ICBA Education | Certification News
Q3 2024

Quarterly Newsletter for ICBA Certified Community Bankers

Educate the Consumer

Make a Dent in Fighting Fraud

By Alan Nevels

With every passing year, there are new threat attacks and innovative variations of old fraud schemes that still reign successful. And criminals continue to do their possible best to gain financial benefit by unearthing schemes designed to dupe consumers into providing their sensitive, personal details that allow access to their banking, card accounts, and mobile devices for authentication.

The ever-shifting landscape of cyber threats can be confusing for consumers and overwhelming for fraud fighters. Mix in the human factors of our "hurriedness" and sometimes over-trusting nature, sprinkled with our poorly created and lackluster password protections, and fraud prevention becomes increasingly challenging.

Continued on page 2

How I Work
Arlene Cooper

Arlene Cooper is the Internal Audit Officer at CNB Bank in Carlsbad, New Mexico and holds Certified Community Bank Internal Auditor (CCBIA) and Certified Community Bank Compliance Officer (CCBCO) designations.

Q. Tell us your background and how you got here.
A. I started my banking career in late 2018 as a Compliance Administrator at CNB Bank. In June of 2021, I was offered and accepted the position of Internal Audit Officer for the bank. I later earned the CCBIA and CCBCO certifications from ICBA.

Q. Briefly describe how you construct your day for optimal productivity.
A. I use my Outlook calendar to prioritize tasks. I tackle the

Banks have been forced into a position of combining payments innovations with a more proactive and layered approach to fraud prevention. “The scale of fraud attacks along with new mandatory regulatory requirements has forced FIs to expand fraud prevention into other areas for improvement,” says Yuval Marco, General Manager, Enterprise Fraud Management, NICE Actimize. “Financial institutions that embrace a modernized strategy incorporating machine learning and AI will not only bolster their defenses, but also enhance customer retention. This ensures a stronger and more resilient position in the face of these evolving threats,” continues Marco.

Sophisticated fraudsters are exercising widespread tactics via myriad communication channels (including text messages, phone calls, emails, and social media interactions) aimed at all ages, with the intent of gathering data useful for criminal intent. Below, let us explore a few of today’s more prevailing fraud schemes and the ways consumers can participate in protecting themselves and your bank from underhanded practices.

P2P Fraud

P2P (Peer-to-Peer) fraud schemes can show themselves in many different methods, and consumers tend to believe that they have protections because these transactions are tied to their bank accounts.

However, it is important to understand that there are no current regulated protections for P2P fraud. Schemes such as overpayment scams, charity scams, and marketplace scams are very popular within P2P transactions, and once the customer hits send there is no means to get the money back.

With today’s heightened use of AI (Artificial Intelligence), the criminals are implementing genius ways to trick consumers to release funds to the benefit of their financial gain. This is even more prevalent via the international channels.

PROTECTION →	Check and double authenticate that funds are being sent to the intended person(s) or business. It is virtually impossible to retrieve monies once sent.

Ransomware & Data Breaches

According to the Verizon 2024 Data Breach Investigations Report, “roughly one-third of all breaches involved ransomware or some other extortion,” and direct extortion attempts, whereby accounts and/or devices are held hostage, have increased to over 9 percent. But many confuse the difference between a ransomware attack and elements involving a data breach.

Continued on page 3

most important and time-sensitive tasks first, then move on to lower-priority ones.

Q. How do you keep track of what you have to do?
A. My daily tasks are guided by the internal audit risk assessment. I follow the assessment’s requirements and make sure to address every detail thoroughly.

Q. Take us through a typical workday.
A. Each morning, I check my email and Teams messages for urgent issues. I then focus on testing and reviewing internal audits. If we're working with external auditors or examiners, I handle any immediate needs. I also answer internal audit-related questions from my colleagues.

Q. Can you share a problem/challenge you're working on or trying to solve?
A. The field is constantly changing with new risks and regulations. Keeping up with these changes and ensuring our audit processes meet current requirements can be challenging. I stay updated by attending conferences and engaging in professional development.

Q. What's the best advice you have for other people in your role?
A. Try to take the “I want to be your safe harbor” approach.

While both cyber threats depend on speed and can be very damaging, a ransomware attack is normally tied to a threat towards targeted and/or specific individual(s) and is designed to infiltrate accounts with encryption, which is then not unseized until demands have been met.

A data breach is usually centered on a phishing attack that is aimed at many individuals, in attempts to capture personal details such as social security numbers, passwords, credit card information, and phone numbers.

PROTECTION →	Ensure that data protection software is always current and maintain strong oversight into the who's and the why's of data access. Ongoing education is key to protection against these threats.

Provisioning Fraud

Provisioning fraud, also known as tokenization fraud, involves the algorithmic replacement of sensitive information through unique codes that safeguard personal data. Provisioning is one of the top practices in use today as protection from fraudsters trying to gain access to data, but the increase in ATO (Account Takeover) fraud has made fraud detections challenging.

"While tokenization is one of the most secure ways to transact, we're seeing fraudsters use social engineering and other scams to illegitimately provision tokens," said James Mirfin, SVP and Global Head of Risk and Identity Solutions at Visa. Fraudsters are accessing and provisioning tokens by way of social engineering and other scams that lure issuers to grant the tokens.

PROTECTION →	Train against social engineering and acts of phishing. Issuers should decline any requests with a CVC 2 mismatch, and decline any suspicious activity, and/or request additional authentication by way of independent or segregated devices.

Costs associated with payments fraud can be sizable, and Machine Learning/ AI will continue to make the battles within the payments space a bit more taxing. Combating new fraud threats takes a multi-layered and global approach, with the requirement of cross-industry collaborations. For organizations to make a dent in fighting fraud, getting employees, cardholders, and merchants on board and engaged is a must.

Alan Nevels is ICBA Payments' senior vice president of card risk and merchant services.

It can be tough for people to hear they're not complying with a regulation. Reassuring them you are not there to reprimand but to educate makes a world of difference.

Q. What are you currently reading?

A. For motivation and inspiration, I'm rereading the New Testament. For pleasure, I'm reading You Like It Darker by Stephen King.

Q. How does your bank use training to solve for succession planning?

A. We cross-train employees in various departments for backup. When positions open or new roles are created, we often fill them quickly because of our ability to hire within our organization.

Q. What is your favorite thing about the ICBA Audit Institute or our other conferences you may have attended?

A. I love meeting new people and hearing the stories and experiences we all share. Making those connections is so rewarding.

Q. How has your designation affected your career/ role at the bank?

A. My designations have helped grant me the ability to make positive changes and influence our company's direction.

Join us at the

ICBA Annual Current Issues Certification Conference

Livestream

Oct. 21–24

Earn live CPE to maintain your certification and keep your finger on the pulse of key issues and trends related to Auditing, BSA/AML, Regulatory Compliance, and Security and Fraud.

Attend one day or all four. Earn 8 CPE for each day you attend!

- **Day 1: Auditing issues**
- **Day 2: Lending & Deposit issues**
- **Day 3: BSA/AML issues**
- **Day 4: Fraud & Physical Security issues**

	4 days	3 days	2 days	1 day
ICBA Members	$1,345	$995	$695	$395
Non-Members	$1,895	$1,295	$895	$495

Visit icba.org/education/seminars to register.

2024 Certification Calendar

Stay current, earn CPE to maintain your certification, or earn a new certification!
Check out our in-person and livestream institute options remaining for 2024.

Certification Institutes			ICBA Member	Non-Member	Non-Banker
Enterprise Risk Management Institute	Sept. 30–Oct. 3	Dallas, TX	$1,699	$2,199	NA
Compliance Lending Institute	Oct. 6–11	Bloomington, MN	$2,899	$3,799	$4,699
BSA/AML Institute	Nov. 5–7	Dallas, TX	$1,699	$2,199	$2,699
IT Institute	Nov. 12–14 and Nov. 19–21*	Livestream	$2,699	$3,599	$4,499

*Indicates an Institute is split over two weeks.
If you wish to test for certification, the testing fee is $500 in addition to the registration fee.

The 2025 calendar and events will be posted soon!

Watch for an exciting announcement about two new certification programs we are rolling out in 2025.

Newsletter sponsored by: ICBA Education