May 21, 2026

9:00 AM–3:00 PM

West End Conference Center | St. Louis Park, MN (Break)

Limited Seats -First 50 Signed up

Cost: $75.00, 5 Sessions

Who should attend

- Bank and credit union fraud managers and investigators
- BSA/AML managers, analysts, and FIU leads
- Compliance, risk, and operations leaders responsible for alerting, investigations, and SAR quality

Session 1 | 9:15 AM–10:15 AM

Solving the SAR and Fraud Reporting Dilemma

Investigation with Precision

Hussian Jaber, Goodlabs, Toronto, Canada (flying in)

Problem statement: Alert volumes are climbing—and false positives are consuming your team's time. Meanwhile, true risk hides in the backlog, documentation varies by analyst, and deadlines tighten. This session is designed to help fraud and BSA/AML leaders regain control: faster triage, stronger investigations, and clearer SAR-ready narratives.

Walk away with tactics you can apply immediately—plus a modern, AI-enabled approach to streamline investigations end-to-end. You'll see how to reduce alert noise, prioritize high-risk activity, and move from "open alert" to "case-ready decision" faster, without adding headcount.

What you'll learn

- Prioritize the right alerts faster to cut time spent on false positives
- Use automated pre-investigation to gather context, enrich data, and tee up case-ready insights
- Standardize investigations with a clear hypothesis, evidence checklist, and audit-ready documentation
- "Show and Tell" how to connect entities and transactions to uncover networks and patterns that siloed tools miss

- Create stronger SAR decision-making and drafting with evidence-backed timelines and narratives (with human review)
- Build a plan for 24/7 fraud and compliance coverage as new payment rails expand

Bonus takeaway: a repeatable investigation workflow your team can adopt—what to collect up front, how to document decisions consistently, when to escalate, and how to produce clearer SAR-ready narratives so cases move faster with less rework.
Reserve your seat: Reply to this invite or contact *[Registration Contact]* at *[Email/Phone]*. Space is limited.

Session 2 | 10:30 AM–11:30 AM (break)

Check Fraud Automation That Stops More Losses—Earlier

Using Digital Imaging and Machine Learning to Cut Check Losses Fast

This is a Must-Learning Session on This Check Technology

John Ravita, SQN Banking System (Virtual Only for Attendees)

Check fraud moves fast—your controls have to move faster. In this session, you'll see how machine learning and image analysis can help flag suspicious checks in real time across check-processing channels. Next, learn how to use **encrypted 2D barcoding** to help validate, check authenticity, and detect common alterations (payee, amount, signature, and check stock). Finally, see how Positive Pay Payee validation can be streamlined by using OCR to capture payee names and automatically compare them to issued-item files, helping reduce manual review, improve decision consistency, and shorten time-to-resolution.

You'll also get a real-world case study showing how a small-to-midsize bank used automation to reduce manual touchpoints and improve consistency in check-fraud decisions. Check-fraud losses are rising, and financial institutions can't afford slow, inconsistent review—especially outside of business hours. See how always-on detection and validation workflows can help your team respond faster, reduce losses, and free investigators to focus on the highest-risk cases.

Session 3 11:45 am -12:15 (Lunch)

Call Impersonations and Spoofing

William Heathershaw | Technology Advisor

Caller ID spoofing allows fraudsters to impersonate businesses, deceive customers, and damage brand credibility. Without call spoofing protection, businesses can realize fraud losses, compliance exposure, and reduced answer rates. Spoof Protection verifies calls and **blocks unauthorized phone numbers before harm occurs**.

In financial services, such as banks, investment firms and insurance companies, spoofing and impersonation attacks are used to carry out account takeover (ATO) attempts targeting customers. Spoof Protection helps reduce these threats.

- Reduce exposure to phishing campaigns intended to defraud customers by accessing accounts and finances
- Enable only authorized enterprise numbers for customer outreach
- Reduce risk of customer deception during fraud alerts, payment verification or account recovery
- Block unauthorized calls to prevent ATO

Session 4 | 1:00 PM–1:45 PM

Social Engineering & Deepfakes: Protecting Customers and Your Institution

What we're seeing now + "show and tell" as visual examples."

Derek Schmidt | John McCullough

Social engineering attacks are getting more convincing—and more costly—for banks and credit unions. In this session, you'll learn how criminals use impersonation, urgency, look-alike messages, and deepfakes to trigger account changes and unauthorized payments. We'll share what we are encountering with these fraud/BSA groups and what you should watch for, along with practical controls, call-back/verification playbooks, and coaching tips to reduce losses and better protect customers.

Watch some deepfake examples and how fast technology is happening.

Session 5 | 2:00 PM–3:00 PM

Panel + Networking: What's Working Now in Fraud & BSA/AML

Join peers from banks and credit unions for a candid discussion on the biggest operational challenges and what's actually working in 2026. Bring your questions and swap playbooks on: alert reduction and prioritization, investigation documentation and SAR quality, check-fraud controls (Positive Pay and seal-based authenticity), impersonation/deepfake response, and building 24/7 coverage without burning out teams.