# Special Report: Fraud Prevention

*Credit Union Management*

APRIL 2020

## COLLABORATIVE SECURITY

Sharing information can help CUs fight off attacks.

PLUS

# Collaborative *Security*

SHARING INFORMATION CAN HELP CUs FIGHT OFF ATTACKS.

**BY STEPHANIE SCHWENN SEBRING**

Fraudsters continually reinvent themselves. Unfortunately, for financial institutions and the public, they do so with vigor, intelligence and expertise. For this month's special report, we dug into best practices in fraud prevention, including the role of collaboration.

## JOIN FORCES

Strength in numbers of fraud fighters pooling resources to net criminals works well in the fight against localized fraud types, such as phishing or skimming.

"Credit unions are one of the most collaborative segments in the payments industry, and that's a huge benefit to leverage," observes Eric Kraus, business executive/fraud, risk and compliance solutions for FIS (*fisglobal.com*), a CUES Supplier member based in St. Petersburg, Florida. "There's a member-driven purpose and openness to learning from each other's successes and challenges. Often, an impacted credit union within a targeted geographic threat vector will reach out to others in the immediate area to provide early fraud warnings.

"For example, a couple of years ago, a group of organized criminals was hitting ATMs along a highway corridor on the East Coast, and several credit unions sounded the alarm proactively. We're also seeing more data-sharing related to areas like negative customer databases to combat fraudulent account openings."

FIS empowers collaboration among its clients through advisory councils and focus groups, annually bringing credit unions of all sizes together for strategic planning.

"These sessions include fraud and risk topics that focus on industry trends, best practice fundamentals, and emerging innovations to protect against threats," says Kraus. FIS also hosts a quarterly fraud forum, where financial institutions from across the country come together to learn from fraud and risk experts, of emerging trends, and dive into key industry performance metrics. Credit unions have an opportunity to ask questions and seek guidance from the assembled experts and other participating credit unions.

Recent topics included a focus on emerging fraud trends in P2P and contactless payments.

"First-party fraud continues to plague the industry," says Kraus. Card-not-present and ATM fraud trends are two other areas of focus.

This continual learning helps institutions from becoming too passive. "Take a defensive posture and understand your weaknesses," he adds. "Assume you're continually under threat because you more than likely are. Have a proactive plan so that you can quickly pivot if fraud occurs and your staff knows what to do."

## RESPONDING TO FRAUDSTERS

"Since the adoption of EMV, credit unions have shifted their focus to the more innovative tactics of fraudsters not seen before," notes Ashley Town, director/fraud services for CUES Supplier member CO-OP Financial Services (*co-opfs.org*), Rancho Cucamonga, California. "They also engage each other when new trends occur and work collectively on solutions for prevention." She notes that CO-OP Financial Services hosts a monthly fraud webinar, Fraud Buzz, to assist. In these sessions, credit union participants and guest speakers from across the U.S. discuss industry fraud trends.

Local fraud collaboration forums are also extremely advantageous. "Often, we see fraudsters attack specific geographic areas utilizing the same fraud pattern," says Town. "Here, having a network of local fraud contacts allows for proactive communication for those likely to be impacted and timely collaboration shortly after a fraud trend arises."

A credit union doesn't want to wait for a monthly call to notify industry peers, she adds. Instead, she recommends participating in a virtual fraud forum, such as an email group or online bulletin board "to alert colleagues and discuss trends promptly, allowing others to be on the lookout."

## WIDENING THE CIRCLE

Liz Little, fraud consultant for CUES Supplier member SHAZAM® (*shazam.net*), a debit and credit payment processor based in Des Moines, Iowa, sees the best outcomes when information is proactively

### MORE ON SECURITY

Tech Time: How to Build a Proactive Data Security Plan (*cumanagement.com/0220techtime*)

Why Security Awareness Matters (*cumanagement.com/011520skybox*)

Don't Be the Weakest Link (*cumanagement.com/0120weakest*)

First Line of Defense™ (*cues.org/firstline*)

shared. This doesn't mean proprietary or internal procedures, but rather spotted trends or fraud. "This includes sharing with us (or your payments processor) any compromised card data," she says. "We, in turn, share this with all members without naming the reporting financial institution."

She also recommends a point person join a community fraud group comprised of law enforcement, postmaster generals, attorney generals and other key players. "Here, credit unions can share and glean information and stay united as an industry, pertinent because of rising fintech competitors that can take advantage of perceived weaknesses" and quickly develop products and services to serve (and potentially steal away) credit unions' members.

Another key stakeholder is the member, notes David McClurg, product manager/digital for Shazam. "Consider that a typical credit union spends about 80% of its time talking to members about products and 20% on how it protects member data. By sharing your story and stressing security innovation with members, you create brand affinity."

Kraus also sees some of the most vigorous collaboration in CUs' member education efforts. "We've seen credit unions partner to provide consumer tips on phishing schemes, social engineering scams or tips on practicing strong cyber hygiene. The more you can educate and empower your members, the more likely they can help in the fight against fraud."

Fraud prevention products—such as Brella™ (formerly known as SHAZAM® BOLT$™), SHAZAM's card control app (*tinyurl.com/shazbrella*)—also can bring members further into the fraud prevention circle. Using the member's smartphone, Brella adds a layer of protection to card transactions by notifying the cardholder of potentially fraudulent activity.

"These products also remind members how hard you're working for them, while transactions are monitored from a self-protection perspective, providing data-rich insights, which help the institution to prevent fraud at a macro level," stresses McClurg.

Onsite crisis management training further promotes collaboration within the broader community. "In our skimming and card cloning presentation, for example, we use actual photos and videos to show how thieves set up these devices and steal from cardholders," adds Little. "A live demonstration encourages interaction with community partners ... including business owners and city officials."

## TAPPING EXPERTISE

Fraudster sophistication is escalating, and the concept of collaboration needs to take on ever more meaning, says Jack Lynch, chief risk officer for CUESolutions provider PSCU (*pscu.com*), St. Petersburg, Florida, and president of CU Recovery (*curecovery.com*).

"Only by working collectively can we combat movements on the dark web, such as the move from counterfeit card information to selling personal information, and other efforts by thieves," Lynch explains. "It's the combination of technology and data as well as our Linked Analysis product (*tinyurl.com/psculinkedanalysis*) that makes a difference."

He notes that PSCU's contact center can detect a fraudster via voice printing. Here, an attempt is made to gather information from one credit union's interaction with a suspected fraudster, then link it to that same phone number to gain information from another credit union.

"Without this data collaboration, a pattern would not be detected until it was too late to avoid a loss," explains Lynch. Analyzing many points of data (including contact center, interactive voice response, online banking and card transactions), aids fraud detection.

There is also a need to tear down siloes internally, stresses Lynch. "Realize everyone within the credit union plays a role, from the front line to lending and new accounts. Develop a plan that incorporates all people and channels holistically—so collaboration is layered, and solutions are reviewed for the right fit."

Another networking avenue is the members' area of PSCU's website, where member credit unions and the online community can follow fraud trends, attend monthly fraud webinars and pose questions to the community in real time.

It's a process. And ultimately, says Lynch, technology can't save any organization from a weak link in its system. "Collaboration includes people, processes and technology, and with a chink in one, all are susceptible. A credit union must ensure all parts are working together, using the same processes to prevent fraud."

## EDUCATING STAFF

Well-informed employees are another advocate in the fight against fraud.

"Knowledge is power," says Cynthia L. Carter, lead compliance officer for training company TRC Interactive, Inc. (*trcinteractive.com*), Harrisburg, Pennsylvania. "It involves many avenues of training—getting information to the people who can make a difference not only to their institution but also the people they serve."

TRC Interactive provides various levels of training to financial institutions in the U.S., including its staff fraud training program (First Line of Defense™, *cues.org/firstline*). "Ten interactive scenarios are provided quarterly to clients" through the program, explains Carter. "Using real-life scenarios, such as check-cashing or deposits with account screens and sample items processed, the front-line employee goes through the transaction as if the person were in front of them."

Using interactive modules (not dialogue reading), the program illustrates how integral collaboration is to the process. "In any given week, we might have hundreds of conversations with financial institutions," notes Carter. "Customers contact us to ask that we highlight a specific fraud situation they have experienced. While not traditional collaboration, a teller in Pennsylvania could be working his or her way through an interactive training scenario a teller in Texas experienced last month. While many resources are used to create scenarios, real-world examples are some of the most valuable."

Carter has also learned it's a mistake to see fraud as a once-and-done training situation: "Ensure information is in the hands of the people who interact with your members every day. Fraudsters are not waiting for a new idea to come to them. Financial institutions need to do everything they can to protect their institutions and the people who rely on them for their financial well-being."

**Stephanie Schwenn Sebring** *established and managed the marketing departments for three CUs and served in mentorship roles before launching her business. As owner of Fab Prose & Professional Writing, she assists CUs, industry suppliers and any company wanting great content and a clear brand voice. Follow her on Twitter @fabprose.*

# Q&A: Safely Sharing *Fraud-Related Information*

CUES member David Stephen Baker, operations & security manager for $700 million Connex Credit Union (*connexcu.org*), North Haven, Connecticut, shares his thoughts on how credit unions can best support fraud investigations while still complying with the rules protecting members' private information.

**Q: What information can CUs share when it comes to fraud prevention?**

In an ideal world, CUs could freely communicate with each other to prevent potential losses. However, a list of legal restrictions—such as the Gramm-Leach-Bliley Act and contractual obligations with card industry vendors—protects members' private information from being shared without their consent or a warrant issued by the government in support of the administration of justice.

**Q: What if organizations ask for information that could be considered "private"?**

The fraud prevention information that CUs share amongst themselves, either directly or through a common vendor, is typically high level and couldn't be used to identify a specific member. For example, a CU might share its observation that a known fraud technique is making a comeback—or that it thinks it has spotted a new scheme being perpetrated in the marketplace. In contrast, law enforcement agencies may request specific information about a particular member or members. And that's where credit unions need to be especially knowledgeable and cautious.

"Sharing comes with certain risks, such as breaking regulations/policy, reputation risk and frivolous litigation risk," Baker says. "Each institution should determine the level of risk it is willing to accept. Communicating ... information (related to fraud investigation) should include a minimal sharing of details."

**Q: How does Connex CU respond to requests from law enforcement?**

"We have specific employees who can communicate about fraud," Baker says. When law enforcement agents call, "these individuals can always safely say, 'Tell me what you think happened, and I'll tell you if you should get a warrant and can start getting information compiled and retained for you.'" Connex CU employees will rarely begin the process of releasing member information without first having several people review the details and reach a consensus about what should be done before they relay that information to an executive, he adds.

"If law enforcement requires information to hold a suspect and is willing to send an email that dictates some type of emergency, we will share enough redacted information to hold a suspect and convince a judge to request more information through the proper channels," he continues. "When another financial institution or the police department calls because one of our members may have done something unscrupulous and there is reasonable doubt, we can either tell them that, based on the information they've provided, obtaining a warrant would be the best next step, or let them know that there's nothing available to help them.

"We typically verify or deny extremely detailed queries or accusations about members' activities," Baker says. "But this only occurs after extensive verifications of the inquiry's source, and we receive detailed information on the incident."

**Q: What are some best practices for deciding whether a request for information is on the up and up?**

"At Connex, we're far more receptive to organizations calling with verifiable International Association of Financial Crimes Investigators (*iafci.org*) credentials," explains Baker. IACFI members include retail loss prevention and financial organizations, fraud investigators, and members of federal, state and local law enforcement agencies. They are specifically trained in financial industry fraud and the information-sharing guidelines. They are fully experienced in what can be communicated and the limitations of sharing before a warrant is required.

Baker suggests joining IAFCI. "It is an amazing group of industry leaders who understand your limits (as a credit union) and can assist with identifying flexibility in the law on specific situations."

Baker also notes that Connex CU prioritizes information-sharing in cases with a high degree of certainty a crime has occurred, causing a loss.

**Q: What other tips do you have for doing a good job with all of this?**

To effectively fight fraud, Baker suggests partnering with a much larger financial institution. For example, Connex CU has a good fraud-prevention relationship with a large regional institution.

"Things show up on our screens long before they hit the radar at a larger institution," he says. "Larger institutions, meanwhile, have the resources to lean on officials and the payment card industry."

Also, consider forming a weekly review committee for fraud and claim responses. "This committee should include ... multiple disciplines within your credit union," advises Baker. "This review helps to eliminate liability concerns and potential delays from placing weighty decisions on one individual. It also allows for fraud trends, losses, exceptions to policy and responses to be communicated to executives, who can ensure decisions are in line with the credit union's policies."

Baker also suggests making sure your CU has a blanket indemnification and liability waiver specific to fraudulent activity communications—as well as knowledgeable legal and compliance advisors on speed-dial. Plus, he says, "Remember, the front line often sees emerging fraud first, so ensure they are properly trained to identify and respond to fraud."

# First Line of Defense™

## New! Low Cost, Online Fraud Prevention Training

First Line of Defense, from the experts at TRC Interactive, is a virtual training system designed to help your employees detect the latest fraud schemes. Subscribe today, and enjoy these features:

- Quarterly lessons with 10 to 12 scenarios, based on real-life fraud attempts
- Simulated transaction screens and documents with your CU's routing number and MCIS
- Learners discover how much money would have been saved or lost based on the decisions they make—a great way to keep track of ROI

Don't wait—stopping even one instance of fraud can save your credit union thousands! Learn more at **cues.org/FirstLine**.

CUES
POTENTIAL, REALIZED.™

PSCU

# From Detection to Predictions: Combatting Fraud with Machine Learning

*By PSCU*

Since it was introduced in 2004, internet users have been fascinated with the "magic" of Google's search predictor. In reality, there is very little magic involved, but rather a machine-learned ability to find complex patterns in data streams that generate actionable predictions in real time.

The latest risk intelligence method for combating fraud operates on a similar premise. When used in conjunction with human-curated adjustments, it creates a mechanism for not only identifying fraud across multiple channels, but also for predicting it.

## From Past to Present

Many organizations initially detected fraud by viewing and analyzing activity logs one platform at a time. While this worked as intended, it could not compete with the newest wave of fraudsters who are skilled at utilizing multiple channels to accomplish a successful fraud scheme. Many of the older fraud detection systems managed to prevent fraudsters from making their final cash-outs, but they were not able to stop the fraudsters from committing fraud in the first place.

## Moving Beyond Detection to Prediction

Linked Analysis is PSCU's proprietary approach to intercepting and predicting fraud through the combined use of machine learning, anomaly analysis, phone printing technology, data analytics and human intelligence. Utilizing a framework primarily relied upon by the IT world, Linked Analysis uses a consortium of data – including phone calls, online banking logins, authorization data, etc. – to monitor connected events across multiple channels, and predict fraud before it happens. By analyzing data holistically, across multiple channels, Linked Analysis can identify and intercept malicious patterns of fraud.


While most credit unions have a plan in place for combating fraud, the real differentiators for Linked Analysis are scalability and reach. With Linked Analysis, PSCU's fraud intelligence teams can analyze data at scale across multiple channels and create alerts about events as they happen – or even before they happen. Consortium data is a key component of Linked Analysis' methodology, where collected metadata related to a fraudulent event is combined with metadata from third-party sources. Intelligence gathered from a variety of sources, including 1,500 PSCU Owner credit unions, is the key to the success of Linked Analysis. Over the past 12 months, PSCU's average save per cardholder was nearly $6,000.

## The Science Behind Fraud Prediction

Machine Learning (ML) is a trending technology in many industries. Just as some companies use it to serve up song suggestions, financial institutions use it to secure accounts and proactively stop fraud. It is also a critical component of Linked Analysis, as ML contributes to the agility needed to continually monitor re-occurrences in fraudulent behavior and analyze information down to the cardholder, merchant or any other individual data element level. In fact, the ML functionality behind PSCU's Linked Analysis can monitor nearly two million unique merchants on any given day and identify anomalies that may be tied to other fraudulent transactions.

A majority of the accounts that PSCU secures using the ML capabilities of Linked Analysis are identified as fraudulent before the fraud actually occurs. This makes for a better credit union member experience, as no money is lost and the credit union does not have to recover funds.

## A Fraud-Stopping Combination

As fraudsters continue to find new ways to commit their crimes, more sophisticated fraud solutions must be implemented as part of credit unions' larger crime compliance initiatives. Delivering a safe and seamless user experience is crucial to keeping credit unions competitive and members happy. It may be a new digital world filled with highly skilled adversaries, but reliable risk management is not out of reach – and PSCU's Linked Analysis methodology enables credit unions to meet force with force via shared data on the threats we face collectively.

To learn more, visit pscu.com.

# Strength in Numbers.

## Stand Safe With Us.

**Your Possibilities Delivered.™**

In the past year, PSCU has saved credit unions more than $277 million in potential fraud dollars, continuing our 40-year reputation as an industry leader in risk management. The latest technology, custom fraud mitigation rules, cross-network analytics, and proactive monitoring keep us present at every point of attack. That way, you don't have to be.

Payments ▪ Risk Management ▪ Digital Banking ▪ Analytics ▪ Loyalty
Mobile ▪ 24/7/365 Contact Center ▪ Strategic Consulting

PSCU

pscu.com
844.367.7728

# New Tech Brings *Revenue & Risk*

FUNDAMENTALS KEY IN CREDIT UNIONS' BATTLE AGAINST FRAUD.

**BY ERIC KRAUS**

The rapid shift of payments to digital channels introduces new opportunities to satisfy members while increasing credit union revenues and profits, but it also presents new risks. Fraudsters are becoming shrewder at creating entry points for their attacks.

## FOUR TYPES OF FRAUD

Fraud is moving toward earlier strikes in a member's tenure. Credit unions should be on the alert for four types of increasing or emerging fraud.

While **card-not-present fraud** isn't new, it is now originating from mobile channels as consumers shift more of their transactions to e-commerce. In fact, about 50% of CNP fraud is now emanating from mobile devices.

**P2P "fast funds" fraud** is gaining traction as fraudsters compromise new accounts and use stolen personal account numbers, debit cards or credit cards to register on a P2P application. For example, fraudsters might open a new account with personal or stolen credentials or take over an existing account. They could then fund a money transfer with the compromised cards loaded into the digital app and send payment to a "partner in crime" or to themselves.

**First-party fraud** is defined as fraud committed by customers who have no intention of paying. Some first-party fraudsters are simply run-of-the-mill deadbeats—for example, they may continuously submit fraud claims, often for less than the amount at which claims trigger a dispute.

A more sophisticated and surging type of first-party fraud is synthetic identity fraud. McKinsey reports (*tinyurl.com/mckinidfraud*) that synthetic identity fraud is the fastest-growing type of financial crime in the U.S. The explosion of personally identifiable information available on the dark web provides a vast amount of fodder for thieves to use in cobbling together synthetic identities. These fraudsters can work over the course of several months to maximize their credit lines and optimize their paybacks before they disappear.

**Contactless card fraud**—often perpetrated when cardholders lose their physical cards and fraudsters find and use them—has also started to grow. Contactless fraud is replacing double-dipping, the practice of getting a product delivered *and* getting a refund for the same purchase. Currently, the rate of contactless fraud is extremely low, according to Visa (*visa.com*), but cases of sophisticated crime rings manipulating the point of sale are occurring. Wily criminals set up a merchant account for fraudulent use and steal a point-of-sale device outright or infect the POS with malware, allowing them to manipulate transmissions.

## ADDRESS THE FUNDAMENTALS

Credit unions should take advantage of the opportunities provided by new digital technologies—for example, adopting contactless cards to drive interchange revenue. But in the race to keep pace, it's easy to overlook "the devil in the details."

To ensure your guardrails are in place:

- Patch systems upon releases.
- Deploy network segmentation to contain threats.
- Adopt and practice crisis management.
- Review backup transaction processing rules.
- Review card parameters, limits and velocity controls.
- Employ cyber monitoring—for example, retain a forensics security company to monitor the dark web and the internet for information fraudsters can use for social media spoofing, enticing consumers to click on an infected link or provide additional personal information.
- Maintain PCI DSS compliance.
- Educate members about how to recognize phishing and social engineering schemes.
- Let members know how you will contact them, what you will ask and what you will never ask.
- Give members card controls and real-time alerts.
- Collaborate with other credit unions to keep abreast of fraudsters and their schemes.

Today's fraudsters are both smart and active in coming up with new schemes. In response, credit unions need to be even smarter and more active with their fraud prevention efforts. Be sure to regularly monitor trends that might affect your organization or your members and respond by updating your fraud-prevention efforts.

Eric Kraus *is VP/GM of fraud, risk and compliance solutions for CUES Supplier member FIS (*fisglobal.com*), Jacksonville, Florida.*

## MORE FROM FIS ON SECURITY

Taming the Digital Risk Tiger *(cumanagement.com/091119skybox)*

Five Tactics for a Credit Union's Fight Against Fraud *(cumanagement.com/0519five)*

# LET'S ADVANCE THE MEMBER EXPERIENCE TOGETHER.

FIS is advancing credit unions and the member experience. Our history of partnership with credit unions and in-depth knowledge of the credit union marketplace spans over 40 years. We are dedicated to creating best-in-class credit union and member experiences through a direct, trusted partnership that delivers shared success.

**www.fisglobal.com/cu**

SHAZAM®

# FIGHTING FRAUD: AN INSIDE-OUT APPROACH

Fraud continues to be a major risk and a serious pain point for credit unions. It's a dark, relentless and multibillion industry in the U.S., threatening your members and you.

While the technologies to fight fraud are improving, so are the fraudsters. Today's fraudsters aren't amateur hackers. Fraud is being carried out by organized criminal groups, domestic and foreign.

It's an ongoing battle, and it's one we must fight on several fronts. SHAZAM advocates a more holistic approach to fighting fraud.

## LOOK INSIDE YOUR OWN WALLS

- Review and tune your daily limit settings regularly.

  It sounds simple, but many times, fraud happens within the daily limit. If you're reluctant to limit your cardholders across the board, keep in mind that each card can be customized with a different limit according to use. Cards used for business purposes, or people who travel frequently, may warrant a higher limit than regular use cardholders. Keeping daily thresholds lower, yet reasonable, can prevent large losses for you while minimizing inconvenience to your members.

- Use artificial intelligence to help your credit union detect and block fraud.

  SHAZAM's fraud management services are powered by FICO® Falcon®. Our clients rely on our system to learn their customers' habits and spending patterns to identify potentially fraudulent purchases in real time.

  We've counseled our clients to block transactions from certain countries or states. That has significantly reduced their fraud. Identifying specific dollar amounts that fraudsters are using to test your defenses, or specific merchants the fraudsters use to try to extract money from your members' accounts can be an effective line of defense.

## EMPOWER CARDHOLDERS

Your members can be fraud fighters, battling on the front line against fraud. But they must be informed and aware. And, they need the tools to do the job.

- SHAZAM provides clients with simple, effective messaging to share with cardholders so they know what to look for when using a card at an ATM, inside a business or at an automated fuel pump. This multiplies the number of eyes looking for signs of compromise.

- Allow cardholders to set their own alerts or blocks by putting a mobile app like Brella™ (formerly known as SHAZAM® BOLT$™) in their fraud-fighting hands. Cardholders receive immediate alerts to potentially fraudulent activity via email and / or text message. It's an added layer of protection with convenience, speed, and security all in one app.

- Remind your members of best practices, like using reputable merchants, secure online sites, and never, ever giving sensitive information by phone, email, or online.

- When you send out a new card, include clear activation instructions. Once the card is active, be sure your processor is verifying expiration dates on transactions. Your processor should also have a set of specialized notifications for online, out-of-town, or larger purchases so they can be approved quickly. Encourage your members to notify you about pending large purchases to avoid declines.

## BUILDING COMMUNITY NETWORKS AGAINST FRAUD

- Create a community of fraud fighters.

  Engage your small business members, merchants, law enforcement and even lawmakers in this fight. When merchants know what to look for, they can help stop fraud at the point of sale. When law enforcement knows what they are looking for, they'll know how to respond.

- Host a community fraud forum, invite these fraud-fighting partners together for a discussion on how to battle fraud.

- Tap into your state and national associations to see what's being done at these levels in the fraud fight.

## WHAT'S SHAZAM DOING?

- SHAZAM engages with policymakers at the state and federal levels. We advocate for changes that will lead to an overarching set of security standards. Mutually agreed upon, third party standards will lead to better, stronger user transaction authentication all along the way, from the merchant, to the network, ending with you, the card issuer.

- We've consulted with state lawmakers nationwide to help craft legislation with stiff penalties for crimes like skimming and card cloning. When stronger penalties are in place, criminals know there'll be consequences if they're caught.

Fighting fraud is a group effort. No single approach will defeat fraud, but if we take a layered approach, starting inside and working out into the community, we'll be miles — and dollars — ahead.

# EXPERTISE.
# GUIDANCE.
# VALUE.

SHAZAM Secure® provides a portfolio of information security analysis and risk mitigation services so you can pick and choose what's right for your institution.

Our team specializes in risk, regulatory, ACH and IT exams; cybersecurity and technical security; crisis management and social engineering.

## ADVANCE WITH THE RIGHT PARTNER.

SHAZAM®

6700 Pioneer Pkwy / Johnston, IA 50131
855-314-1212 / shazam.net /