REFINITIV EXPERT TALK

Teaming talent and technology to beat criminals at their own game

Keep bad players from scoring on your consumers by fielding new technologies and training up your people, coaches Stacey Nash, Head of Enterprise Financial Crime for USAA

Established in 1922 and focused on serving the needs of active and retired U.S. military members and their families, USAA offers a multitude of banking, insurance, investment and retirement products and services to a customer base that numbers over 12 million. It can be said that the company was founded on the principles of serving those who serve and protecting those who protect.

One way the company is increasingly called upon to do that is to shield its members from potential cybercrimes, such as phishing attacks and various scams, as well as to educate them to the dangers inherent in today's digital landscape. Stacey Nash, Head of Enterprise Financial Crime for USAA, provided us with a firsthand account of the organization's efforts in its fight against financial crime.

The people who are perpetuating crimes aren't going to go and get honest jobs. They're going to constantly try and figure out how to commit crime. We have to be just as vigilant in our forward thinking as far as building the capabilities to protect consumers.

Stacey Nash, Head of Enterprise Financial Crime, USAA

REFINITIV: Can you describe the duties and oversight you are accountable for in your position?

STACEY NASH: Our team (Enterprise Financial Crime) is responsible for enterprise fraud strategy, as well as the operational execution of that strategy across USAA. We work with other areas of the enterprise to operationalize the fraud strategy through things like prevention, detection, investigation and recovery. Those are the four prongs that we focus on.

Our team is also responsible for the authentication strategy and capabilities for USAA, which is critical at this time and juncture. We work with the rest of the organization to ensure we're protecting our members while constantly trying not to introduce too much friction and inconvenience.

I would say that that leads into the talent development piece of my role and that of our leadership team. We are constantly striving to ensure that we've got the best people and the best minds, because ultimately, the financial criminals that we're fighting never stop recruiting and they never stop trying. We have to stay ahead of that and ensure that we've got people who are constantly committed to developing solutions to detect and deflect a lot of the things that we deal with on a daily basis.

REFINITIV: We are seeing financial criminal activity evolve with advances in technology. What kinds of financial criminal activity are you being confronted with the most, and what are you seeing as some of the more common areas of attack?

NASH: In a typical day, USAA blocks more than nine million cyberattacks and prevents on average $8.7 million in fraud losses. Some of the things have remained pretty consistent through the years, such as something as basic as phishing. We continue to see this predominantly in email, but we've seen cases where it has transitioned to robocalls or text. In every one of these cases, the fraudsters are impersonating a credible company or an individual, or even potentially, in some cases, a family member. That, I would say, is more of a traditional vector that we still see because it still works. They've just evolved, and they've actually upped the sophistication of some of these things.

Thinking about the last few years of the threat landscape, if you think back to not even four or five years ago, we were constantly seeing merchant and card data that was being compromised. Then with the shift to EMV/smart payment cards that took place across the U.S., that fraud vector was closed. The criminals couldn't monetize that anymore.

You could literally see the shift between the card data compromises to compromises that involved Personally Identifiable Information data – things like birthdate, name, address, driver's license, all of the things that institutions (not just banking institutions, but any institution that has any virtual landscape) leverage to authenticate people.

The challenge has been in figuring out how to authenticate and ensure we're talking to our members, while at the same time knowing that in the traditional capabilities that we leveraged, much of that information has been compromised and is available among hackers.

Other criminal activities we're constantly seeing are scams – anything from romance scams to wire transfer scams (sometimes tied to a home purchase, employment, etc.). These are situations where people, especially in the day and age of social media being so prevalent, are giving a lot of trust to somebody on the other side of their computer or their device. They're actually being convinced into either giving access to their information or giving access to their funds, or actually sending funds to somebody that they believe has great intentions or somebody who's posing as someone else. Those are some of the things that we're seeing on a regular basis that we're constantly trying to educate our membership on. Don't trust everything you read or everything that you get because unfortunately, not everybody has the best of intentions.

REFINITIV: We're seeing a greater push around data privacy. Organizations that ask for and collect a person's data are responsible for managing it appropriately and don't hold on to data they don't need. At the same time, they need that data to be able to verify a person and also to comply with regulations. Add to that the complexity of it being traded on the dark Web, so that you're not really sure if the person who's giving you the data is legitimately that person. How do you evolve your fight against financial crime with those kinds of technologies? Where do you see that going these days?

NASH: The biggest component of that for USAA is proactively promoting multifactor authentication (MFA). We're getting away from leveraging PII information, so it's the transition from knowledge-based information (log-ins and passwords) to a combination of factors including something the member has (such as a phone), something they know (for example, a PIN or who they are) and something they are, like a fingerprint or their voice. We currently have over three million members enrolled in MFA, and there's a tremendous push to continue to drive that up over the course of the next year or so.

REFINITIV: What are some of the programs that USAA has in place to educate its members about financial crime issues?

NASH: There are a few things. We've got a constant drumbeat of education and awareness through many of our channels (website, email and social channels). We leverage as many opportunities as we can. The multifactor authentication push has actually provided a tremendous platform with our members, to educate them on how it works and the benefits of security.

Another piece that we're focused on is through the annual report we send out to our members. In our most recent report which was sent to over seven million members, we included the option to request more information on increased security measures to keep their accounts safe. That was, by far, the highest option that membership selected to obtain more information. It's definitely top of mind, so we're constantly leveraging every opportunity we can, to educate membership both from a passive perspective and from a proactive perspective.

REFINITIV: With the advent of FinTech enhancements such as mobile banking and investing, what impact are you seeing that having on financial crime?

NASH: FinTech and the enhancements that all of these things are providing us with, to make our lives easier, are also providing the criminals that we're fighting with capabilities. What we've focused on at USAA is to ensure that we're a leader in the industry, offering the best in biometric options through our mobile apps and leveraging technology wherever we can. We're in a unique position, given the virtual nature of our relationship, and also given the vastness and the diversity of our membership from a location perspective and from a user experience perspective. We're an organization that embraces technology, and there's a constant focus to merge security with ease of use for our members.

USAA is a financial institution that's dedicated to support active duty U.S. veterans and their families all over the world. They're not always in geographies where technology is performing as well as we might wish. We consider all of those components. It's really about making sure that we're there when they need us, and we're not making it too cumbersome, while at the same time constantly doing our duty to protect them.

REFINITIV: What is some advice you would give to other financial professionals in the fight against financial crime?

NASH: When I think about the areas of banking that I've been in over the last 20 years, fraud is one area where competitors will come together to share best practices and leverage strengths because we are fighting the same criminals. It's an innate desire and need to protect membership, because at the end of the day, the funds that are going to fraud are going to fund bad things. None of us want to see those funds go towards that. We'd all much rather invest that money in capabilities to further protect our membership.

Also, I would advise professionals to leverage the opportunities to be active in the industry. Learn from other opportunities. Ultimately, we're in this fight together. Continue to drive education and awareness, and share tips on detecting and deflecting scams and things that are victimizing consumers. Constantly strive together to think ahead and build for the future, because I think the people we're fighting are doing that. They're not sitting back and waiting. They're thinking about, "What's the next thing we can do?" The people who are perpetuating crimes aren't going to go and get honest jobs. They're going to constantly try and figure out how to commit crime. We have to be just as vigilant in our forward thinking as far as building the capabilities to protect consumers.

Stacey Nash
Head of Enterprise Financial Crime, USAA

As the Head of Enterprise Financial Crime for USAA, Stacey has accountability for fraud prevention and detection and also owns authentication strategy for the enterprise. Prior to USAA, Stacey held similar roles at Santander and TD Bank. With over 20 years' experience in financial services, she has spent the majority of time in risk and operational roles focused on consumer and business security, protection and operational effectiveness. With a passion for industry collaboration and partnership, Stacey has been an advocate for shared data models aimed at reducing risk while achieving increased security and consumer protection. Stacey has served in an advisory position for both the American Bankers Association and the Consumer Bankers Association. She has also held positions on Risk Advisory Boards for Experian PLC and Early Warning Services, LLC, a joint venture between Bank of America, BB&T, Capital One, JP Morgan Chase, PNC Bank, U.S. Bank and Wells Fargo.