Cyber, Fraud & Physical Security Conference

MARCH 4-6, 2026



CYBER

Delve into the latest trends and challenges in cyber security, with more breakout sessions this year focused on cyber/IT topics.



FRAUD

Fraud losses continue at an all time high. Sessions dedicated to fraud topics will provide information on current trends and provide you with best practices and fraud prevention and detection strategies for your bank.



PHYSICAL SECURITY

Technological advances for the physical security professionals will be highlighted, with subject matter experts and law enforcement professionals exploring the trends and mitigation strategies for banks of all sizes.

Please join us as we learn methods to take our security posture to the next level. Security experts will heighten your awareness of trends seen in the industry; industry experts will help us identify concerns of the moment as well as the near and far future. Professionals will share tools they've picked up along the way and help you understand how the tools will impact you, your bank and our banking community. Don't miss this opportunity to network with other community bank cybersecurity personnel, security providers and industry experts!

Register today at: indiana.bank

CONFERENCE AGENDA

INDIANA BANKERS ASSOCIATION

Wednesday, March 4, 2026
Physical Security Track

7:30 - 8:30 am - **Registration and Continental Breakfast**

8:30 am - **Opening General Session**
When Violence Comes to Work — Through the Eyes of Survivors
Jim Rechel, President - The Rechel Group, Inc.,
Carol S. Dodgen, CPD - Dodgen Security Consulting

9:45 am - **Mastering the Art of De-Escalating Angry Customers, Co-Workers, and More**
Polly Westcott, PsyD, HSPP - Indiana Health Group

11 am - **Banker Panel Discussion**
Workplace Violence in Banking: Lessons from Those Who Lived It

12:30 pm - **Lunch**

1:30 pm - **Active Threat Response and Preparedness for Financial Institutions**
Terry Choate, CEO/President - Blue-U Defense, LLC

2:45 pm - **Active Threat Response and Preparedness for Financial Institutions (cont.)**
Terry Choate, CEO/President - Blue-U Defense, LLC

4:15 pm - **The Perfect Storm**
Patrick Dix, Vice President, Client and Association Engagement - SHAZAM

Thursday, March 5, 2026
Cyber/Fraud Track

7:30 - 8:30 am - **Registration and Continental Breakfast**

8:30 am - **Opening General Session**
Jim Rechel, President - The Rechel Group, Inc.

9:00 am - **Cybercrime: How to Keep Your Bank Safe from Insider & Outsider Threats**
Jeff Lanza - The Lanza Group

10:15 am - **Breakout Sessions**
AI in the Vault: Ensuring Confidentiality with Microsoft 365 Copilot
Zach Shelton, Principal, Cy Sturdivant, Principal - Forvis Mazars

Using Video Intelligence to Strengthen Security and Improve Service in Financial Institutions
Len Harvey, Regional Sales Manager - Verint

11:15 am - **Breakout Sessions**
What Bankers Need to Know About Agentic AI
Jim Perry, Senior Strategist - Market Insights, Inc.

ATMs, BlackCats, and IoCs. Oh My!
Michael Hartke, Executive Vice President - infotex

12:15 pm - **Lunch**

1:15 pm - **From Application to Attack: Inside Modern Account-Opening Fraud Rings**
Steven Gonzalo, CEO/President - American Commercial Bank & Trust

2:30 pm - **Banker Fraud Panel Discussion**

3:45 pm - **Fraud Trends for 2026: Perspectives from the US Postal Service**
Ron Barron - United States Postal Inspection Service

5:00 - 6:00 pm - **Cocktail Reception with the Exhibitors**

Friday, March 6, 2026
Cybersecurity Track

7:30 am - **Early Bird Session: InfraGard Q&A**
Kyle Johnson, CISSP, Managing Principal Consultant - Mandiant (now a part of Google Cloud)

8:00 am - **Data Integrity in the 20s**
Dan Hadaway, CISA, CISM, CRISC, Founder - infotex

8:45 am - **Passwordless Networks and FIDO-2**
Matt Babicz, CISA, Senior Manager, Cybersecurity Consulting - Plante Moran

9:45 am - **Why Good People Make Bad Security Decisions**
Jordan Rosiak, vCISO, Senior Advisor - Bedel Security

11:00 am - **The Critical Path: Your Next Move in the Incident Response Adventure**
Kyle Johnson, CISSP, Managing Principal Consultant - Mandiant (now a part of Google Cloud)

12:30 pm - **Conference Adjourns**

Contact us for more info! mgibbs@indiana.bank 317-333-7161

SESSION DESCRIPTIONS DAY ONE

When Violence Comes to Work — Through the Eyes of Survivors
This joint session examines workplace violence in the banking industry through both investigative case studies and survivor perspectives. Jim Rechel analyzes three fatal bank incidents to reveal warning signs, response challenges, and institutional decisions, while Carol Dodgen shares survivor-informed insights on preparedness, resilience, and recovery. Together, they deliver practical lessons to help organizations prevent violence, respond effectively, and sustain a culture of safety and compassion.



Mastering the Art of De-Escalating Angry Customers, Co-Workers, and More
Whether you're on the front line with customers or supporting teams behind the scenes, knowing how to defuse tension is essential. In this engaging session, Dr. Polly Westcott shares how understanding the brain's anger response helps security, IT, and banking professionals de-escalate conflict, strengthen teamwork, and keep operations running smoothly.



Workplace Violence in Banking: Lessons from Those Who Lived It
Following the documentary When Violence Comes to Work: An Inside Examination, this moderated panel brings together banking security leadership, law enforcement, and individuals directly impacted by fatal bank workplace violence incidents. Panelists will share firsthand experiences, behind-the-scenes investigative findings, response challenges, and institutional decision-making before, during and after each event. The discussion is designed to provide bank security professionals with practical, experience-based lessons to strengthen threat recognition, preparedness, response and recovery.



Active Threat Response and Preparedness for Financial Institutions
Choate's sessions emphasize proactive employee preparation, policy development, and understanding human responses in active threat situations. Attendees learn how to build security-mindful cultures, improve individual situational awareness, and implement pragmatic practices that bridge the gap between theoretical "run, hide, fight" models and real-world survival outcomes.



The Perfect Storm
This session will examine how converging fraud, cyber, and operational threats —including social engineering, ATM compromise, and ransomware attacks— create high-impact crises for financial institutions. Attendees will gain practical guidance on preparing for, managing and recovering from these events, with a focus on decisive leadership, coordinated response and institutional resilience.

Contact us for more info! mgibbs@indiana.bank 317-333-7161

SESSION DESCRIPTIONS DAY TWO

Cybercrime: How to Keep Your Bank Safe from Insider and Outsider Threats
This presentation breaks down the evolving tactics used by both internal and external cybercriminals targeting financial institutions. It highlights real-world attack scenarios, common warning signs, and the organizational blind spots that make banks vulnerable. Attendees walk away with practical strategies to strengthen defenses, reduce human-factor risk and build a security-aware culture that protects customers, data and the institution's reputation.

From Application to Attack: Inside Modern Account-Opening Fraud Rings
Sophisticated criminal organizations are increasingly targeting the largest financial institutions by exploiting weaknesses in account-opening processes. This session explores real cases in which my institution and our customers were attacked through well-orchestrated schemes that began with fraudulent account creation.

Banker Fraud Panel Discussion
Three bank volunteers - representing three different bank sizes - will share about a significant loss in their institution within the last 12 months and how the fraudsters bypassed the systems/procedures they had in place.

Fraud Trends for 2026: Perspectives from the US Postal Service
Postal Inspector Ron Barron of the Postal Inspection Service will be presenting emerging trends in robberies and additional threats to postal service employees, including impacts to mail delivery. Additionally, the presentation will include how the theft of mail is resulting in massive monetary losses to companies, individual citizens and banking companies via check fraud.

JOIN US AT 5:00PM

Cocktail Reception with the Exhibitors
Attend this casual networking reception, which includes light hors d'oeuvres, complimentary beverages and vendor prize drawings.

BREAKOUT SESSIONS:

AI in the Vault: Ensuring Confidentiality with Microsoft 365 Copilot
In today's highly regulated banking environment, generative AI tools like Microsoft 365 Copilot must be leveraged securely and remain in full compliance. This session will show executives how to harness Copilot's productivity benefits without compromising confidentiality. We will outline clear "dos and don'ts" for Copilot use – from policy-level requirements to practical tips for all institutions.

Using Video Intelligence to Strengthen Security and Improve Service in Financial Institutions
Banks continue to rely on video data for security, but the role of video is expanding. With the help of modern AI, the same camera infrastructure can reveal patterns, inform staffing decisions, support fraud investigations, and enhance the customer experience — all while promoting safety. This session will explore how financial institutions can create value from video data without replacing existing systems or overhauling operations.

What Bankers Need to Know About Agentic AI
As artificial intelligence moves beyond copilots and chatbots into autonomous, goal-driven systems, bankers face a new challenge: not whether agentic AI will matter, but how to prepare their institutions for the next frontier in banking's AI journey—using it responsibly and competitively.

ATMs, BlackCats, and IoCs. Oh My!
What does a ransomware attack look like, as it crawls over remote management and monitoring software to our ATMs? A well-known ATM service provider was once the subject of a ransomware attack. This presentation includes a review of the timeline, what the infotex SIEM was able to see, and a rundown not only of the IoCs, but the control structures that worked and did not work to thwart the attack.

SESSION DESCRIPTIONS DAY THREE

Early Bird: InfraGard Q&A
InfraGard is a public–private intelligence-sharing framework that links cybersecurity and risk professionals in critical sectors (including financial services) with the FBI to exchange threat indicators, best practices, and emerging risk insights. In this early bird session, Kyle Johnson, a director on the InfraGard Indiana Board of Directors, will bring us up to speed on InfraGard, its mission, and how to join and participate.

Passwordless Networks and FIDO-2
As cyber threats continue to escalate and credential based attacks remain one of the most common entry points for adversaries, financial institutions are rethinking how they authenticate users. This session explores the rapid industry shift toward passwordless networks and the adoption of FIDO 2 authentication standards, which offer phishing resistant and highly secure alternatives to traditional passwords and even legacy MFA.

Why Good People Make Bad Security Decisions
Even well-trained, well-intentioned employees fall for phishing, click risky links, bypass controls or delay reporting incidents. This session dives into the psychology behind those decisions—cognitive bias, urgency, habit and workload—and how they play out in community banks. With relatable scenarios and actionable insights, attendees will learn how to design processes, communication, and reinforcement that guide people toward safer decisions. This is a human conversation, not a technical one.

The Critical Path: Your Next Move in the Incident Response Adventure
The digital walls are always under threat, but when the worst happens, will your team crumble or command? Stop wondering about your cyber readiness. Join Mandiant for an interactive tabletop exercise where you'll be thrust into the heat of a critical cyber-attack and forced to make real-time, high-stakes response decisions. See exactly how prepared you are against real-world scenarios.

Thank you to our conference sponsors!

LUMU
MIDWEST SECURITY SERVICES Security You Can Trust!
LOUISVILLEGEEK
aunalytics
ICBA
Hanwha Vision
infotex
forvis mazars
dormakaba
BEDEL security CELEBRATING 10 YEARS

Thank you to our Security & IT Planning Committee!

Tab Browning, Horizon Bank, Michigan City
Ray Claycomb, Hoosier Heartland State Bank, Crawfordsville
Brian Dowers, The Fountian Trust Company, Covington
Robert Duke Jr., First Farmers Bank & Trust Co., Kokomo
Michael Etter, Security Federal Savings Bank, Logansport
Joanie Foreman, Lake City Bank, Warsaw
Al Fullerton, First Bank RIchmond
Dan Hadaway, infotex, Dayton
Tammy Hall, First Merchants Bank, Greenwood
Devon Jackson, First Harrison Bank, Corydon
Robert Martin, First Farmers Bank & Trust Co., Kokomo
Christy McBride, First Federal Savings Bank, Evansville
Becky Oakley, Farmers State Bank, LaGrange
Jim Rechel, The Rechel Group, Cincinnati, OH
Matthew Reisner, The National Bank of Indianapolis
Michelle Sloan, First Savings Bank, Corydon

Hotel Accommodations
The IBA's Cyber, Fraud & Physical Security Conference is being held at the Renaissance Indianapolis North Hotel, 11925 N. Meridan Street, Carmel, IN 46032, on March 4-6, 2026. Room rates are $169 based on single/double occupancy. The cutoff date for reservations is February 10, 2026. Reservations received after the cutoff date will be accepted on a space or rate available basis. Please call 1-800-468-3571 to book your stay with our group rate.

Trade Show Exhibits
Visit with exhibitors to become aware of tools, products and resources to more effectively manage technology risk. As an additional benefit for attendees, an exhibit area will feature companies showcasing their products and services of interest to security and technology personnel. All breaks and meals, plus the Wednesday after-hours reception, will take place in the exhibit area so that you will have plenty of opportunity to visit with the exhibitors.

Who Should Attend?
This conference is designed for those who are responsible for physical security, cybersecurity, fraud, IT planning, network administration, information security and operations, as well as any others who are responsible for making technology decisions at your institution, including senior management.

Cyber, Fraud & Physical Security Conference
March 4 - 6, 2026
Dept. 71

Name:_____

Bank:_____

Address:_____

City/State/Zip:_____

Email:_____

Phone:_____

FEES
Full Conference Attendee: $695

Payment Information - Total payable to the IBA Foundation, Inc.

(Please circle one) Check Enclosed Invoice Me VISA MasterCard AMEX

Cardholder Name:_____

Card Number:_____ Exp. Date:_____

CVV Code:_____ Zip Code:_____

Cancellation Policy
Cancellations received in the IBA office 14 business days prior to the scheduled program will be refunded in full. Due to commitments with the hotels, cancellations received less than 14 business days prior to the scheduled program are not refundable. Substitutions are welcome. Registrants who do not attend the program or send a substitute will be responsible for the entire registration fee.
Conference Exhibitors and Sponsors:
If IBA receives a written cancellation by February 18, 2026, you will receive a full refund less a $50 handling fee on exhibit rentals and sponsorships. There will be no refund on exhibit registrations or sponsorships after February 18, 2026.

Contact us for more info! mgibbs@indiana.bank 317-333-7161