm the normal [fraud mitigation] mechanisms." This is especially true for community banks, which often lack the IT security resources of their larger counterparts. Hence, many banks have been forced to "move staff around, and all banks are moving more security efforts online to address customer needs [and] behaviors."

Despite all these added pressures, community banks remain hopeful that they can warn customers how to

avoid these potential scams, especially as the pandemic enters its second brutal wave. Many recent scams have been connected to the \$669 billion Paycheck Protection Program, launched this past April to combat the economic downturn. Federal agencies have warned that, with the \$2 trillion Coronavirus Aid, Relief, and Economic Security (CARES) Act, even more criminal opportunities will emerge. [↗](#)

Karen Epper Hoffman has been writing about banking and technology issues for nearly a quarter of a century for publications including American Banker, Bloomberg Businessweek and Financial Times' The Banker.



Combating fraud from the very start

BY HOWARD ALTMAN

Banks are addressing account opening weaknesses as criminals exploit pandemic-related security gaps.

Nearly a year into a deadly pandemic that's changed almost every aspect of our lives, financial institutions are still struggling to deal with the evolving security ramifications.

For banks, the challenges begin with the start of their relationships with new clients, according to [a recent report](#) by BioCatch. The cybersecurity firm says 85 percent of financial institutions experience fraud in the account opening process. Cybercriminals use stolen credentials or synthetic identities to create new accounts with the intent of committing fraud. Data breaches and phishing attacks provide fuel in the form

of Social Security numbers, addresses, phone numbers, login IDs and other personally identifiable information.

The pandemic has exacerbated the problem of account opening fraud, as employees across industries and sectors have moved out of their offices and into their homes, which are less secure, according to financial industry officials and cybersecurity experts. That has created a new set of challenges as the financial industry struggles to balance security and customer satisfaction.

“The pandemic created a large increase in online account and banking activity, and it has altered the ways in which each bank might use data to gain

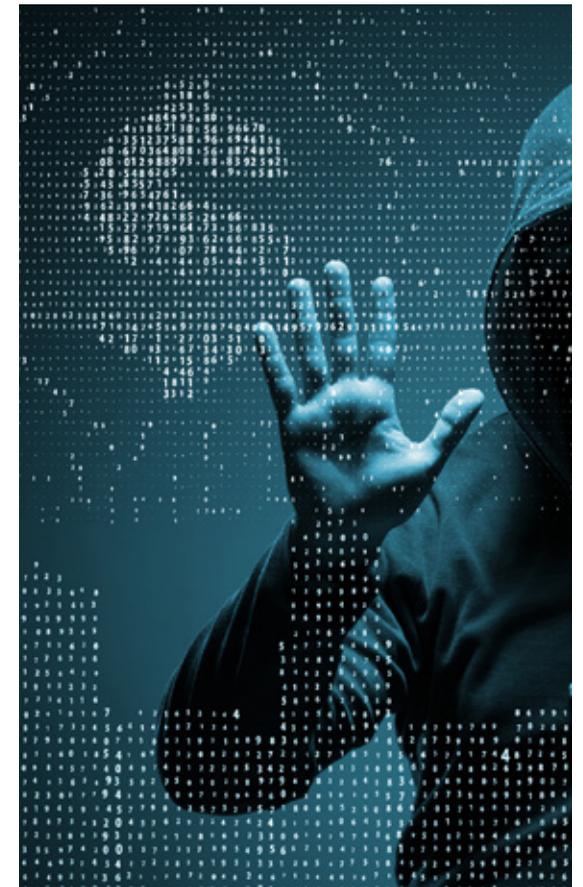
When a fraudster has taken over your known phone number, often known as SIM Port fraud, they are able to validate their possession of the number.

CHRIS GERDA
BOTTOMLINE TECHNOLOGIES

comfort with the accounts opened online,” says [Chris Gerda](#), risk and fraud prevention officer at [Bottomline Technologies](#), a business payments and processing solutions firm based in Portsmouth, New Hampshire.

The most nefarious examples of account takeover or identity theft fraud have involved remote-access takeovers of a victim's computer or cell phone, says Gerda. “When a fraudster has taken over your known phone number, often known as [SIM Port fraud](#), they are able to validate their possession of the number, and this is often a strong factor in a bank's decision to allow an online account opening or new consumer loan approval.”

The good news, says Gerda, is that most financial services providers were already doing online account opening and many were deeply engaged in the online lending space prior to the online rush. This helped when their brick-and-mortar operations were disrupted, he says, though an upswing in applications by new customers has presented some challenges.



BANKS ARE MORE FOCUSED ON TRAINING

As a result, banks are increasing the amount of training that employees receive. [Ed Marcheselli](#), managing director of learning and development at [BAI](#), noted a 19 percent increase in the usage of BAI's contact center compliance training curriculum during the first six months of the COVID-19 pandemic as banking employees from roles across the organization were re-deployed and cross-trained to support the increased contact center volumes.



As COVID-19 continued to create challenges, requests for additional training increased, Marcheselli says.

“We received additional requests for training on topics like spotting e-signature fraud and preventing COVID-19 medical fraud,” he says. “We provided microlearning courses—interactive, five-minute minicourses—to allow busy financial services employees to learn important regulatory information quickly and efficiently.”

Gerda offers five ways banks can help prevent account opening fraud:

- » Correlate multiple data points for each online application and revamp processes if you have all your “eggs in one basket.”
- » Design a system of case management for new online applications that can pivot to new forms of data and easily ingest new [Application Programming Interface calls](#), a set of protocols, procedures and tools allowing interaction between two applications.



It's a challenging time for financial institutions because abandoned calls could adversely impact the bank and have regulatory issues.

NERMEEN GHNEIM
FIRST NATIONAL BANK

- » Do not rely on scores from third parties when analyzing your new account applications. Go deeper to understand specific risk codes and use that data in your own rule sets covering due diligence for applications.
- » Use anti-fraud solutions that offer repositories of threat intelligence of known bad actors, which can track fraud across other institutions using the solution so that everyone can benefit together from that data.
- » Partner with anti-fraud solution providers using API calls to enrich the data you gather at account opening.

[Nermeen Ghneim](#), a branch manager at Pittsburgh-based [First National Bank](#), cautions that banks must keep customer satisfaction in mind when implementing any solutions. “It’s a challenging time



for financial institutions because abandoned calls could adversely impact the bank and have regulatory issues,” she says.

Financial services organizations have been directing the calls through an automated verification system that requires the consumer to enter their banking information while they are on hold to get a representative, says Ghneim.

“The majority of banks have an automated tool that can detect a spoofed phone number, and it will determine if it’s a high- or low-risk phone number,” she says. “Those who fall in the high-risk phone numbers category could go into further verification questions.”

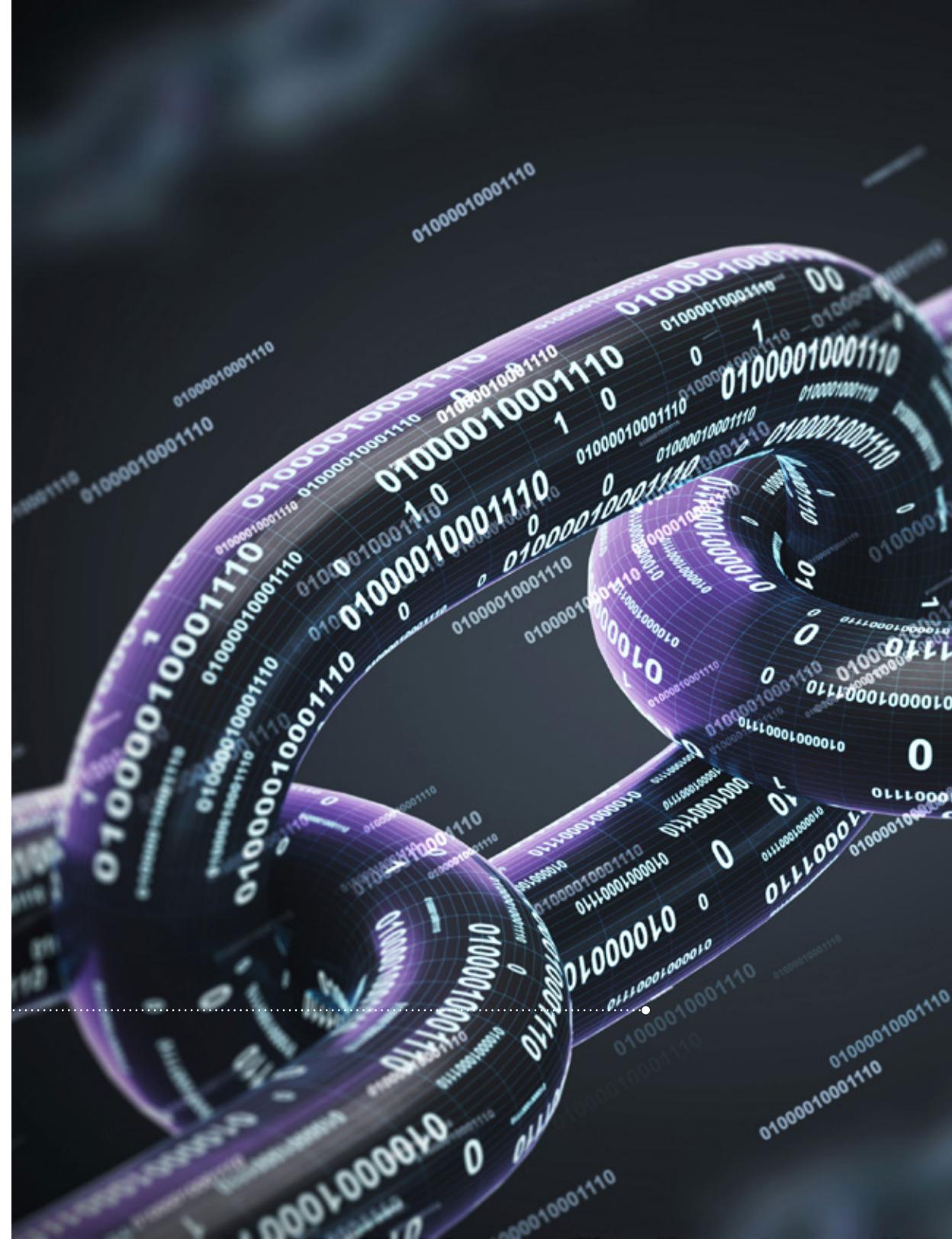
Ghneim says that, to help with the abandoned-call rate and reduce wait times and the number of calls in the queues, banks internally outsourced their calls to retail branch employees so they can help with the volume and to go through the verification process. Those retail branch employees can also answer questions, handle basic requests and help lower the ratio of abandoned calls. ↗

[Howard Altman](#) oversees coverage of issues affecting troops and their families as managing editor of *Military Times*. His work has appeared in the *New York Times*, *Daily Beast*, *Philadelphia Inquirer*, *Tampa Bay Times* and other publications.

Profitable defense against financial crime

BY CHERYL CHIODI

Using a holistic approach featuring automation and analytics can mitigate risk, deliver a better CX and generate revenue.





The experiences of COVID-19 in 2020 taught financial institutions that they must reimagine the way they assess and manage risk. Fraud volume keeps growing, so frontline risk teams must be empowered with the technology necessary for powerful analytics, more-robust alert management and improved accuracy.

There is no shortage of data in financial services—structured, unstructured, transactional, account-level and even behavioral—that when combined can drive insights to deliver new, customer-centric offerings. While the use of consumer data is the subject of increasing regulation, there remains tremendous potential to innovate to bring benefit to both financial institutions and their customers. However, the technological advancements that make it possible to deliver innovative products and services to banking clients can, when in the hands of nefarious actors, also make fraud more pervasive.

As financial institutions look to reset, reinvest and reimagine their business in 2021, there must be an

urgent focus on effectively combating fraud through predictive analytics, robotic process automation (RPA) and natural language processing (NLP). This requires shifting the mindset from a narrow focus on false positives and loss prevention to a broader emphasis on gaining actionable insights that tangibly enhance business value.

THE BENEFITS OF BREAKING DOWN SILOS

According to the LexisNexis [2020 True Cost of Fraud™ Study](#), every dollar's worth of fraud costs financial services firms \$3.25, up 11 percent from the previous year. Financial crime not only puts financial institutions at risk for monetary loss, but reputational damage as well.

In the financial services industry, healthy client relationships, built on a reputation of trust, translate into customer satisfaction, improved customer value and customer loyalty. Since client acquisition costs are so high—one [recent study](#) found that the average total cost for a financial advisor to acquire a new client

is more than \$3,000—financial crime prevention and reputational protection have a significant impact on a financial institution's bottom line. By converging fraud, anti-money laundering (AML) and cybersecurity, financial institutions can consolidate data across historically isolated functions for a more holistic view of risk.

With significant similarities in the data collected across AML, fraud and cyber teams, breaking down these silos can provide a more transparent view of the threat landscape, better detect suspicious transactions and streamline investigations. Since the criminals are using cyberspace to commit fraud and ultimately need to monetize that information and launder the proceeds to make them appear legitimate, it makes business sense to bring these functions together.

Regulators in some countries expect firms to have a holistic view of risk across functions and to [report cyber events](#) as part of normal AML and Suspicious Activity Report (SAR) obligations. With this model, financial institutions can also reap the benefit of reducing operational costs and enhancing efficiency while developing a cross-functional view.



By converging fraud, anti-money laundering (AML) and cybersecurity, financial institutions can consolidate data across historically isolated functions.

WHAT DOES A HOLISTIC STRATEGY LOOK LIKE?

A holistic strategy is embedded in the culture of the financial institution—not treated as a project, but built into the DNA. This kind of strategy is risk-based and looks at all of the access points, including hardware, software, people, processes and content. It is a dynamic, continually evolving combination of prevention, detection, analysis and response that enables financial institutions to combat advanced threats and potential losses.

With a holistic approach that uses past events and creative thinking to identify problems before they occur, financial institutions can collaboratively collect and analyze intelligence from across the organization. This model improves intelligence-sharing across the industry and allows financial institutions to participate in exercises or drills that can continually test and improve security playbooks.

While it is important to examine each point in the banking relationship and each transaction, the most effective place to begin is the onboarding process.



or fines. There is greater protection against identity theft and fraud from a customer perspective and fewer security incidents increase uptime, allowing customers seamless access to their financial lives.

HOLISTIC APPROACH USING MODERN TECHNOLOGIES

There are a host of benefits that come when a financial institution achieves a holistic fraud prevention strategy. Of course, the most significant and crucial benefit is financial—mitigating those massive potential losses, which, according to EY, are estimated at [\\$1.4 trillion to \\$3.5 trillion](#) each year.

Improving organizational visibility and reducing manual effort via AI, RPA and NLP can also free up security practitioners to focus on protection and mitigation, rather than compiling data from multiple sources and creating roll-up reports.

Reimagining risk through this lens requires more than technology investment. As stated before, people, processes and content all play a part in the successful implementation of a holistic approach. At the board level, a priority must be placed on financial crime operations, which includes dedication to providing sufficient human and technological resources.

Top management will soon be convinced that this approach not only ensures a robust defense against the most difficult attacks financial institutions encounter, but that enhancing customer experience, generating revenue and mitigating financial crime risk are complementary endeavors, and each strengthens the other. ↗

Cheryl Chiodi is solutions marketing manager for financial services at [ABBYY](#), a global digital intelligence company based in Milpitas, California.

Streamlining onboarding by leveraging modern technologies enables financial institutions to filter out suspicious and fraudulent actors and deliver a more frictionless experience to good clients.

Using a combination of technologies, including artificial intelligence (AI), RPA and NLP, financial institutions can ingest and process both structured and unstructured documents, minimize manual steps and reduce the need for making redundant requests of the client. Establishing an effective client onboarding process not only enables faster detection of potential fraud, it plays a significant role in developing strong and long-lasting relationships with new clients.

A holistic strategy also provides the visibility necessary to better prepare for auditing and compliance requirements. It improves efficiency, protects the brand and reputation, and protects against sanctions

ABBYY®

Improve KYC processes and the content that fuels them

Learn More abbyy.com/finserv



Small business has a big fraud problem

BY ANDY SHANK

*10 ways to minimize the risk
and deal with the outsized impact
of schemes and scams.*



Prevention and mitigation strategies can mean the difference between a thriving enterprise and a shop closing its doors. Fraud incidents tend to disproportionately affect small businesses, since the relative size of a financial loss makes up a much bigger chunk of revenue compared with larger organizations.

Compounding the problem is the duration of fraud. Because small businesses are less likely to spend the time and money needed to reduce risk, fraud is more likely to endure for longer periods before being detected.

Smaller businesses also have fewer fraud controls than larger organizations and, as a result, become victims more frequently. For example, [billing and payroll fraud](#) at small businesses occur twice as often compared with larger organizations, while check and payment tampering occur at four times the rate.

FRAUD FROM EVERY DIRECTION

No matter their size, all businesses face numerous fraud vulnerabilities. On the low-tech side, internal fraudsters can skim money from a business before it is deposited and recorded on the books. Other tricks

include fictitious invoicing, bogus reimbursements, check tampering and payroll schemes.

On the technological side, small businesses have for years faced the threat of hackers, with common intrusions such as malware and viruses. But the nature of attacks has changed. In the past, hackers meant to destroy data and, in doing so, showcase their skills. Today, they seek to go undetected so they can steal company trade secrets, customer payment information, customer personal information and vendor records. Hackers can even remotely lock a business's computer system and hold it for ransom.

Most schemes like this originate through a malicious email opened by an unsuspecting employee. When an employee interacts with a malicious email, the goal of the email is usually to gain access to the employee's email account or system access. In 2019, [the FBI received 23,775 complaints](#) about such business email compromise, which resulted in more than \$1.7 billion in losses.

Another growing area of exposure includes identity theft in which fraudsters steal business information, such as tax identification numbers, and wreak havoc by taking out loans in a company's name. Fraudsters also target a business's customer records to sell customer identities on the black market. Mobile devices have introduced new vulnerabilities to in-house networks, giving perpetrators new entry points. If your employees can use their own devices for business purposes, how confident are you that the devices are not compromised?

The good news is that small businesses can implement policies, procedures and safeguards that can increase detection, minimize losses and ensure effective resolution of fraud. Consider these 10 low-cost strategies that could significantly reduce the risk and impact of fraud for your business:

- 1. Be thorough when hiring.** [Internal staff accounts for 37 percent of fraud](#), so your ability to protect your business starts with recruitment.
- 2. Establish a code of conduct.** Employees are less likely to cross the line if they have a strong sense of company rules and expectations.
- 3. Educate and cross-train your employees.** Your staff must be aware of all the ways a company's financial health and reputation can be compromised. Rotate job responsibilities so that one person does not remain in a sensitive position for a long period.
- 4. Keep close tabs on finances.** Check bank and credit card statements monthly and know how much it costs to run your business, as well as how much money is coming in.
- 5. Bolster computer security.** Protect your network with firewalls, anti-malware and email phishing detection products.
- 6. Be aware of regulatory changes.** Pay close attention to local, state and federal requirements for protecting customer information and reporting fraud.
- 7. Use checks with security features.** Checks with security features such as holograms, thermochromic heat-sensitive ink, chemical reactive paper and a true watermark make duplication difficult for fraudsters.
- 8. Use a fraud detection monitoring service.** Having a set of eyes on the business can help detect fraud so you can minimize the damage.



Unfortunately, the threat of fraud is here to stay, so small-business owners must be diligent in reducing risk.

STRATEGIES FOR MITIGATION

Given the rampant nature of fraud nowadays, small businesses also need to plan for the day it happens. Consider these ideas for alleviating fraud's impact:

- 9. **Subscribe to a fraud remediation service.** *Fraud remediation advocates can determine the threat, investigate acts by unknown parties or employees of the business, and spearhead the investigations needed to prepare cases and speed the path to a resolution.*
- 10. **Look to experts to implement a response plan.** *Work with a recovery service that can provide an action plan for the critical first 48 hours after the discovery of a security breach or fraud.*

DON'T WAIT—START NOW

Unfortunately, the threat of fraud is here to stay, so small-business owners must be diligent in reducing risk.

The [median time to detect an internal fraud scheme](#) is 14 months. This means businesses must be looking for both internal and external threats at all times, but they need not go it alone. Financial institutions can help small businesses integrate fraud prevention and mitigation into their workflows to help prevent fraud and minimize its impact. ➤

Andy Shank is vice president of fraud and risk management at Harland Clarke. He brings more than 18 years of experience assessing risk and investigating fraud at the local, state and federal level and across multiple sectors.

Count On Us To Deliver For You



Consumers are in charge. It's no longer enough to simply satisfy your customers, it's about engaging them to keep you first in their minds.

Harland Clarke can help. With us, you have a single, trusted partner dedicated to executing on your business strategy and supporting your long-term success.

We deliver every step of the way. Count on us for superior customer experience (CX) solutions designed to give you a powerful competitive advantage.

Acquisition

Cards

Cash

Checks

ContactCenter

Conversion

Digital

DirectMail

Insight

Promo

Anti-fraud technology with a human touch

BY KATIE KUEHNER-HEBERT

AI and ML solutions are rooting out hidden risks, while enhancing the customer experience.

The use of artificial intelligence and machine learning in bank fraud analytics is continuing to move from reactively mitigating fraud that's already occurred to preventing fraudulent activities from actually happening—but in ways that try not to block legitimate customer transactions.

How to accomplish this? By incorporating more customer behaviors into AI/ML models—including how they might hold their cell phones and the different ways they interact with their bank—to better determine if they are the ones actually conducting transactions and other activities.

In the past, controls and technology solutions were focused mainly on developing business rules and

analytical models to identify potential high-risk transactions, says [Philippe Guiral](#), who leads [Accenture's](#) North America fraud and financial crime practice in New York City. However, these controls and solutions lack a complete view of the customer's behavior.

"It was a one-size-fits-all approach that generated a high number of false positives, creating bad experiences for customers—and also creating the need for a large fraud operations team to manage the high volume of alerts," Guiral says.

As anti-fraud technology has become more advanced and scalable, he says, some banks are now investing in a cross-product, omnichannel view of customer behavior—leveraging customer data across domains

It's critical to have a strong fraud analytics solution that can give banks a comprehensive view of a customer's identity.

KIMBERLY WHITE
LEXISNEXIS RISK SOLUTIONS



within the organization, to gain more insights of customer behavior to better assess whether any particular transaction is suspicious.

A growing number of banks are now building cases to show these solutions can not only improve fraud prevention rates, but also enhance the customer experience and be applied across additional functions—including financial crime, Know Your Customer, risk and customer intelligence—to uncover hidden risks and discover new opportunities, he says.

GETTING TO KNOW THE CUSTOMER BETTER

Indeed, it's critical to have a strong fraud analytics solution that can give banks a comprehensive view of a customer's identity and real-time insights into application activity, says [Kimberly White](#), senior director of fraud & identity at [LexisNexis Risk Solutions](#) in Alpharetta, Georgia.

"We proactively prevent fraud using a multilayered, risk-based approach employing technology solutions that incorporate identity verification and fraud analytical models, combined with multifactor authentication to help prevent fraud and improve the overall customer experience," White says.

Likewise, [FICO](#) has been using AI and ML to solve the "precision challenge" in an effort to reduce false positives, says [Liz Lasher](#), Miami-based vice president of portfolio marketing for fraud and financial crimes.

Bank strategic teams are also now converging three domains—identity management, fraud and financial crimes—to achieve economies of scale and make more contextual decisions that result in consistent customer experiences, operational efficiencies and reduced false positives, she says.



It's not always the best course of action to prevent a transaction from happening, but rather to allow the transaction to happen and then investigate after the fact.

AARTI BORKAR
IBM SECURITY

"It's not always the best course of action to prevent a transaction from happening, but rather to allow the transaction to happen and then investigate after the fact," Borkar says. "That way, they don't block transactions that are legitimate, and the investigation also gives banks details to figure out how to prevent the fraudster from attacking again."

Such investigations often happen using a broader threat response platform, she says. Additionally, insights from these incidents can also be analyzed and correlated in threat intelligence feeds, in order to prevent broader proliferation of similar incidents globally. "So fraud analytics is often a mix of proactive and reactive measures," Borkar says.

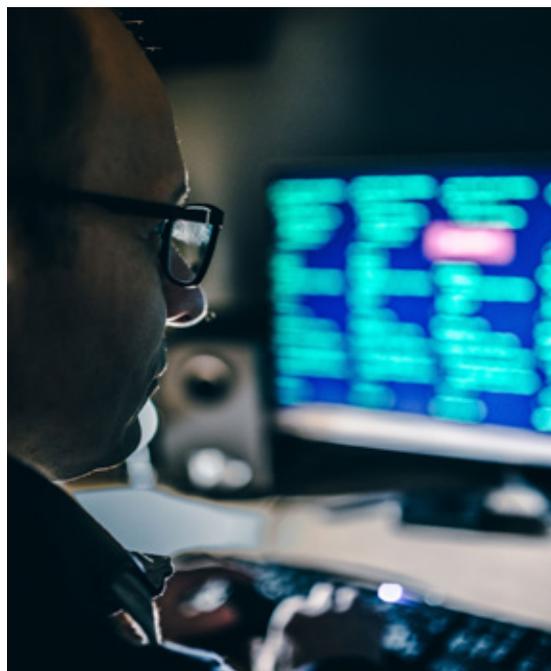
Lasher agrees, saying that while prevention is a critical goal, "mitigation is also important, as banks want

[IBM Security](#) is enhancing real-time analysis to prevent customer identities from being stolen. This effort includes employing a combination of ML models with behavioral techniques, says [Aarti Borkar](#), vice president of product and strategy, who is based in San Francisco.

"We're able to recognize patterns of behavior for users who regularly log into an application, such as a banking app, including whether they hold their mobile device horizontally or vertically, the way they type their password in a particular way and mouse movements," Borkar says. "We combine those behavior patterns with machine-learning models to build a risk model to better assess the identity of the individual using the bank app."

MITIGATING FRAUD HAS ITS PLACE, TOO

While AI and ML solutions are getting better at proactively stopping fraud, sometimes mitigating fraud is more prudent, the experts say.



to strike a balance between preventing fraud and customer experience, by lessening false positives. Banks need to establish trust and consistency with their good customers, so that they can stay the preferred brand."

While reliance on technology continues to grow, humans still play a critical role in fraud analytics, from designing AI/ML models to determining whether an activity is actually fraudulent or legitimate. One such role is building comprehensive algorithms to ensure there are no blind spots, such as not flagging fraud that has been happening in one geography but not yet in another, Borkar says.

"Humans are also needed to review analytical results to make decisions on what to do next," she says. "Finally, everyone within an organization needs to be educated on how to support fraud prevention, and follow the rules set up by their security teams." 

Katie Kuehner-Hebert has more than two decades experience writing about financial services topics that include retail and commercial banking products and services; payments systems; mergers and acquisitions; and security and fraud issues. She is based in Running Springs, California.

Security without compromise

BY JORDAN RIEK

As ATMs become more sophisticated, so must your security measures to thwart physical and online attacks.





Today's ATMs operate more like mini-branches than ever before. This means that financial institutions must ensure their devices are protected against criminals targeting them for purposes of theft, intrusion and compromise.

Establishing effective defense mechanisms, however, is just the first step. Hardened ATM security requires an institution to be aware and vigilant of new criminal schemes every day to protect its cardholders, as well as its brand.

Protecting ATMs from fraud attacks requires a blend of physical and cybersecurity measures. ATM fea-

ture functionality and operating designs continue to expand—and so does the battlefield where ATM security managers and ATM-focused criminals meet. Each new ATM feature or system brings a potential new way for criminals to learn and reverse-engineer how those mechanisms work so they can try to compromise devices.

ATTACK METHODS USED ON ATMS

A physical attack on an ATM often includes attacking the device's surrounding environment in addition to the ATM itself. Some of the ways criminals compromise the physical security of an ATM include card

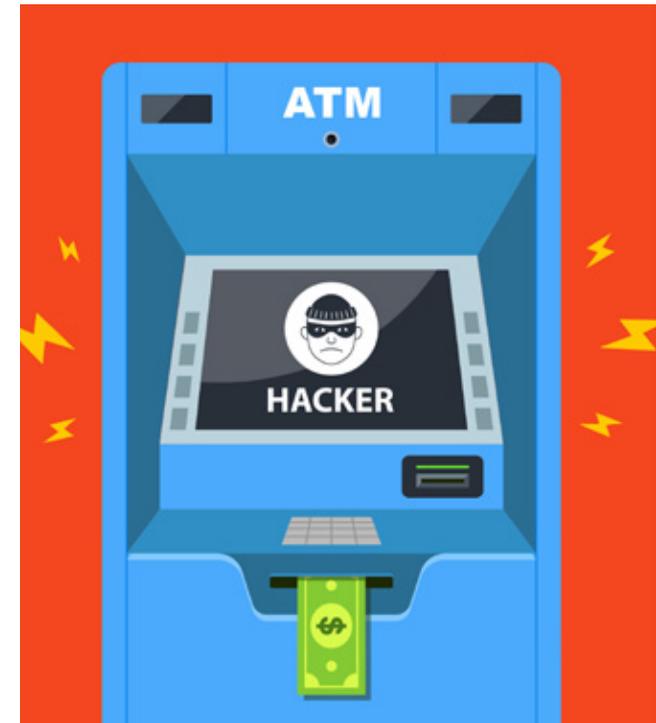
Hardened ATM security requires an institution to be aware and vigilant of new criminal schemes every day to protect its cardholders, as well as its brand.

skimmers, crowbar smash-and-grabs and other brute-force attempts to open the machine on-site or remove it to another location to open it. An institution should consider and secure the device's surrounding environment before it actually places the machine.

Cyberattacks on ATMs are those that target computer systems, applications, network and data. These include malware introduction, endoscopic attacks (used in "jackpotting" schemes), BIOS manipulation, ransomware installation and wiretapping.

These types of attacks are often the work of sophisticated criminal enterprises that might "stalk" an ATM network for some time before attacking it. They use reconnaissance to gather information about the network, device software and monitor capabilities of the ATM management system prior to launching the attack based on their findings.

Maintaining ATM security vigilance requires a combination of security acumen—regular intelligence



gathering and sharing, as well as a clear but flexible strategy for protecting both the fleet and sensitive cardholder data. First and foremost, ATM managers should think about where data resides or is transmitted and ensure its security. In addition, ATM use behaviors are generally similar, making it relatively easy to detect potential fraud using analysis tools.

PHYSICAL SECURITY CHECKLIST

- » *Review the ATM's perimeter for potential vulnerabilities and consider how a criminal might physically compromise a machine. Establish a perimeter security plan before installing a device. Look for items like bolting of the base, car approach paths and visibility.*

- » Educate in-store and on-site personnel to validate all ATM service personnel, establish a reporting protocol for reporting suspicious behavior and periodically check machines for compromised components.
- » Give cardholders an avenue to report a potentially compromised machine or suspicious activity.
- » Check cameras and other security devices regularly to ensure they are in good working order.
- » Install GPS tracking devices within both the cash and the device itself.

Participating and sharing information in security-focused peer and trade groups [...] help to keep ATM security managers informed of potential schemes.

CYBERSECURITY CHECKLIST

- » Harden the ATM by:
 - Encrypting all hard drives connected to the ATM
 - Securing communications with the ATM's dispenser
 - Disabling unnecessary operating system functions, ports and connections
 - Installing the latest patches for the ATM model
 - Enabling MACing between the ATM and processing switch
- » Enable multifactor authentication for all ATM software/system/network administrators; review audit logs regularly.
- » Segregate the ATM channel from the environment as much as possible.

- » Secure ATM communications using encrypted links wherever possible.
- » Undertake periodic vulnerability tests and modify software/hardware configurations as required.
- » Maintain your awareness of updated threat intelligence against the ATM channel.

BEST PRACTICES FOR PROTECTING ATMS

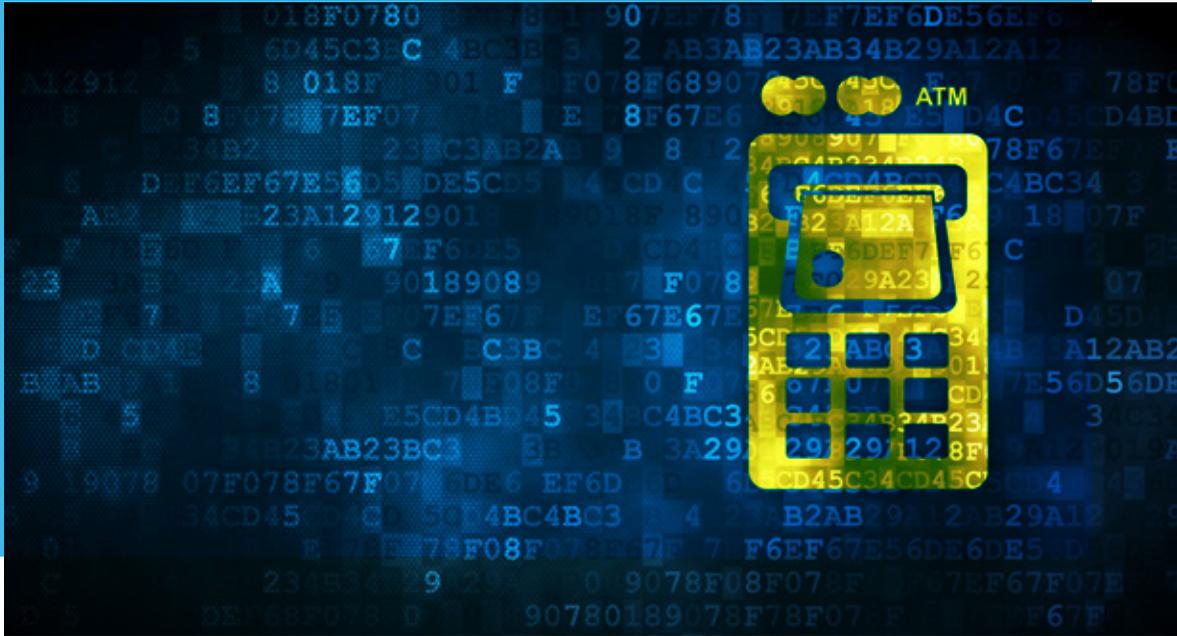
Based on our deep knowledge of ATM security and our experiences with customers around the world, we recommend all financial institutions consider incorporating some or all of these best practices into their ATM security protocols:

- » **Share information:** Gather and share information freely, which will help make the ATM fleet and the larger market a



safer environment for all stakeholders. Participating and sharing information in security-focused peer and trade groups, as well as monitoring warnings and updates from organizations like the Secret Service, the FBI and card networks help to keep ATM security managers informed of potential schemes before an institution may become a target.

- » **Risk analysis:** Regularly analyze physical and cyber concerns, and based on the findings, along with intelligence gathered from various sources, appropriately set up the device fleet to defend against them.
- » **Physical controls:** Place defined controls on the device's physical security and monitor with a consistent, standardized control approach and protocols. Incorporating static



controls, or “set-and-forget” strategies, don’t work. Criminals innovate and organizations must keep up by enabling flexible security controls through the use of their risk analysis mechanism.

» **Staff education:** Whether it is the staff in-store, in the branch or in the back office, ensure the team maintains an increased awareness and knowledge of themselves as targets because criminals may well be looking to gain access to the ATM fleet, its network, software and cardholder data.

their hands and knees and look at the world from an infant’s point of view. Assessing ATM fraud and security risks should be done in a similar manner.

In other words, put yourself in the mindset of a criminal and ask, “How could I compromise this device?” The answers to this question can help drive an ATM fraud prevention platform that stays current and protects your fleet for years to come. ↩

Jordan Riek is senior vice president, information security, at Houston-based [Cardtronics](#), the world’s largest non-bank ATM operator and a leading provider of fully integrated ATM and financial kiosk products and services.

ATM fraud is preventable with vigilance and consistent best practices. It’s not unlike the way new parents are instructed to baby-proof their house: get down on



Strategic Certainty In an Uncertain World

Cardtronics provides stable, secure, high-availability ATM services built on a one-of-a-kind network. In an age defined by uncertainty, your self-service channel should never be in question. On-demand ATM services from Cardtronics... your ATM challenge solved.



ATM BRANDING
Our prime locations, your brand experience.



ATM MANAGED SERVICES
Your ATMs driven by our ATM operating expertise.



ALLPOINT NETWORK
Surcharge-free withdrawals and deposits. Everywhere.

Better verification with less friction

BY CHAD DAVIS

Ramping up your authentication standards doesn't have to mean sacrificing customer experience.





Organized crime rings have been targeting the banking industry with sophisticated and automated online attacks for several years. They now account for most fraud losses and are able to spread their activities across multiple jurisdictions, which makes stopping them very difficult for law enforcement.

Attackers take an ever-evolving variety of approaches, including phishing, social engineering and planting

client-side malware. The goal is often to obtain credentials, which will later be used in large-scale campaigns such as credential stuffing and fake account fraud. Because it can provide a high rate of return, credential stuffing is one of the most common types of attacks in the banking industry.

Credential stuffing, which involves using automated systems to access user accounts with stolen usernames and passwords, has become a common tactic

in recent years for these criminal organizations, who have adopted increasingly sophisticated methods to circumvent the traditional countermeasures deployed by financial services institutions.

In particular, hackers are deepening their capabilities around imitating legitimate users. They use the same tools that users do, automating production browsers like Chrome, Firefox and Safari, and proxying through residential IP addresses. By emulating human traffic and behavior, they can bypass lower-friction defenses, MFA gates and rate limits to take over accounts, crack cards or steal data. Malware sits resident on victims' computers, scraping their credentials and delivering them back to fraud marketplaces.

Intelligent phishing proxies, which seamlessly skin over a legitimate website and then intercept the traffic that goes through, are also on the rise. Users are fooled into thinking they are logging in to their email account or online banking platform, since the web page looks the same. In reality, a cybercriminal is stealing their credentials.

In response to this growing threat, banking and financial services organizations have been drastically stepping up their authentication efforts.

"Five years ago, it was not uncommon to find that the only way an organization was authenticating users was through a single login form on a webpage. Fraudsters had free rein past that point," says [Jarrod Overson](#), director of engineering at [Shape Security](#). "Now, multifactor authentication is commonplace, we're seeing more magic links and then even past the first login gate, companies are increasingly risk-scoring each user's behavior to assess whether they need to be authenticated further."

SECURITY ≠ FRICTION

While institutions have added more security to their authentication, they've also added more friction to

Five years ago, it was not uncommon to find that the only way an organization was authenticating users was through a single login form on a webpage.

JARROD OVERSON
SHAPE SECURITY

the user experience. CAPTCHA tests are frequently derided on social media networks as a painful process for proving human identity, while even multifactor authentication causes a significant level of disruption to a customer journey, particularly if the user doesn't have their smartphone in hand.

This additional friction comes at a time when IT, marketing and sales departments are already eroding the seamlessness of their digital channels, whether it be through pop-ups urging people to accept privacy policies, user session tracking or customer journey mapping. When companies apply additional security layers to those applications, it can easily feel like they are imposing dramatically more friction than is necessary.

These organizations may believe they are improving security defenses, but they are likely overlooking the



automated and manual (human-driven) fraud, allowing for new tactics to mitigate risk without the consumer discomfort, including:

- » **Analyzing device, network and environment** signals to uncover anomalous behavior, such as login success rates, devices per user, users per device and variations in IP addresses, user agents and session data
- » **Detecting human behavior** using artificial intelligence (AI) and machine learning (ML) based on organizations with similar attack profiles and risk surfaces
- » **Leveraging historical fraud files** to further train ML algorithms on the types of attacks that are common for a particular organization

“Companies need to architect a better balance between security and user experience,” Overson says. “Attackers have started with basic tools that did a simple job and have evolved over the last five years to more convincingly look generically human. Now they are moving towards more aggressively looking specifically human. As defenses improved to block questionable behavior, attackers responded by creating tools to exploit and imitate individual users with all their nuances.”

Chad Davis is a senior banking marketing manager at Seattle-based **F5**. A longer version of this article originally appeared in the *Future of Authentication* special report published by *Raconteur* in 2020.

downstream damage they are causing to their account holder's experience. Too much friction can negatively impact account creation, logins and conversion rates. More worryingly, they may soon find their social media pages blighted by poor reviews that damage their brand and reputation, and ultimately this can affect sales.

Minimizing the impact that increased security measures have on the user experience can be accomplished, but rarely through traditional means. Banks and credit unions should look to newer technologies aimed at stopping criminal organizations' use of both



FINANCIAL FRAUD RISING: KEY STRATEGIES TO COMBAT ATO ATTACKS

Most fraud losses are the work of organized crime rings. Learn how financial institution risk execs are protecting themselves from the increasing volume of account takeover (ATO) attacks.

[Find ways to fight back >](#)

Past Issues

DECEMBER 2020

[Making a bigger impact in 2021 »](#)

NOVEMBER 2020

[Building a more diverse, equitable and inclusive workforce »](#)

OCTOBER 2020

[Marketing today: Strong bonds, strong brands »](#)

SEPTEMBER 2020

[Data and analytics: Better decisions by the numbers »](#)

AUGUST 2020

[Lenders going digital to deal with COVID-19 »](#)

BAI Banking Strategies
Executive Report

**Taking the fight to
the fraudsters**

January 2021



STAY TUNED FOR

February 2021

DIGITAL TRANSFORMATION:
OPERATIONS

March 2021

BANK BRANCH EVOLUTION

