BAI POWERING SMART DECISIONS.®

Combating the latest security and fraud threats

A BAI SPECIAL REPORT PRESENTED BY ALKAMI TECHNOLOGY

LETTER FROM THE EDITOR

BY RACHEL KONING BEALS

Taking on fraud demands a nimble defense

Perhaps the most confounding truth about the fraud fight is that financial institutions and their customers can be equally vulnerable at both ends of the technology spectrum.

Paper check fraud is rising sharply, by FinCen measures, via outright mail theft and digital manipulation. Forgery techniques and ink itself are more sophisticated. And then at the automated end of the tech spectrum, fortification must constantly adapt because bad actors will exploit artificial intelligence (AI) as it becomes more mainstream. Fraudsters might emulate another's voice or likeness to fool biometric authenticators, for instance.

For certain, fraud risk and its solutions touch all aspects of banking: front, middle and back office. The expert panel we've gathered for this **BAI Special Report: Combating the latest security and fraud threats**, approaches our topic from varied backgrounds but is united in a goal to deliver a safer, more satisfying banking experience for retail, SMB and commercial customers.

According to at least one practitioner we interviewed, industry fraud sensitivity has shifted recently. Fraud versus friction has always been a delicate balance. Seamless transactions for the customer took precedence, although preferably not at the expense of creating easy access for the fraudster. Yet even with said safeguards, the system historically tilted in favor of customer ease. And now? Says a panelist: "The trend is stronger measures to reduce fraud and provide tailored solutions for account holders with differing security needs and risks."

Customers presently seem to prefer reassurance of safety. They don't want hassle, but they are soothed when the communication around fraud measures is clear. Trust is currency.

Other key takeaways in our report:

- *The first line of defense is now more dynamic and collaborative with digital functions increasingly responsible for customer experience and the innovation of products and services.*
- *Neobanks and sponsor banks are being asked by regulators to increase scrutiny of first- and second-line fraud controls.*
- *A multilayered approach can tackle fraud challenges from many directions, including putting in place improved network security, strong password tools and dynamically evolving authentication solutions.*
- *Scaling and sharing uniform fraud practices across institutions, even competitors, could reduce gaps and speed up collective reaction to incidents, benefiting consumer confidence.*

We know you'll find even more valuable insight within.

Rachel Koning Beals is Senior Editor at BAI.

CONTENTS

Dynamic fraud controls: A new way of looking at banking's three lines of defense

Ken Allen
Industry Consultant

Page 3

Banks must redouble vigilance with fraud threats from all directions

Dianne S. Walker
First Horizon Bank

Page 6

Financial services organizations increasingly look for stronger, tailored solutions to fight fraud

Brad Cranford
Alkami Technology

Page 9

Tapping a variety of tactics to thwart fraudsters–from employee education to increasing customer awareness

Casey Morgan
Commerce Bank

Page 12

Dynamic fraud controls: A new way of looking at banking's three lines of defense

Q&A WITH **KEN ALLEN, INDUSTRY CONSULTANT**

KEN ALLEN HAS BEEN an executive in the financial services and technology space for more than 20 years, heavily focused on leading the verification, fraud and compliance areas of companies. His operational experience includes working at Tier 1 financial institutions, at the world's largest money-remittance company and at a global credit bureau. He has also been on the solutions-provider side of the table at multiple fintech companies.

Ken is passionate about using all available signals to create the risk/reward balance that every consumer and business desires. In this pursuit he leverages available technology, especially digital options, to solve the equation of risk and fraud.

What is the risk-based organization model for banks and financial institutions, and how does it relate to fraud prevention?

A risk-based organization model is a way of managing risk in banking and financial services by aligning the roles and responsibilities of different functions and levels of the organization. It relates to fraud prevention by ensuring that there are adequate controls, as well as checks and balances to detect, prevent and mitigate fraud risks.

KEN ALLEN
INDUSTRY CONSULTANT

What are the three lines of defense in fraud prevention, and what are their roles and responsibilities?

The first line consists of the **strategic and operational functions** that own and manage the fraud risks and controls on a day-to-day basis. The second line consists of the **governance and oversight functions** that monitor and challenge the effectiveness of the fraud risk management framework and policies. The third line consists of the **internal audit function** that provides independent assurance on the adequacy and effectiveness of the fraud-risk management system.

> "A risk-based organization model is a way of managing risk in banking and financial services by aligning the roles and responsibilities of different functions and levels of the organization."

What changes are happening in the three lines of the defense model due to the digital transformation and the emergence of fintechs and neobanks?

The first line is becoming more dynamic and collaborative with the digital and transformation functions responsible for the customer

experience and the innovation of products and services. In addition, neobanks and sponsor banks are increasingly being asked by regulators to increase scrutiny of first- and second-line controls. With the advance of fintech solutions permeating banking, it is ever more important to have strong risk-control frameworks to establish and manage risks.

Continuing with legacy fraud controls is no longer acceptable because of the false positives, the false negatives, the impact on customers and banks' ability to interact with regulatory and social media groups. Regulators increasingly want higher levels of client satisfaction with a strong framework. This requires thinking differently than before and challenging the status quo. But it must be done in a scalable and non-biased governed way so as not to increase risk. It should optimize the risk/reward tradeoff.

> "Being on the "bleeding edge" is usually not accepted in most banking oversight processes. But being on the "leading edge" in certain areas of need can be justified with strong diligence and testing."

How do you drive change in the fraud prevention tools and processes within the organization, and what are the challenges and opportunities?

You need a clear strategy, a supportive second line and a willingness to test and validate new solutions. You also need to work with the digital and transformation functions responsible for the customer experience and the innovation of products and services. Some of the challenges are regulatory compliance, the procurement process and the integration with existing systems. Some of the opportunities are improved efficiency, accuracy and customer satisfaction. Being on the "bleeding edge" is usually not accepted in most banking oversight processes. But being on the "leading edge" in certain areas of need can be justified with strong diligence and testing.

How is AI changing the fraud prevention landscape, and what are the benefits and risks of using AI tools and techniques?

Artificial intelligence (AI) is changing the fraud prevention landscape by enabling more dynamic, adaptive and intelligent solutions that can detect, prevent and mitigate undue risks by bad actors. Some of the benefits are reduced manual work, enhanced data analysis and a better customer experience. Of course, some of the AI risks are the technology's ethical, legal and security implications. And then there are potential bias and errors. Because of those risks, there needs to be human oversight and intervention.

Most recently, generative AI has broken through due to the adoption and acceptance of large language model (LLM) capabilities. This technology is rapidly gaining acceptance with investors and is affecting everyday interactions, such as incorporation into customer support and operations teams in the near term. For example, a bank's drive-thru might include an AI bot. But the sharing of data with any third party, and its inherent fraud vulnerabilities, along with other risk and privacy considerations, will come under increased scrutiny. How this technology evolves in banking will require financial services leaders to thoroughly test, while collaborating with regulators on the possibilities.

Banks must redouble vigilance with fraud threats from all directions

Q&A WITH **DIANNE S. WALKER, FIRST HORIZON BANK**

DIANNE S. WALKER IS an accomplished banking professional with more than 20 years of experience in the financial services industry. As director of Contact Center Banking at First Horizon Bank, headquartered in Memphis, Tenn., she oversees multiple teams dedicated to delivering exceptional customer service and driving operational excellence. Dianne is passionate about leveraging technology and data-driven insights to optimize contact center performance. She is adept at developing and executing customer-centric initiatives that align with business objectives and regulatory requirements.

Dianne drives strategy and leadership for the consumer, small business and technical support teams for First Horizon's Contact Center Banking delivery channel. She also has oversight of the organization's fraud-claims management and complaint-management process, as well as e-commerce and direct sales. These teams offer both sales and service, meeting the client where and how they want to connect, whether through digital, social media or phone.

What are some of the leading causes of compromises to a consumer's or small business owner's account?

I'll start with **phishing**, which takes the form of phishing emails, texts or phone calls to trick customers into revealing sensitive information, such as credit card numbers and login credentials. The second threat is **weak or repeated passwords** that make it easier for attackers to gain unauthorized access. Third is **malware and viruses**. This malicious software is installed unbeknownst to consumers through what seem to be harmless links and allows bad actors to steal login credentials and even grant remote access to the attackers. Finally, there is **social engineering**, which can include both targeted and untargeted manipulative tactics. That includes impersonation or pretexting to trick individuals into divulging sensitive information or performing actions they normally would not, such as transferring funds.

"Check fraud remains a persistent issue, especially as criminals adapt their tactics to exploit vulnerabilities in digital and paper-based payment ecosystems. We've seen more sophisticated forgery techniques. Also, fraudsters attempt to capitalize on the use of remote deposit capture—or mobile deposits—where they attempt to deposit the same check multiple times at multiple financial institutions."

DIANNE S. WALKER
FIRST HORIZON BANK

Check fraud has increased sharply. What forms are you seeing that trend take? Is it the source of a growing number of claims, disputes and interactions with customers?

Check fraud remains a persistent issue, especially as criminals adapt their tactics to exploit vulnerabilities in digital and paper-based payment ecosystems. We've seen more sophisticated forgery techniques. Also, fraudsters attempt to capitalize on the use of remote deposit capture—or mobile deposits—where they attempt to deposit the same check multiple times at multiple financial institutions. Social engineering is prevalent in this space as well: fraudsters manipulate customers into unwittingly facilitating fraudulent check transactions, such as sending payments to fake vendors. All of these scams drive claims and other interactions with customers.

Your clients are inundated with messages in several channels. But how do you break through the clutter and get their attention about the latest scams or fraud risk in general?

As an organization, our marketing and digital teams are vigilant with their efforts to provide targeted messaging that is relevant

to our clients. As director of the Contact Center delivery channel, my focus is on virtual banker awareness and detailed training on how to support clients who suspect their information may have been compromised or who have potentially experienced fraud. We have been successful in this effort through clear and consistent communication. We explain potential fraud risks and provide real-life examples of common fraud schemes, such as phishing scams, impersonation attempts and social engineering tactics. Our organization is intentional in our efforts to educate our clients on the warning signs of potential fraud. We take advantage of every client connection, sharing tips on how to recognize scammers who are trying to obtain sensitive information, as well as how to reduce clients' risk of falling victim to fraud. Of course, we emphasize the importance of recognizing and responding to alerts initiated through digital banking, which is designed to help customers effectively monitor their account and quickly report any concerning activity.

What role is social media playing in fraud prevention and engagement with customers?

From a First Horizon standpoint, social media is playing a significant role in fraud prevention by providing our clients another channel to provide feedback and identify potential issues. It allows us to respond swiftly. Social media also serves as a platform for informing customers about common scams and security measures. Engagement-wise, social media facilitates direct communications with customers, fostering trust and loyalty through personalized interactions and quick responses to inquiries or concerns. On the other hand, fraudsters capitalize on social media by exploiting its wide reach and interconnected nature to help execute various scams—phishing schemes, identity theft, fake promotions and fraudulent investment schemes. Fraudsters often create fake profiles to impersonate legitimate businesses or individuals and use manipulative tactics to deceive users into sharing personal information and financial details.

"We take advantage of every client connection, sharing tips on how to recognize scammers who are trying to obtain sensitive information, as well as how to reduce clients' risk of falling victim to fraud."

Financial services organizations increasingly look for stronger, tailored solutions to fight fraud

Q&A WITH **BRAD CRANFORD, ALKAMI TECHNOLOGY**

BRAD CRANFORD IS the director of product management for digital banking solutions provider Alkami Technology, where he specializes in security and fraud prevention. He is an accomplished product leader with experience in all aspects of product delivery, including product management, engineering and sales support. Brad is an experienced people manager with well-rounded management and technical experience in leading cross-functional teams to solve complex business problems and bring new products to market.

A longtime strategic product leader at Alkami, Brad has helped direct its strategy in fraud prevention, banking core integrations, data, marketing, account opening and loan origination while Alkami has transformed from a small fintech to a public company.

When you host security reviews with financial services clients, are they asking to have more friction or less friction applied to their customers' digital banking experiences amid these fraud challenges?

In the past, the most common conversation with a financial institution was about making the user's experience more seamless and balancing that with their need to control fraud. But the trend is for financial institutions looking for stronger measures to reduce fraud and provide tailored solutions for account holders with differing security needs and risks.

Some industries have introduced passwordless authentication for customers. Has the financial services industry adopted it? And will it reduce friction while bolstering security?

Broadly speaking, no, the financial services industry has not adopted passwordless authentication yet. But interest is growing, probably due in part to sustained public support of passwordless solutions by Apple and Google. Passwordless solutions like FIDO2 passkeys are promising because they can help eliminate the risk of reused passwords, phishing attacks and data breaches.

Additionally, many institutions are transitioning or have transitioned from using hard tokens to soft tokens for their business clients' money-movement activities, such as when using electronic disbursement or collection channels like ACH, wire and instant payments. Biometric authentication and other approaches may also be incorporated in a multilayered security approach.

A scam that appears to be on the rise is credential stuffing. What does that mean, and how can clients protect their organizations from this nefarious practice?

Credential stuffing is typically an automated attack using large batches of credentials acquired from data breaches. These attacks are generally cheap for bad actors to try even when success rates

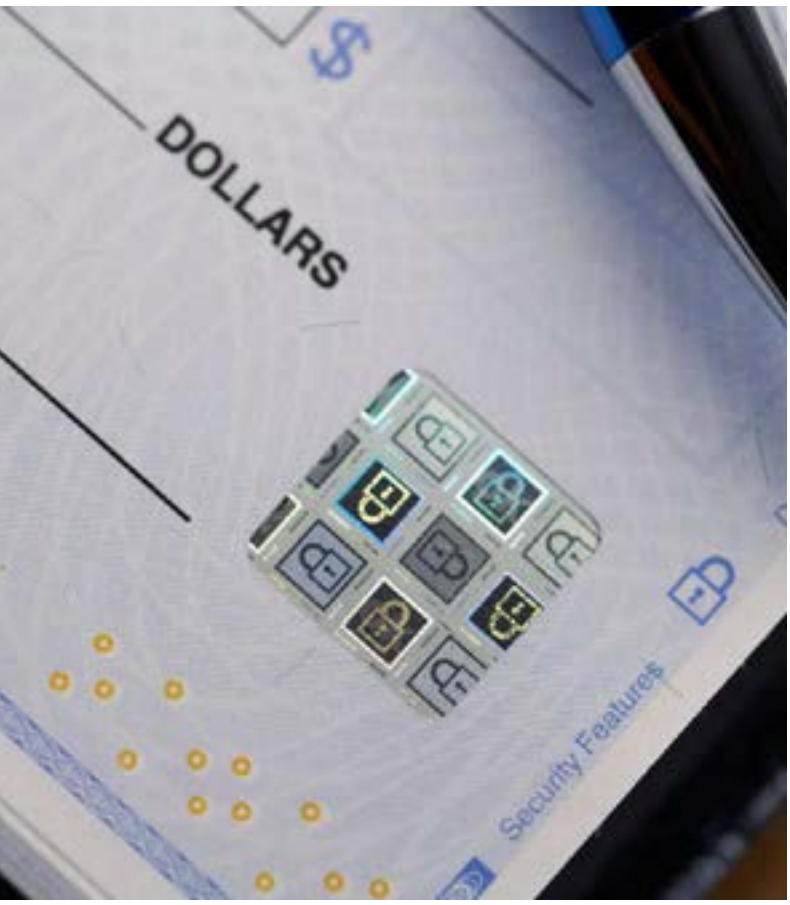
BRAD CRANFORD
ALKAMI TECHNOLOGY

are very low due to their untargeted nature. Financial institutions can directly address these attacks by using advanced networking solutions and data modeling to detect and block these attacks. But the challenge grows more difficult with bad actors' use of distributed systems.

A multilayered approach is needed to address the challenge from many directions, including improved network security tools, strong password tools and dynamically evolving authentication solutions. Other solutions include leveraging multifactor authentication (MFA) to protect accounts that might be breached and ongoing account-holder training to help users get smarter about protecting themselves and reporting suspicious activity. Data modeling services that monitor and detect potential account takeover attacks that might result from exposed credentials can also help thwart credential stuffing.

Just like consumers, small businesses have been victimized by account takeovers. How can businesses mitigate this fraud?

Commercial banking accounts have several tools to help with their unique challenges for security. These include dual (or multi-person) approvals, which not only help address internal fraud risks but



provide additional protections against a single individual falling for social engineering scams.

Additionally, commercial accounts may subscribe to services such as check positive pay and ACH positive pay to proactively protect themselves from check and inbound ACH fraud. ACH credit origination protection can also be used to detect unknown payees on outbound disbursements from file to file. Businesses should confirm any change in their vendors' payment addresses and changes to vendors' routing number and bank account information through established channels.

Bots are behind a growing number of fraud or fraud attempts. How can financial institutions help their clients protect themselves from these types of attacks?

As discussed with credential stuffing, automated attacks are best defended with multiple layers of solutions. These include network layer tools to detect and block harmful activity, machine learning and AI tools to dynamically evaluate incoming requests, as well as strong post-authentication tools such as MFA and account takeover detection to protect accounts that may become compromised.

Financial institutions have been struggling with check fraud. Are there any new technologies to deploy against this growing challenge?

Check positive pay services remain one of the most effective tools for protecting commercial accounts from check fraud. Given the increases in USPS blue box mail theft, check washing and fraudulent check creation, we have seen financial institutions require check positive pay with payee verification for their business, commercial and corporate clients using check positive pay.

> "Check positive pay services remain one of the most effective tools for protecting commercial accounts from check fraud."

Payee verification allows for the "payee name" field on the check issuance file to be compared to the presented check's payee name. When systematically compared, altered items can be identified and flagged as exceptions for further review by the financial institution or the check issuer—their business client.

Financial institutions should also protect their internal accounts and general ledgers with check and ACH positive pay capabilities.

How can banks and credit unions continue to build and maintain trust with customers amid this high-threat atmosphere?

Financial institutions must communicate well and educate users to build and maintain their trust to address the ongoing fraud challenges. Institutions engaging well with their account holders see improved reporting of suspicious activity, such as phishing sites, impersonation scams and increased security awareness from their users. When account holders can see their financial institution is engaged in securing their accounts and not just adding confusing steps and roadblocks without paying attention to the end user's experience, trust and two-way communication increase.

Tapping a variety of tactics to thwart fraudsters—from employee education to increasing customer awareness

Q&A WITH **CASEY MORGAN, COMMERCE BANK**

CASEY MORGAN IS director of retail operations for Commerce Bank, a position he has held for the last 10 years of his 23-year tenure at the bank.

Casey is responsible for transaction procedures, new account openings, banker systems and cash controls throughout the bank's 140+ branches and its customer care center. And he's part of a larger team that promotes Commerce's annual company-wide Hackathon, which encourages Commerce staff to collaborate on creative solutions that improve products and services. In fact, the idea for a unique text-based check fraud prevention service emerged from a recent Hackathon.

What key steps do you take to help your staff prevent fraud and fraud attempts?

Our key steps include automated system alerts for a variety of transactions and customer requests, customer authentication procedures for both in-person and remote interactions (phone, email, chat, etc.) and employee education on a wide variety of fraud scenarios and trends.

CASEY MORGAN
COMMERCE BANK

Do recognition programs for your team play a role in fraud mitigation?

Yes. We have a program called Fraud Fighters that rewards team members for stopping fraud and completing training activities to keep them engaged on fraud trends and red flags. To encourage participation, team members are awarded fraud detective badges and points that are redeemable for prizes and gift cards.

How do regulators impact how your organization approaches its fraud mitigation strategy and your recommendations to customers?

Regulations must be reviewed frequently to ensure they are still effective. One example is funds availability, or Reg CC. More fraud could be prevented if banks could place holds for larger amounts or for longer periods when checks meet certain risk criteria, such as

being an unusually large amount, coming from an unfamiliar or out-of-footprint bank or otherwise not matching what we would expect a customer's normal deposit behavior to be.

Do measures like presenting more anti-fraud messaging in your branches help raise awareness among your customers? Are there other tactics that have been helpful?

As branch traffic patterns shift, we leverage in-branch and digital channels to increase customer awareness of fraud activity, prevention tools and recovery steps. We also have annual training for team members and alert bankers when there is increased fraudulent activity in their area. By educating customers and team members, we increase our chances of detecting and preventing fraud.

Are you seeing an increase in business identity theft? If so, what form does that take, and how can FIs help their customers combat and understand business identity theft?

Unfortunately, we have seen a rise in business identity theft. Fraudsters obtain checks, often through mail theft, create fake documents with names leveraging a real company and then attempt to open new accounts. Financial institutions can help prevent this by having robust Know Your Customer (KYC) and Customer Due Diligence programs that require sufficient validation of the business, its representative and application legitimacy.

> "Unfortunately, we have seen a rise in business identity theft. Fraudsters obtain checks, often through mail theft, create fake documents with names leveraging a real company and then attempt to open new accounts."

Why is it important for the banking industry to present a united front in mitigating fraud?

Banks of all sizes are facing fraud issues, and we can certainly be better equipped to fight against it by working together. A united front would also demonstrate to the public that our industry is committed to protecting our customers' confidential information and helping customers protect their assets. To me, this means a more coordinated approach to sharing information about emerging fraud trends and known fraud rings. It also means coordinating on successful prevention techniques, scaling more uniform practices across all institutions to reduce gaps and getting behind faster collective action in response to incidents. Finally, we can share our collective concerns with our regulators to promote regulatory change in this area.

Combating the latest security and fraud threats

A BAI SPECIAL REPORT PRESENTED BY ALKAMI TECHNOLOGY

BAI Banking Strategies

Discover additional BAI Banking Strategies content, BAI research and other thought leadership. »

About BAI

BAI is a nonprofit, independent organization that delivers the financial services industry's most actionable insights, enabling leaders to make smart business decisions every day.

To view more thought leadership from BAI, please visit bai.org.