SLIDES 1–16 • FOUNDATION + THREAT-LED EFFECTIVENESS

1. Know the crime, know the money, then use TRACER

The class objective and operating shift

- Apply BSA fundamentals in a practical, risk-based way that produces useful intelligence: ask targeted questions → analyze better data → confidently decide → write useful SARs.
- The shift: less checklist completion and "just in case" filing; more threat awareness, defensible reasoning, pattern recognition, human judgment, FI cooperation/exchange of information, and quality over quantity.

Foundation: what are we actually trying to detect?

Core acronyms: BSA=Bank Secrecy Act • AML=Anti-Money Laundering • ML=Money Laundering • CFT=Countering/Combatting the Financing of Terrorism • TF=Terrorist Financing • PF=Proliferation Financing •CDD=Customer Due Diligence • EDD=Enhanced Due Diligence • SAR=Suspicious Activity Report • CTR=Currency Transaction Report • FI=Financial Institution •OFAC=Office of Foreign Assets Control • BO=Beneficial Owners • MSB=Money Service Business • PEP=Politically Exposed Person • PSP=Professional Service Provider

- The BSA's reach is broader than "banks." The deck highlights banks/credit unions/trust companies plus covered non-bank FIs such as MSBs, check cashers/money transmitters, currency exchangers/prepaid access, casinos, securities/commodities firms, insurers, precious-metals dealers, and loan/finance companies. More importantly are the non-covered FIs which are control gaps.
- Specified Unlawful Activity (SUA) is the predicate crime behind money laundering – Money laundering is a financial transaction involving the proceeds of SUA or designed to conceal the nature, location, source, ownership or control of those proceeds; or evading BSA recordkeeping or paying taxes on those proceeds.

Money laundering vs. terrorist financing

- In ML the funds are criminal proceeds; look for source of funds/wealth, layering, beneficial ownership, concealment, shell entities, rapid movement, and integration.
- TF asks primarily: Who will receive the money and what will it support? Funds may be legal, illegal, or mixed and may be small; focus on ultimate beneficiary, destination, affiliations, geography, intermediaries, sanctions connections, and purpose.

Recognize typologies, not isolated transactions

- Common ML/TF typologies in the deck: commingling; fraudulent documents; funnel activity; informal transfer systems; layering; shell companies/legal entities; structuring/smurfing; trade-based money laundering; and virtual-currency laundering.

TRACER — the workshop framework

T — Threats / Triggers: Know emerging threats in near real time.
R — Reprioritize: Shift attention and resources to what matters now.
A — Analyze: Get the right records faster; identify patterns and linkages.
C — Comprehend: Use human judgment: WHY did this happen; does it make sense?
E — Exchange: Share intelligence internally, with other FIs, and with law enforcement when appropriate.
R — Report: Produce useful SARs through investigation, linkage, fields/keywords, and strong narrative.

Threat-led BSA cycle: operationalize the threat

1. **Threat** — What crime, typology, or network are we concerned with?
2. **Vulnerability** — Which products, channels, customers, and geographies create exposure?
3. **Indicator** — What behavior or transaction pattern would appear at the bank?
4. **Control** — What monitoring rule, search, due diligence step, or staff observation would detect it?
5. **Outcome** — What should be documented, escalated, reported, or improved?

Turn external intelligence into local action

- Sources of Threats: negative news, local law enforcement, criminal subpoenas, 314(a), 314(b), frontline or internal referrals, SAR trends and law enforcement follow-up, fraud/loss data, national/international priorities, FinCEN issuances.
- Read FinCEN issuance as an action document ("operationalize"): capture filing keyword/field/contact instructions; list typologies/entities/products/channels/geographies/victims; convert red flags into bank-search questions; identify staff who need awareness; log monitoring, EDD, training, case-template, and reporting changes.
- Always ask: Where would this show up in our bank?

Frontline curiosity is a control

- Train 3 questions: (1) What changed from normal? (2) Does this fit what we know about the customer? (3) What should BSA know now?

Notes: _____

SLIDES 17–29 • RECORDS AS INTELLIGENCE (ANALYZE, COMPREHEND, EXCHANGE)

2. Open the case with questions, not random printouts

The five-question evidence map

1. **Identity** — Who is the customer and who actually controls the activity? Use CIP, beneficial ownership, signatures, online users, shared identifiers, state filings, and open-source data.
2. **Source** — What activity generated the funds? (Why is your customer getting $?) Consider ACH/wire originators, P2P, deposit items, checks, ATM & cash deposit logs, loan files, contracts/invoices; consider volume, location, timing, denomination, and structure.
3. **Use -**How were funds deployed? (What did your customer use the $ for? Typical household or business use? Or unusual **money movement**?) How quickly, where, and through which rails? Consider wires, over the counter withdrawals, ACH, cash, P2P, checks, monetary instrument purchases, credit card payments, ATMs, loans, night deposits, and transfers.
4. **Network** — What related accounts, owners, counterparties, addresses, devices/IPs, beneficiaries, or geographies connect the activity?
5. **Purpose** — What legitimate business or personal reason explains the activity?

CIP & Beyond / Beneficial Ownership / CDD: Ese the file to test the story

- Compare opening purpose, requested products, risk rating, expected source/use/volume/geography with actual activity.
- Are there name variants/DBAs, registered agent, ID-verification outcomes, address, phone/email, employer/occupation/industry, expected volume, IP/device, or commercial-mailbox indicators that can be verified or proven anonymous?
- For legal entities: owners/control person, formation date/state, licensing/operations footprint, or shared identifiers across otherwise unrelated customers.
- CDD is not just a form; it establishes what should make sense: who benefits/controls, normal source/use of funds, expected products/channels/geographies/counterparties/volumes, and what change should trigger EDD, investigation, or SAR decision.

Transaction rails: what to pull and what each can reveal

- Cash / Beyond CTRs: aggregate cash activity for analysis by customer, account, location, business day, signer, and related accounts. Test structuring, velocity, geography/timing, denomination, and whether the cash volume fits the business or employment model.
- Cash cross-check: combine CTRs, cash logs, cash-in/out, ATM/location/denomination data with ACH, wires, P2P, MIs, loans, and internal transfers; compare to peers and explain exceptions.
- Monetary instruments records: Consider multiple; Look at purchaser, remitter, payee, funding source, serial number/date, branch, signer; aggregate across people/branches/day and link purchase to later deposit/endorsement when possible.
- Wires: identify originator, beneficiary, FI chain, country, purpose/reference codes, request channel, IP/device/callback notes, exceptions/overrides, and relevant sanctions/FinCEN/internal watchlist hits.
- P2P / ACH / debit / ATM: counterparties, handles/memos, QR codes, rapid pass-through, ACH originator/addenda, school/insurer/government/payroll sources, merchant type, ATM location/time, deposit-withdraw pairing, out-of-area behavior, and essential-needs gaps.

The hidden evidence: ask, “What else do we know?”

- Fraud notes, complaints, disputes/Reg E claims, login history, IP/device/contact changes, mobile/RDC/check images and endorsements, loan/credit/employment/insurance files, merchant/treasury records, safe deposit box access and teller/referral observations.

Exchange + urgency: fill the gaps before you decide

- 314(b): registered participants may voluntarily share permitted information to identify/report possible ML, TF, fraud/SUAs, sanctions evasion, narcotics trafficking, and related crime. Useful for repeat actors, mules/common payees/shared IDs, rapid exits, student-aid rings, trafficking, and shell entities.
- Broad purpose – “to improve compliance program” – Shared information may include transaction/account facts, alerts/indicators/research, IP/device/geolocation, video/contact/payee details.
- Guardrails: verify participant, safeguard confidentiality, use only for permitted purposes, and never share SARs or SAR existence.
- Prioritize by harm + recoverability: Can funds be stopped/recalled/frozen/blocked/recovered? Is a victim/public program being harmed now? Is the activity TF, sanctions evasion, trafficking, or ongoing fraud? Can another FI/law enforcement fill a gap quickly? What filing/preservation deadline applies?

Recordkeeping output: the evidence grid

- For each evidence source document: what was reviewed → exact fact found → why it matters → what is still missing → whether it supports or refutes concern → decision impact.
- Decision impacts may include no SAR, escalation, SAR, EDD refresh, law enforcement, 314(b), OFAC escalation, or control changes. Document the date the bank actually determined the activity met the SAR standard; avoid labeling it “suspicious” prematurely.

Notes: _____

SLIDES 30–37 • REPORT, RE-PRIORITIZE

3. Turn evidence into a defensible decision and a useful SAR

SAR decision memo: organize the decision before drafting

- Suspicious activity: What exactly is unusual, unexplained, illegal-looking, evasive, harmful, or inconsistent with expected lawful activity?
- Chronology / available facts: Source and movement of funds, counterparties, channels, locations, other FIs/accounts.
- Subjects: Who conducted, attempted, benefited from, controlled, or facilitated the activity?
- Urgency: Victim issues, ongoing risk, law-enforcement/hotline contact, OFAC/sanctions action, or recoverability.
- Filing plan: Initial/continuing SAR, requested fields/keywords, related SARs, supporting documentation, and date of determination.

Write a story-based first paragraph

- A fact-based opening may list deposits and withdrawals but leave the reader asking, “Why is this suspicious?”
- A stronger opening gives Who + What + Amount + Timeframe + Why it matters. Link the customer’s stated profile to actual source, movement, counterparties/network, and the suspected typology.

SAR rule of thumb

- Do not just list transactions.
- Explain the suspicious activity the transactions reveal.
- The first paragraph should answer: “Why am I reading this?”

Quality-control check before filing

- Can the reader understand the suspicious activity in paragraph one? Are all key parties identified with roles, accounts, and locations?
- Does the narrative explain why the activity is inconsistent with lawful purpose/profile? Are requested keywords/fields included? Is supporting documentation complete and easy to retrieve? Useful beats long.

Prioritize -- Red flags: move from list to logic

- Do not count red flags as standalone rules. Cluster indicators by customer, channel, counterparties, timing, and purpose.
- Example: staffing company + ACH from construction firms + rapid cash/check exits + many individual payees + accompanied/coached workers + weak payroll explanation creates a connected pattern. The cluster matters more than “cash withdrawal = red flag.”

The Elephant in the room

- • Escalate facts—not accusations. Capture who appeared, what was said, who controlled the interaction, and what documents or transactions were observed. Curiosity is not confrontation.
- Community banking is personal; AML must remain professional. You are reporting activity you cannot reasonably explain—not “turning in” a customer you dislike or distrust.

Convert guidance to controls: one advisory → one action log

- Advisory intake: identify the risk, products, fields, red-flag clusters, SAR keywords, and contacts.
- Monitoring/tuning: identify queries/alerts that can find the universe of possible concern; if existing alerts detect it, refine/add additional factors that pinpoint the priority.
- Take out duplicated, non-useful, or reprioritized alerts.
- EDD: identify questions/documents that could validate lawful purpose. Train staff who can see behavior before the system does. Update risk assessment, metrics, case identification, SAR trends, exceptions, and control changes.

Board and management reporting through TRACER

- Threats: How does the threat apply to our customers/products/geographies/channels?
- Reprioritize: What resource/process changes follow?
- Analyze: What records/fields/system gaps limit investigations? Comprehend: Where can EDD explain activity—or fail to?
- Comprehend: Use your human judgment and consider the threat questions to make a decision.
- Exchange: Share information with other FIs, within your FI, and law-enforcement -- contact can change an outcome
- Report: What SAR trends show useful intelligence—not just more filings?

Notes: _____

SLIDES 38–46 • PRACTICE + CLOSE

4. Apply the framework to current typologies

Mini exercise: sudden ACH deposits + rapid P2P outflows + shared device

- Potential threats in the deck: student-aid fraud, mule behavior, and possible identity theft/straw-student activity.
- Ask: Which record do I open first and why? What CDD/EDD fact would change the decision? What pattern causes escalation? Which SAR keyword/field may be relevant if suspicious?

Payroll / labor exploitation: does "payroll" make economic sense?

- Estimate the workforce implied by revenue, contracts, locations, and operations. Compare payroll processor activity, EFTPS/federal tax payments, state withholding/unemployment, workers' comp, health benefits, payroll registers, employee rosters, Forms 941/W-2 summaries, and recurring employee payments.
- Explain large cash withdrawals/checks to individuals; search checks by maker/payee and common cashing patterns. Compare claimed electronic payroll with repeated large Friday cash withdrawals.
- Assess shell/staffing intermediaries: new entity, no/weak footprint, shared address, unrelated beneficial-owner history. Search exact shared values first—address, phone, EIN, email, device, IP, signer—and use 314(b) where appropriate.
- Human observations matter: Are workers, account holders, or representatives controlled, accompanied, or coached? Customer interaction records may be among the strongest evidence.

Durable Medical Equipment (DME) / health care fraud

- Trigger: a new medical supplier receives ACH credits and sends funds rapidly to foreign companies.
- CIP/BO: ownership/control/nominee indicators, licensing, provider footprint. Deposits: ACH originators/payors and volume versus business age/size. Exits: wires, checks, cash, MIs, digital-asset ramps, shell counterparties.
- EDD: contracts/invoices, tax/payroll, inventory, employees, patient/service legitimacy. Compare revenue with payroll, rent, inventory, licenses, suppliers, and real operations; map deposits to ultimate beneficiaries; look for shared identifiers across providers.

Federal student aid fraud: connect source, control, and exit

- Search ACH originators for schools, education-related payment facilitators/refund processors, and repeated refund patterns. Link customers by shared address, phone, email, device/IP, opening location, beneficiary, or organizer.
- Trace exits through cash, P2P, checks, wires, ATMs, or a common third party; compare to a real student profile: tuition, housing, books, meals, transportation, and ordinary living expenses.
- Escalate rapid funneling with little education/living activity; inconsistent school/enrollment/use-of-funds explanations; identity-theft/fraud history; or related SAR/314(b) information suggesting a broader ring.

Human trafficking: transaction pattern + control facts + frontline observations

- Trigger example: multiple late-night ATM deposits + P2P receipts with vague memos + immediate transfers.
- Review locations/timing, deposit-withdraw pairing, unrelated payors, rapid sequential payments, travel/lodging/prepaid activity, and unusual gaps in essential-needs spending.
- Capture who appeared, who directed, who possessed documents/cards, who transferred funds, and who benefited. Do not confront suspected victims or traffickers; follow internal escalation and law-enforcement protocols as appropriate.
- Host-city/event timing is context—not a standalone basis for suspicion. Record factual observations without speculation. When related to the cited World Cup Notice, use the requested keyword/field from the guidance.

Final TRACER check before closing a case

T — Threat: What threat/trigger am I actually investigating?
R — Reprioritize: What deserves attention now because of harm, urgency, or recoverability?
A — Analyze: Which records prove identity, source, movement, network, and purpose?
C — Comprehend: Does the activity make sense for this customer and lawful purpose?
E — Exchange: Who can supply the missing piece—fraud, operations, another FI, or law enforcement?
R — Report: What linkage, fields, keywords, and narrative make the SAR useful?

Remember

- See the threat. Follow the trail. Understand the WHY. Tell the story.
- Technology can help find the trail, but effective AML still depends on curious people who know how to think.

My action item: _____