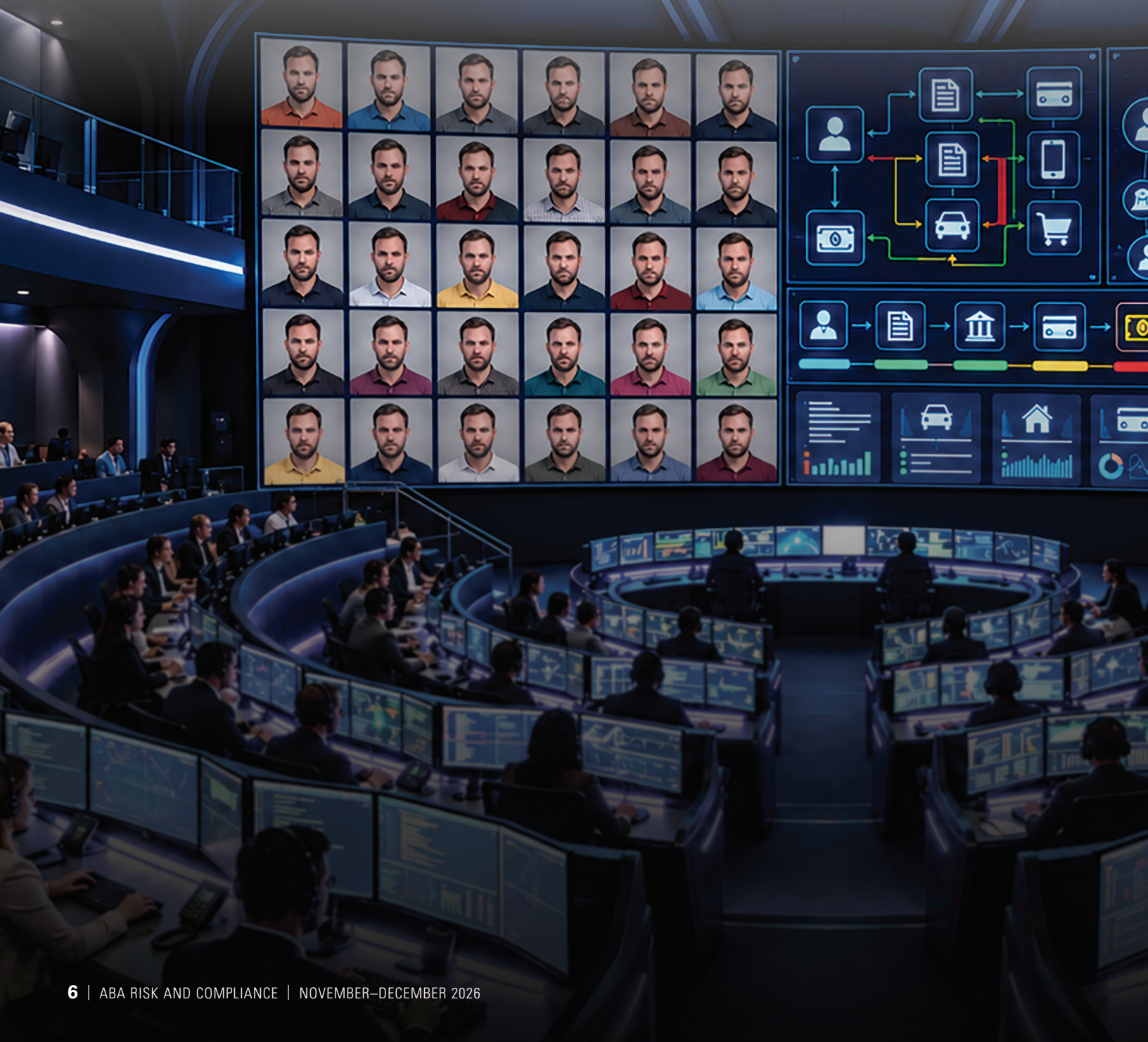
Inside the New Fraud Arms

An interview on identity, AI and the



Race

changing face of fraud



STOCK.ADOBE.COM / ANZE / BONOTOM STUDIO, INC. / CHATGPT

BY SEPIDEH ROWLAND, CCBCO, CAFP

Not long ago, fraud professionals could count on familiar warning signs: poorly crafted phishing emails, obviously fake identities and fraud rings that followed recognizable patterns. Today, those signals are disappearing. Artificial intelligence (AI) has fundamentally changed the fraud landscape, giving criminals unprecedented speed, scale and sophistication. Deepfakes are becoming increasingly convincing, counterfeit documents are more difficult to detect, and "fraud as a service" has transformed cybercrime into a thriving commercial enterprise.

The numbers reflect this accelerating threat. According to the FBI's 2025 Internet Crime Report, the Internet Crime Complaint Center received 22,364 complaints involving AI-enabled fraud, resulting in nearly $893 million in reported losses. At the same time, financial institutions are confronting increasingly sophisticated attacks that target not only banks, but also consumers, businesses and government programs.

To better understand what is changing and what financial institutions should do about it, Sepideh Rowland, the magazine's Editorial Advisory Board co-chair, sat down with Mike Cook, head of fraud insights at Socure. With nearly four decades of experience building fraud prevention systems and studying criminal behavior, Cook draws on extensive research, fraud-ring analysis and observations from one of the industry's largest data consortiums to explain how today's criminals are adapting, why traditional defenses are becoming less effective and where banks should focus their investments.

What follows is their conversation about the future of fraud, the growing importance of layered defenses, and why collaboration, innovation and faster adaptation may be the banking industry's best hope for staying ahead.

Fraud is skyrocketing, and the numbers are alarming. From your perspective, what does today's fraud landscape look like?

I've spent nearly 40 years building fraud systems and studying fraud patterns, and I've never seen anything like the last 18 months. Even in the last six months, the pace itself has accelerated dramatically. The bad actors are getting much better, and everything has changed.

The speed of attack is incredible. The way criminals create identities has changed completely. The days of gibberish email addresses and obvious fraud signals are disappearing.

What's really concerning is that criminals are learning from the experts in fraud prevention. If you ask ChatGPT for the top signals banks use to detect identity fraud, it will give you a solid list because, over the years, fraud-prevention professionals have done a good job of identifying and sharing information about what works. And, the more openly the industry talks about how fraud is detected, the more information criminals have to help them defeat those defenses.

"I've spent nearly 40 years building fraud systems and studying fraud patterns, and I've never seen anything like the last 18 months."

A three-year analysis of those signals found that bad actors are actively working to overcome — and in some cases are already overcoming — every one of those signals.

AI is now being used to build identities. Criminals are using automation and orchestration to create better attacks. Deepfakes and counterfeit documents are becoming increasingly convincing. The speed and scale of fraud today is unlike anything I've experienced in nearly four decades.

That tracks with what I've seen firsthand. In one AI experiment involving the creation of a fictitious document, the system suggested adding things like wrinkles, watermarks and other signs of wear to make it look more authentic. It really drove home how sophisticated these tools have become. Artificial intelligence is making it possible to create increasingly realistic identities and deepfakes. What risks do banks need to understand today?

The risk is that deepfakes are getting better. Banks need technology that can identify manipulated images and videos because you can't manually determine whether they're real.

But detecting a deepfake is only one part of the process. Banks need a layered approach to identity verification that combines image analysis with signals such as the device information, location, time zone, IP address, haptic signals — such as how a user taps, swipes or holds a device — and other behavioral indicators, as well as proxy information.

My concern is that the industry could make the same mistake it made with KYC. Some institutions began treating KYC as a fraud solution by itself. It wasn't. Deepfake detection is important, but it is only one component of a layered approach to fraud prevention.

Fraud-as-a-service has become a business model for organized crime. Criminals are no longer relying only on stolen credentials; they're passing liveness tests, creating convincing deepfakes and bypassing traditional KYC controls. What are you seeing?

Fraud-as-a-service is real, and it's become much more sophisticated. I'm subscribed to hundreds of Telegram channels where criminals openly sell identities, new email addresses, deepfakes and other tools. The quality of those services has improved dramatically.

How are these criminal networks using AI to stay ahead of the controls banks have traditionally relied on?

They're operating much more like legitimate businesses. Before, there wasn't a lot of thought put into building an identity. It was all done manually, and the fake documents were easily recognizable. This is no longer a fight against individual fraudsters. It's a fight against networks.

A fraud ring isn't necessarily a group of people anymore. It could be one person using fraud-as-a-service tools purchased online. They're buying complete identities with selfies and deepfake videos that are much better and much cheaper than they used to be. The gibberish email addresses are gone. Today's identities are well-formed, with properly formatted addresses. Criminals are orchestrating their attacks and using residential IP proxies to make those identities appear legitimate.

What AI has changed is that you no longer have to know AI to be a fraudster. The services are available openly on the Internet, not just on the dark web. You can see people selling identities at scale on social media.

They're also making those identities harder to detect. They'll include prior phone numbers, addresses and email addresses from a victim's history because they know that can confuse fraud models. They're using AI, automation and orchestration to attack us much better than they've ever attacked before.

As fraud-as-a-service becomes more sophisticated, where do you see criminals focusing their efforts? What trends concern you most right now?

The biggest concern I have today is identity theft. There's always been first-party fraud, synthetic identity fraud and identity theft. Many people say synthetic fraud is exploding, but what we're seeing is that identity theft is growing while synthetic fraud is actually flat or even declining.

Why? Because stolen identities are easier to acquire, more complete and more effective. A well-formed identity theft attempt is harder to detect than synthetic identity fraud, so that's where criminals are focusing.



"This is no longer a fight against individual fraudsters. It's a fight against networks."

What concerns me most is what that means for consumers. Scams are already increasing rapidly, but I think we'll look back in a few years and wish they were only growing at today's rate. Identity theft and increasingly sophisticated money-movement schemes will be supporting the next wave of scam attacks against consumers.

The largest fraud rings no longer focus on a single target. They're building complete financial identities that can be used across multiple industries. If they steal your identity, they don't just want your credit card. They want a bank account in your name, government benefits deposited into it, and the ability to move money using your identity.

That's why banks have to do a better job stopping fraud at the front door. The more stolen identities make it into money movement platforms, the more successful those scams become. Consumers are becoming the easier target, especially as criminals utilize a consumer's actual online and social-media presence to create more convincing deepfakes.

Earlier, you talked about criminals building complete financial identities, not just stealing accounts. I recently heard from a medical practice that became the victim of exactly that kind of fraud. Criminals rerouted the practice's mail, opened bank accounts in its name and diverted reimbursement checks for nearly a year. The physician assumed payments were simply delayed. When law enforcement finally reached out, he ignored the calls because he'd been told for years not to respond to unsolicited phone calls, texts or emails — exactly the advice agencies like the IRS give to help consumers avoid scams. Are you expecting to see more attacks like this?

Yes. It's going to become much more confusing because people won't know who's real anymore.

The bad actors are studying human behavior. They're learning what words and tactics keep people engaged long enough to build trust, talk about finances and eventually convince someone to send money. They're getting better at understanding how to manipulate people.

That's why I think we're going to see many more scams. As deepfakes improve, people will believe they're talking to a family member, a trusted business or a government official. It becomes much harder to distinguish what's real from what's fake.

Financial institutions are trying to keep pace with rapidly evolving threats. What can banks do to stay ahead?

The first thing banks need to do is stay on top of their technology providers. They should be asking when models were last updated, how often they're updated and how vendors are responding to changing fraud patterns. Deepfake technology is evolving so quickly that you have to pay close attention to those behavioral changes, and that takes continuous investment.

The bigger challenge, though, is model governance. Compliance is essential because you don't want to create unnecessary friction for legitimate customers. Younger people, older adults, immigrants and underbanked consumers can sometimes look like fraudsters in the data, so governance matters.

What has to change is the speed. I think compliance has to speed up.

I compare it to a fire station. Imagine if firefighters had to stop and hold an executive meeting before they could suit up, get on the truck and respond to a fire. By the time they made a decision, the building would already be burning. Fraud is moving at that kind of speed today. It changes too quickly for lengthy approval processes.

Banks need to use AI and other technologies to accelerate the model governance process. At some banks, models approval takes so long that they are already two model versions behind. By the time a model is approved, fraud patterns have already changed, and unnecessary financial losses are taking place.

The biggest thing banks can do — particularly institutions with lengthy model governance processes — is embrace AI and other technologies, and work with policymakers to find ways to speed up the process without sacrific-



"It's going to become much more confusing because people won't know who's real anymore."

ing compliance. Compliance is important because it protects consumers. But when fraud continues unchecked, that hurts consumers too.

From a banking industry perspective, we've often said institutions have to do more than simply check the regulatory boxes. They have to meet regulatory expectations while keeping pace with rapidly evolving threats. I'm also curious about community banks and credit unions. Many CEOs still believe, "This doesn't happen here." They rely on manual processes, spreadsheets or legacy systems and often don't have formal model governance. What are you seeing?

Fraud affects community banks, credit unions and small regional banks. They're not attacked as heavily as the largest banks, payment platforms or crypto companies, but they are attacked, and the consumers at those institutions are impacted.

Many larger institutions have embraced AI, but community banks are often more hesitant. What's the distinction you're seeing?

For smaller banks in particular, relying on KYC and manual reviews presents challenges. KYC isn't a fraud solution. It's not going to catch fraud.

A layered approach is needed. KYC by itself isn't enough, and neither are manual reviews. They may work when you're opening a limited number of new accounts each day, but these attacks are only going to scale. They"re not going to be able to handle that volume manually.

Earlier, we talked about criminals using AI. Are consumers using AI to commit fraud as well?

Yes, consumers are starting to use AI to perpetrate fraud, and the scale of first-party fraud is concerning.

One example is what people are sharing on TikTok. They'll take a picture of a computer that arrived in perfect condition and ask AI to make it look crushed. The AI generates an image showing the damaged product, and they'll send that to the retailer saying, "This is how it arrived. I'm not sending it back. Send me a new one or refund my money."

That's unbelievable.

I wish I could say it's shocking, but it's not anymore. Nothing is shocking anymore.

In your current role, you have access to one of the industry's largest fraud consortiums, giving you a unique view across financial institutions and other industries. Historically, many organizations have been reluctant to share information because they view each other as competitors. But in fraud, collaboration can be a powerful tool. What have you learned about the value of a consortium, and why is information sharing becoming so important?

One of the biggest advantages of a large fraud consortium is the ability to see patterns across industries. When you can analyze fraud across thousands of institutions and multiple sectors, you begin to see behaviors and trends that no single organization could identify on its own.

That broader view allows you to conduct better research, build better models and understand how fraud rings are evolving. We've been able to study attacks across industries and found that many of the same fraud rings are targeting multiple sectors at the same time. Without that kind of visibility, you simply don't see those connections.

I'm encouraged because I think there's been a real shift. Banks used to say, "We don't want to share our fraud data because it will help the competition." But it's fraud we're fighting, not each other.

I also think the government has recognized that appropriate data sharing is important, as long as it's done within privacy and security guidelines.

What I've found is that when people come together around evidence instead of anecdotes, they're much more willing to ask questions, share experiences and learn from one another. I haven't seen that level of collaboration before, and it's encouraging.

We've talked about collaboration across the industry, but what about collaboration inside financial institutions? Fraud, BSA/AML, information security and the business lines have traditionally operated in silos, even though each has pieces of the puzzle. Are you seeing those groups work together more effectively?

They're talking more than they were, but they need to talk a lot more than they are. I'd also add Human Resources [HR] to that list because hiring fraud has become a much bigger issue. Criminals are using deepfakes, fake LinkedIn profiles and other tactics to infiltrate organizations.

What's interesting is that fraud teams often say, "That's an HR problem." It isn't. HR doesn't know how to handle fraud by itself. Cybersecurity, fraud,

"It's fraud we're fighting, not each other."

BSA/AML, HR and the business lines all need to be talking because the entire organization is under attack. It's no longer just new accounts, transactions or the call center.

The group I see becoming much more involved is cybersecurity. The infrastructure supporting fraud has grown tremendously. Criminals are buying identities, email addresses and phone numbers and using tools that make it much harder to identify fraud rings.

That means banks have to look beyond the fraud itself and understand the infrastructure enabling it. It's no longer just about an IP address. It's about understanding the services, technologies and the individual companies behind those attacks and how they contribute to fraud.

The more organizations share information internally, the stronger their layered defenses become.

If you were advising a compliance or fraud officer evaluating a technology provider, what questions should they be asking to determine whether that vendor is keeping pace with today's threats?

The first question I'd ask is, "How much are you investing in your product?"

You want to understand how quickly the solution is evolving. How often are you updating the models? What technologies are you using? What innovations are you bringing to the market?

I'd also ask how they're researching new fraud patterns and how they're acquiring new data. If a provider isn't continually improving its models and adapting to new threats, it's going to fall behind.

Years ago, incremental improvements to the same models could be made because fraud evolved more slowly. Those days are gone. If you're not innovating today, you're losing.

Banks should look for providers that continue to invest in their technology, their research and the people building those systems.

It seems like every technology provider now says it has an AI solution. If I handed you a crystal ball and asked where we'll be five years from now, what do you see? Will the industry get ahead of this, or is this simply the new reality?

I do think it's the new reality.

I've been doing this for almost 40 years, and this is the most concerned I've ever been. The bad actors are working together better than ever before. They have new infrastructure, fraud-as-a-service tools and AI technologies they've never had before, and they're using them very effectively.

The speed and scale of attacks will continue to increase. Deepfake technology has improved dramatically over the last 18 months, and the pace of improvement keeps accelerating. The identities criminals create will become even more convincing, and the attacks will become more accurate.

That means banks have to continue working with government to make sure they have the tools they need to fight fraud. Compliance processes will have to move faster, and banks will need to continue strengthening controls at the front door to keep fraudulent identities out before accounts are opened and money begins to move.

I also think consumers have to become part of the solution. They're often the easiest target, and our industry has to find better ways to engage them in protecting themselves from fraud. That's going to be one of the biggest challenges over the next several years.

One thing that really stands out to me is your point about friction. In banking, we often talk about reducing friction because we don't want consumers abandoning the account-opening process. But when I talk with law enforcement, I hear the opposite. They tell consumers to slow down — to pause long enough to recognize when something doesn't feel right.

I recently spoke with a medical practice where an exhausted employee clicked a link simply to make a pop-up disappear. That one click led to a ransomware attack that exposed the practice's data. Sometimes a little friction gives people the moment they need to stop, think and avoid becoming the next victim.

Any final thoughts for bankers?

This is an all-hands-on-deck moment for the industry. The bad actors have changed the game, and banks have to keep evolving. That means investing in technology, working with the right partners and recognizing that manual processes alone won't keep pace with the speed and scale of today's fraud.

To contact to learn more about Mike Cook, visit LinkedIn.com/in/mike-cook-2b41245/. ■

ABOUT THE AUTHOR

SEPIDEH ROWLAND, CCBCO, CAFP, is a partner at Klaros Group and leads the anti-financial crimes practice. She brings more than 25 years of legal and compliance experience across banking, money services, virtual assets, and fintech, building and running consumer and financial-crimes programs that meet regulatory requirements and reflect industry best practices. Sepideh has served as chief compliance officer, BSA/AML officer, and sanctions officer at community banks, money services businesses, and other respected financial institutions, as well as senior counsel at the American Bankers Association. In 2023, she received the American Bankers Association Distinguished Service Award for Financial Crimes in recognition of her career contributions.

Sepideh received a J.D. from Michigan State University School of Law, a B.A. from George Washington University, and is a member of the State Bar of Michigan and the District of Columbia Bar. Sepideh also serves as an Independent Director for Battle Financial, Inc. Reach her at **LinkedIn.com/in/sepidehrowland**/.