BSA & Beyond

Moving from Compliance to Financial Intelligence

Kristen J. Stogniew, Esq., CFE
BankTalk - August 2026

Kristen J. Stogniew, Esq., CFE, Partner
kristen.stogniew@saltmarshadvisors.com

Today's objective

Explain my new practical framework for applying BSA fundamentals to achieve "effectiveness" while addressing real world AML/CFT priorities.

BSA & Beyond promise

- Ask targeted questions
- ↓
- Analyze better data
- ↓
- Confidently decide
- ↓
- Write useful SARs

YOU can do thi

Ask any question at any time

Basic Acronyms

BSA → Bank Secrecy Act

The foundational law authorizes the Department of the Treasury to impose reporting and other requirements on financial institutions and other businesses to help detect and prevent money laundering

ML → Money Laundering

Financial transactions involving the proceeds of specified unlawful activity

AML → Anti-Money Laundering

Preventing, identifying, and reporting money laundering

TF → Terrorist financing

Solicitation, collection or provision of funds – from legitimate or illicit sources – with the intention or knowledge that they will be used to support terrorist acts or organizations.

CFT → Countering/Combatting the Financing of Terrorism Preventing, identifying and reporting terrorist financing

PF → Proliferations financing

Providing funds or assisting with financial transactions that support the development, acquisition, or spread of nuclear, chemical, biological, or radiological weapons.

Financial Institutions *extract from 31 U.S.C. §5312(a)(2)*

✓ "Banks" which includes Banks, Credit Unions and Trust Companies

– "Non-Bank Financial Institutions" (NBFIs)

- ✓ Money Service Business
  - ✓ check casher
  - ✓ money transmitter
  - ✓ currency dealer or exchanger
  - ✓ issuer or seller of traveler's checks or money orders
  - ✓ provider of prepaid access
- ✓ Licensed casino or gaming establishment with annual revenue over $1,000,000
- ✓ Securities Broker/Dealer and Commodities Firm
- ✓ Insurance Company
- ✓ Dealer in Precious Metals, Precious Stones, or Jewels
- ✓ Loan or Finance Company (Residential Mortgage Loan Originator; Housing Government Sponsored Enterprise)
- – Persons involved in real estate closings and settlement *Final rule for title agents was effective ~~12/1/2025~~ 3/1/2026; Vacated by TX court
- – Investment banker or company *Final rule eff ~~1/1/2026~~ 1/1/2028
- – Persons engaged in the trade of antiquities
- – Automobile, boat, or airplane sales
- – Pawnbroker
- – Travel Agency
- – U.S. Postal Service

✓ *= is regulated under BSA/AML*

https://bsaaml.ffiec.gov/manual/Appendices/05 List of "Financial Institutions"

Specified Unlawful Activity extract from 18 U.S.C. §1956

- Bribery
- Commissions or gifts for procuring loans
- Counterfeiting offenses
- Theft, embezzlement, or misapplication by bank officer, agent or employee
- Human trafficking
- Human Smuggling
- Fraudulent bank entries
- False, forged or counterfeit statement, document or thing to influence the FDIC
- Fraudulent loan or credit applications
- Computer fraud and abuse
- Concealment of assets from conservator, receiver, or liquidating agent of financial institution
- Concealment of assets from bankruptcy trustee or creditors
- Bank and postal robbery and theft
- Financing of terrorism
- Firearms trafficking
- Trafficking in counterfeit goods and services
- Theft or bribery concerning programs receiving federal funds
- Mail or wire fraud
- Equity skimming
- Counterfeit/forged securities
- Theft or conversion of public money, property, or records including by government contract
- Threatening or injuring a family member of a federal official
- False oaths and claims
- Variola virus
- Congressional or cabinet officer assassination
- Goods falsely classified
- Entry of goods by means of false statements
- Smuggling goods into or from the united states
- Removing goods from customs custody
- Border tunnels
- Property mortgaged or pledged to farm credit agencies
- Espionage
- Transactions involving nuclear materials
- Destruction by explosives or fire of government property or property affecting interstate or foreign commerce
- Interstate communications
- Unlawful importation of firearms
- Conspiracy to kill, kidnap, maim, or injure certain property in a foreign country
- Murder
- Kidnaping
- Hostage taking
- Willful injury of government property
- Destruction of property within the special maritime and territorial jurisdiction
- Presidential assassination
- Child pornography
- Violence against maritime navigation or fixed platforms
- Copyright infringement
- Missile systems designed to destroy aircraft
- Radiological dispersal devices
- Receiving military-type training from a foreign terrorist organization
- Precursor and essential chemicals
- Aviation smuggling
- Transportation of drug paraphernalia
- Supplemental nutrition assistance program benefits fraud
- Foreign corrupt practices act
- Atomic weapon
- Activities with respect to North Korea
- Terrorist acts abroad against United States nationals
- Use of weapons of mass destruction
- International terrorist acts transcending national boundaries
- Providing material support to terrorists
- Destruction of aircraft
- Violence at international airports
- RICO offenses

Fraud IS Money Laundering...FinCEN 314(b) Fact Sheet December 2020 and again June 2020

U.S. Money Laundering Statutes

18 USC §1956 – Conducting or attempting to conduct a financial transaction in a way that conceals or disguises the nature, location, source, ownership or control; structuring to avoid recordkeeping; or evading taxes on… the proceeds of "specified unlawful activity" (aka "predicate offenses")

20 years imprisonment; $500,000 fine or 2x; forfeiture

18 USC §1957 – Deposit, withdrawal, transfer or exchange of funds >$10,000 of the proceeds of SUA. Knowledge is irrelevant.

10 years imprisonment; forfeiture

31 USC §5324 – Prohibits structuring

5-10 years imprisonment; up to $1mm fine; forfeiture

Those who AID or ABET have same punishment as if committed the crime

"Willful Blindness" the deliberate avoidance of knowledge = knowledge

ML vs. TF

Money laundering disguises the source of criminal proceeds.
Terrorist financing supports terrorism—whether the funds come from legal or illegal sources.

Investigation focus

•**ML:** Source of funds, source of wealth, unexplained income, transaction layering, beneficial ownership, and integration into the legitimate economy.
•**TF:** Ultimate beneficiary, destination, affiliations, geography, purpose, intermediaries, sanctions connections, and repeated small transfers.
•**Both:** Customer profile, counterparties, transaction purpose, account behavior, concealment, cross-border movement, and possible SAR escalation.

	Money Laundering (ML)	Terrorist Financing (TF)
Primary objective	Make illicit proceeds appear legitimate or usable	Raise, move, or use funds to support terrorism
Source of funds	Usually criminal proceeds	May be legitimate, criminal, or mixed
Main concealment concern	Where the money came from	Who will receive it and what it will support
Typical amount	Often larger or structured transactions	Can involve very small amounts
Common patterns	Layering, shell companies, unusual cash, rapid movement, asset purchases	Donations, remittances, crowdfunding, cash couriers, charities, personal transfers
Key question	"Is the customer disguising the origin of criminal proceeds?"	"Will the funds benefit a terrorist, facilitator, organization, or act?"

Common ML/TF Typologies

Typology refers to a documented method used by criminals to launder money or finance terrorism.

It describes the techniques, behaviors, and red flags associated with specific financial crimes.

- Comingling: Mixing illicit funds with legitimate business revenue.
- Charities and non-governmental organizations: Infiltrate legitimate or create fake ones to divert donations (TF)
- Fraudulent documentation: Falsifying invoices, contracts, or shipping records to hide ownership, origins or uses
- Funnel: Multiple deposits in one jurisdiction withdrawn in another – or vice versa
- Informal money transfer systems (e.g., Hawala)
- Layering: Moving funds through multiple accounts or jurisdictions to obscure origins and increase jurisdictional complexity
- Shell Companies & other legal entities: Fictitious or sham entities hide ownership and source of funds
- Structuring/Smurfing: Breaking large sums into smaller transactions to avoid reporting thresholds
- Trade-Based Money Laundering: Manipulating invoices or shipments to disguise illicit flows
- Virtual currency laundering: Using crypto exchanges, mixing services, and anonymous wallets to hide transaction

Create a shell company right here!

www.sunbiz.org

Why a new framework, Kristen?

Pace of change ↑

- New material to work with – Priority guidances and direct requirement to be risk-based
- Broadened sanctions – indirectly controlled persons/entities/vessels requires broader research
- Technology/AI – opportunities and threats for FIs and bad actors
- Stablecoin – opportunities and threats for FIs and bad actors
- Exploitation of U.S. gaps in global economy – antiquities, real estate, investment advisers, gatekeepers, payment providers

Federal agency exam strictness may have lightened…but States have not and FinCEN (as primary rule-maker) has been very busy (providing us material to work with).

Goal-post has moved, again => Less second guessing & imposing the auditor's preferred control, more allowing management to defend reasoning…Less "strict rules violations" alerts, more "threat-based" alerts…Less regulatory compliance, more financial intelligence.

So, what new processes do we need? Near real-time threat assessments…regular re-prioritizing/shifting of resources…better (faster, more comprehensive) data, data review, pattern recognitions…HUMAN understanding of the WHY of the activity…better FI cooperation…and better SARs – investigation, linkage, and narrative (quality over quantity, less "just in case")

✨ **TA-DAH.....!** ✨

T — Threats/Triggers

Know the emerging threats in near real time

R — Reprioritize

Continuously shift attention and resources to what matters most

A — Analyze

Get records faster, look more comprehensively, and recognize patterns and linkages

C — Comprehend

Use human judgment to understand **WHY** the activity is happening – does it make sense?

E — Exchange

Share intelligence and cooperate across financial institutions and enforcement agencies

R — Report

Produce better suspicious activity reports (SARs) through investigation, linkage, and strong narrative - quality over quantity

Threat-led BSA cycle

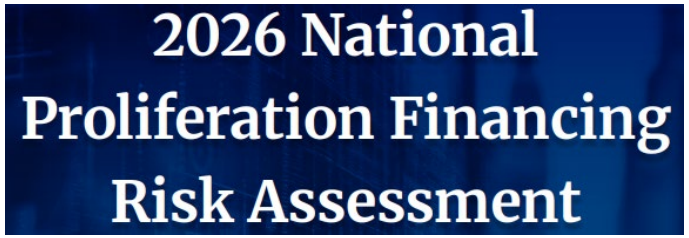
Start with the threat and work backward to the records and controls that actually or should happen ("operationalize").

- **Threat**: What crime, typology, or network are we concerned with (FinCEN or other source of priority)?
- **Vulnerability**: Which products, channels, customers, and geographies create exposure?
- **Indicator**: What behavior or transaction pattern would appear at the bank?
- **Control**: What control, monitoring rule, search, or due diligence process would detect it?
- **Outcome**: What would be documented, escalated, reported, or improved?

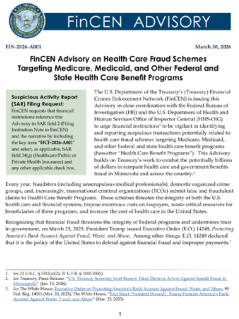
Where might we find threat info?

- Negative news

  (create a Google search for “fraud” “money laundering” “terrorist financing” and your state)
- Local law enforcement
- SAR filings – internal and regional – and law enforcement follow up
- Fraud & Financial losses to the Bank
- Frontline
- National & International priorities
- FinCEN Issuances

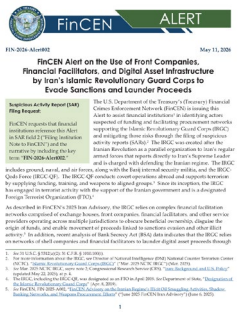


Recent FinCEN issuances (www.fincen.gov)

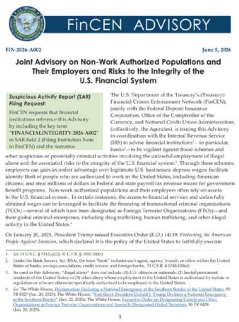


Health care fraud
3/30/2026

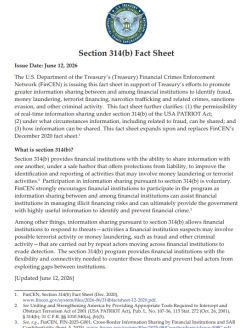
World Cup human trafficking
5/11/2026



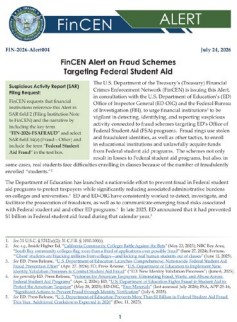
IRGC sanctions evasion
5/11/2026



Non-work authorized employer risk
6/5/2026



314(b) Fact Sheet
6/12/2026



Federal student aid fraud
7/24/2026

How to read a FinCEN advisory quickly:

- Highlight the SAR filing request: keyword, field, contact/escalation instructions
- List the named typologies, entities, products, channels, geographies, and victims
- Convert each red flag into a bank-search question
- Decide which staff need awareness: teller, wire desk, deposit ops, lending, treasury, fraud, audit
- Log control changes: monitoring, due diligence, training, case templates, board/risk reporting

Email me for an AI skill/prompt that will summarize FinCEN guidances in a useful format
Kristen.Stogniew@saltmarshadvisors.com

Also follow Sarah Beth Felix on LinkedIn as she explains how to operationalize these, as well as respond to enforcement actions

National priorities → local controls

The questions to ask…examples:

- **Fraud**: Who can receive government or insurance payments and quickly launder them?
- **Transnational Criminal Organizations (CTO)**: What geographies, counterparties, trade patterns, and funding flows matter?
- **Human trafficking/smuggling**: What cash, P2P, lodging, payroll, and control patterns are visible?
- **Cybercrime**: Which wires, ACH, P2P, mule accounts, and foreign beneficiaries need fast escalation?
- **Corruption/sanctions**: Which owners, front companies, and non-obvious control relationships need review?

Ask:
“Where would this show up in our bank?”

Frontline training: curiosity is a control

The frontline does not decide SARs. They surface the "something ain't right" moment early enough for BSA to act.

ASK before you assume

Train the first three questions:

1. What changed from normal?
2. Does this fit what we know about the customer?
3. What details should BSA know now?

Escalate facts — not accusations.

Frontline curiosity strengthens TRACER

T	**Threats**	Notice new scams, elder exploitation, mule cues, coaching.
R	**Reprioritize**	Escalate urgent/high-harm issues quickly.
A	**Analyze**	Capture the transaction, document, statement, or behavior.
C	**Comprehend**	Explain the customer context only they can see.
E	**Exchange**	Share internally with BSA, fraud, and operations.
R	**Report**	Give facts that improve SAR linkage and narrative.

Curiosity is not confrontation. It is community banking done well.

TRACER: Threats • Reprioritize • Analyze • Comprehend • Exchange • Report

Why TRACER is “effective”

A program is effective when it produces useful, timely intelligence—not just completed checklists.

- Team knows threats and priorities, to know what questions to ask and to spend appropriate time & resources doing it
- Customer Due Diligence (CDD) allows for identification of higher risk customers for applicable threats, and establishes expected (lawful) activity
- Team performs Enhanced Due Diligence (EDD) and investigates alerts and cases timely, using good records and techniques that are most likely to answer the questions
- SARs are complete, accurate, timely, and useful to law enforcement
- Risk/threat assessment and reporting adapt to guidance or activity changes

Effectiveness lens

Useful to law enforcement

Connected to real activity

Documented facts + decision

Feedback loops improve controls

Record retrieval plan: five questions & intro to evidence map

The BSA rules tells you to keep records. Effectiveness is knowing when and how to use them.

Open the case file with questions, not with random printouts.

1. **Identity**: Who is the customer and who actually controls the activity?
   - ✓ CIP, Beneficial Owners, signatures, online banking users, shared identifiers, state filings, open-source
2. **Source**: Where did the funds originate and are they lawful?
   - ✓ ACH/wire originators, check images, deposit items, cash logs, loan files, contracts/invoices
   - ✓ Consider volume, location, timing, denomination, and structure
3. **Movement**: How quickly, where, and through which rails did funds come and go?
   - ✓ wires, ACH, cash, P2P, checks, MIs, debit card, ATM, loan payments, night deposit, transfers, other bank records
4. **Network**: What related accounts, owners, counterparties, geographies, or devices connect the activity?
   - ✓ related accounts, counterparties, common devices, addresses, beneficiaries, ownership, geographies
5. **Purpose**: What legitimate business/personal reason explains the activity?

Every retrieved record should answer one of these.

CIP, Beneficial Ownership, and Customer Due Diligence

In an investigation, don't stop at "we have the four pieces." Use recordkeeping and due diligence to test the story.

- Opening purpose, requested products, risk rating, sources and uses of funds and expected activity (as compared to actual activity and uses/funding sources, geographies and products used)
- Check name variants, prior names, DBAs, registered agent
- SSN/ITIN/passport/foreign ID and verification outcomes
- Address, IP/device, phone, email, employer, occupation, industry, expected volume, and geographies
    - Is address a commercial mail receiving agency (e.g. UPS location or private mailbox service)?
- For legal entities: identify owners, control person, registered agent, formation date, formation state, and business/operations footprint
- Look for shared identifiers across unrelated customers
- Document whether facts are stale, inconsistent, missing, or explained

Effectiveness lens

Opening purpose

Expected activity

Control/Beneficial Ownership

Identifying information

Shared identifiers

Cash records: what to look for

Cash is not suspicious by itself. Patterns are.

- **Aggregation**: transactions by customer, account, location, business day, signer, and related accounts
- **Structuring**: repeated transactions below thresholds, split locations, split people, split instruments
- **Velocity**: cash in followed by immediate cash out, P2P, wire, MI, or transfer
- **Geography/timing**: ATM activity away from residence or late-night/early-morning patterns
- **Purpose**: does the business / employment model generate cash or need cash at that volume?

Effectiveness lens

Aggregation

Velocity

Geography

Purpose

CTR and cash log cross-check

A practical cash review usually requires multiple views.

- Pull CTRs, cash logs, cash-in/cash-out, branch location, ATM records, and denomination data
- Search by customer, signer, account, tax ID, address, phone, and cash handler
- Compare activity before and after risk events, guidance, media, business changes, and onboarding
- Map cash to non-cash rails: ACH credits, wires, P2P, monetary instruments, loans, and internal transfers
- Compare to peers
- Summarize exceptions in plain English: why the cash is or is not commensurate with profile and legal activity

Monetary instruments: the bridge product

MIs can connect cash, third parties, and distancing behavior.

- Search/sort by purchaser, remitter, payee, funding source, serial number, branch, date, and signer
  - Watch for remitter that is not a deposit customer, could be undisclosed purchaser and if for >$3k in cash, would require additional recordkeeping.
- Aggregate across business day, branches, accounts, and related persons
- Look for repeated purchases under recordkeeping or CTR thresholds
- Compare MI use to customer purpose: rent, payroll, school, travel, contractor, vendor, settlement
- Link MI purchase to later deposit or endorsement when possible

Effectiveness lens

Wire records: the fastest path to source and destination

Wire review must answer more than amount and date.

- Originator (our customer for outgoing wires, other side for incoming wires); Beneficiary (our customer for incoming wires, other side for outgoing wires); beneficiary FI, intermediary/correspondent FIs, country, payment purpose, reference codes
- Account number ≠ customer name
- Repeated beneficiaries, new beneficiaries, round dollars, rapid in-and-out, high-risk geographies
- Source of request – in branch, email, online (IP address?)
- IP/device or callback notes if available; exceptions or overrides to controls
- Screens against OFAC/sanctions, FinCEN keywords, high-risk jurisdictions, and internal watchlists

Evidence stack

Originator

Beneficiary

FI chain

Purpose

CDD link

P2P, ACH, debit card, and ATM *detail*

FinCEN guidance increasingly points to non-traditional clues.

- P2P: counterparties, memos, usernames/handles, QR codes, rapid pass-through, common destinations
- ACH: originator names, school/insurer/government-related sources, payroll processors, private ATM operators, returns, addenda
- Debit card: hotel, travel, gas, adult-service-adjacent merchants, unusual essential-needs patterns
- ATM: location, time of day, deposit/withdraw pairing, gas station usage, out-of-area behavior
- Card/P2P/debit activity may show control, exploitation, or mule behavior when cash/wires do not

Source: FinCEN FIN-2026-NTC1, Human Trafficking During the 2026 FIFA World Cup, May 11, 2026.

Other bank records: the “hidden” evidence

Modern investigations are not limited to BSA records.

- Fraud case notes, customer complaints, disputes, Reg E claims, suspicious login history, IP/device, phone number or email changes
- Debit card, ATM, mobile deposit, Zelle/P2P, ACH addenda, RDC images, check images, endorsement data
- Loan/credit files, employment/income docs, insurance docs, merchant processing, treasury services
- Teller/referral notes: who appeared, who spoke, who controlled the customer, who was present?
- Open-source and subpoenas: use consistently, document source and date

Ask frontline, loans and operations:
“What else do we know?”

Customer Due Diligence goal: know what should make sense

CDD is not a form; it is the basis for every monitoring decision.

- **Customer type**: new, seasoned, individual, cash-intensive business, Money Service Business (MSB), marijuana related business (MRB), Non-governmental organization (NGO), school-related, health care provider, staffing, import/export, VASP (virtual assets) exposure
- **Geography**: residence, operation, counterparties, wires, travel, foreign beneficiaries, high-risk/sanctions jurisdictions
- **Products/services**: cash, wires, ACH, remote deposit, P2P, debit card, MIs, correspondent, loans, merchant

✓ Who benefits from and controls the activity?
✓ What lawful activity do we expect for this customer?
✓ What source of funds and use of funds would be normal?
✓ What products, channels, geographies, counterparties, and volumes make sense?
✓ What change would be meaningful enough to refresh EDD, open an investigation, or file a SAR?

saltmarsh

314(b): information sharing is the missing link

Community banks rarely see the whole trail. 314(b) helps fill the gaps between institutions.

Voluntary safe harbor for registered participants sharing information to identify/report activity that may involve ML, TF, fraud/SUAs, sanctions evasion, narcotics trafficking, and related crime.

What it can solve

- Repeat actors moving bank to bank
- Mules, common payees, shared IDs
- Rapid exits and missing counterparty context
- Student-aid refund rings, trafficking, shell entities

What may be shared (broad)

- Transaction and account facts
- Alerts, indicators, research
- IP/device/geolocation data
- Video, contact, payee details

Receiver FI need not even have the other side transaction.

Guardrails

- Register and verify participant
- Safeguard confidentiality
- Use only for allowed purposes
- Do NOT share SARs/existence

TRACER takeaway: Exchange information early enough to improve the decision — SAR, no SAR, EDD, hold/recall, closure, or monitoring change.

Source: FinCEN Section 314(b) Fact Sheet, June 12, 2026.

Prioritize based on harm and recoverability

Fast action can change the outcome for victims and law enforcement.

- Can funds be stopped, recalled, frozen, blocked, or recovered?
- Is a victim, public program, or vulnerable person currently being harmed?
- Does the activity involve terrorist financing, sanctions evasion, trafficking, or ongoing fraud?
- Can another FI, law enforcement, or 314(b) participant provide missing facts quickly?
- What is the deadline for SAR filing, continuing review, and supporting documentation preservation?

Urgency is part of effectiveness.

Recordkeeping output: the evidence grid

Close every record review with a concise workpaper.

- **Record reviewed**: source system, date range, fields searched, and criteria used
- **Fact found**: exact activity, amount, date, party, channel, location, or exception
- **Interpretation**: why it supports lawful activity, unusual activity, or suspicion
- **Gap**: what cannot be determined and whether more information is needed (internal or external/314(b))
- **Decision impact (Conclusion)**: no SAR, escalation, SAR, EDD refresh, law enforcement, 314(b), OFAC escalation
    - Be careful of stating “suspicious” or “SAR” until it has been “determined” to meet filing requirements; document that date, and your process in Policies & Procedures.
- **Feedback:** risk rating, monitoring rule change, training, control, or board-reporting change

One grid makes the SAR easier.

Recordkeeping Output: Evidence Grid

Shows what was reviewed → what was found → why it matters → what conclusion it supports

Evidence Source	What Was Reviewed	What Was Found	Why It Matters	Supports / Refutes
CIP / CDD	Profile, occupation, address, expected activity	Restaurant employee; expected payroll and normal consumer spending	Sets baseline for activity review	Baseline
ACH / Payroll	90 days of incoming ACH	Payroll from 3 employers; funds quickly transferred out	May indicate third-party control of wages	**Supports concern**
Transfers	P2P, internal transfers, wires	Most incoming funds sent to one individual within 24 hours	Identifies who benefits from the funds	**Strong support for concern**
Shared Values	Phone, email, address, IP/device	Same phone/IP linked to 4 other customers	Shows possible network, not isolated activity	**Strong support for concern**
Branch / 314(b)	Teller notes + FI information sharing	Companion controlled ID; another FI saw same identifiers	Corroborates behavior and external connections	**Escalate**

Conclusion Evidence collectively suggests possible third-party control and networked activity; expand related-account review, document disposition, and file SAR if warranted.

Money Story → **Evidence Grid** → **SAR Narrative**

SAR decision memo

The SAR is the product of the investigation—not the objective. Quality over quantity.

Include:

- **Suspicious activity**: What exactly is unusual, unexplained, illegal-looking, evasive, or harmful (as compared to what you would expect and/or what you suspect is occurring)
- **Chronology/Available facts**: source of funds, movement of funds, counterparties, channels, locations, including other banks and accounts that are involved; ID the records that support the conclusion
- **Subject(s)**: Who conducted, attempted, benefited, controlled, or facilitated the activity
- **Urgency**: Any law enforcement call, hotline, OFAC, victim, or ongoing-risk action
- **Filing plan**: Initial/continuing, fields, keywords, related SARs, supporting documentation, date of determination

Story Based:

The first paragraph should answer "Why am I reading this?"

Fact-based vs. story-based SAR opening

Both use facts. The stronger opening tells the reader why those facts matter.

Fact-based opening

ABC LLC deposited 17 checks totaling $243,500 from January 3 through March 14. Funds were withdrawn by cashier's checks and cash. Bank reviewed account activity and determined it was suspicious.

- Facts are present but disconnected.
- No customer context or expected activity.
- **Reader still asks:** Why suspicious?

Email me for an AI skill/prompt for re-writing your SAR narrative

Story-based opening

Bank is filing because ABC LLC, a six-month-old lawn-care business expected to receive local customer payments, received $243,500 in insurance-related ACH/check deposits over ten weeks and moved 92% of the funds out within 48 hours to unrelated individuals and a foreign trading company. The pattern is inconsistent with ABC's stated business and suggests possible fraud-proceeds laundering through a newly formed company.

- Who + what + amount + timeframe + why it matters.
- Links profile, movement, and suspicion.

SAR rule of thumb: do not just list transactions — explain the suspicious activity the transactions reveal.

Quality control checks

A useful SAR passes these checks before filing.

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

Useful beats long.

The elephant in the room

You are not turning in your customer. You are reporting activity you cannot reasonably explain.

“Here is activity that does not make sense based on what we know, here is what we investigated, and here are the facts that may be useful to someone who can see a bigger picture than we can.”

Being a good TRACER does not mean being suspicious of your customers. It means being curious enough to recognize when their activity does not make sense or puts your bank at risk.
The hardest SAR you will ever file is on the customer you like. The customer you have known for years. The customer whose kids you know. That is exactly when we have to separate the person from the activity. We are not reporting the person because we dislike or distrust them. We are reporting activity because we cannot explain it.

Community banking is personal. AML has to remain professional. You can care about the customer and still report suspicious activity. Those two things are not inconsistent.

Red flags: from list to logic

Don’t count red flags, connect them

Ask whether the customer, channel, counterparties, timing, and purpose combine to create a suspicious pattern.

Human-trafficking example

A **single large cash withdrawal** may have a legitimate explanation.
But suppose you see:
A newly opened labor-staffing business receives ACH payments from several construction companies, rapidly withdraws much of the money in cash, writes checks to numerous individuals, has workers accompanied by the same person when they come into the branch, and cannot clearly explain its payroll process.
Now the indicators reinforce one another:
Customer: staffing company with questionable workforce structure
Channel: ACH in → cash/checks out
Counterparties: construction companies + numerous individuals
Timing: funds rapidly dispersed after receipt
Purpose: claimed payroll activity doesn't match normal payroll practices

That **cluster** is much more meaningful than saying, “cash withdrawal = red flag.”

Convert guidance to controls

After every FinCEN advisory, update at least one concrete thing.

- **Advisory intake sheet**: ID risk, products, fields, red flag clusters, SAR keywords, contacts
- **Monitoring/tuning**: ID fields and alerts that detect the typology
  - Can system query ID the universe of potential concern?
  - If alerts already detect, what additional factors should be considered in pinpointing the specific threat/priority?*
- **EDD checklist:** ID questions and documents to potentially validate lawful purpose of activity/red flags
- **Train:** staff who can see the behavior before the system does*
- **Reporting:** update risk assessment, metrics, ID cases, consider SAR trends, document exceptions and control changes*

One advisory → one action log

Board and management reporting

Report effectiveness through the TRACER lens—not just volume.

Threats: How does threat apply to our customers, products, geographies, and channels? Or, do we need more information in order to determine this?

Reprioritize: What changes will we make to existing processes to focus on this new priority?

Analyze: What records, fields, or system gaps limit our ability to investigate this threat?

Comprehend: Where will our EDD processes explain activity—or fail to explain it?

Exchange: What information sharing, fraud coordination, or law-enforcement contact has made a difference?

Report: What SAR trends show useful intelligence, not just more filings?

Exercises / Case Studies

Mini exercise: make a search plan

A customer has sudden ACH deposits, rapid P2P outflows, and a shared device with other new accounts.

- What threat(s) could this involve?
- Which record do you open first and why?
- What CDD/EDD information would help you decide suspicious (or not)?
- What transaction pattern would cause escalation?
- Which SAR keyword or field might be relevant if suspicious?

Answer pattern: student aid fraud + mule behavior + possible identity theft/straw student activity

Mini exercise: Questions of concern for payroll/labor exploitation

Are funds are being used for lawful payroll, or concealment?

- How many workers should the business have based on revenue, contracts, locations, and operations?
  - Do payroll processor/tax deposits/workers' comp records support the stated workforce? Does the claimed workforce make economic sense for this business?
- Why are large cash withdrawals or checks to individuals needed?
  - Search checks by maker/payee and identify common cashing patterns
  - A company claiming electronic payroll but repeatedly withdrawing $40,000 in cash every Friday as compared to a legitimate cash-intensive employer
- Do counterparties look like newly formed shells or staffing intermediaries?
  - Shell indicators: new entity, no footprint, shared address, unrelated BO history
  - Network-analysis tools are especially powerful: search the exact values first—same address, phone, EIN, email, device, IP, signer.
  - Where appropriate, 314(b) information sharing can help determine whether another FI sees the same network.
- Are workers, account holders, or representatives being controlled, accompanied, or coached?
  - The best tools are often the bank's own **human observations** and interaction records.

Some Customer, Third party, and Open-source Intel:

- NAICS/industry benchmarks
- Dun & Bradstreet/Hoovers or similar business websites and job postings
- Secretary of State records
- Google/Maps location checks
- contracts/invoices provided by the customer
- Website/domain search
- BBB records
- payroll ACH volume
- recurring payroll checks
- revenue flowing through the account
- number/size of operating locations
- EFTPS/federal tax payments
- state withholding and unemployment payments
- workers' compensation premiums
- health-benefit payments
- recurring checks/ACH credits to employees
- payroll registers
- Forms 941/W-2 summaries,
- workers' comp certificates or audits
- employee rosters
- payroll-processor reports

Source: FinCEN/FDIC/OCC/NCUA FIN-2026-A002, Non-Work Authorized Populations, June 5, 2026.

Mini case study: Durable Medical Equipment (DME) supplier with rapid exits

Trigger: new medical supplier receives ACH credits and wires to foreign companies.

- CIP/BO: ownership, control, nominee indicators, licensing, provider footprint
- Deposits: ACH originators, payors, payment volume versus age/size of business
- Exits: wires, checks, cash, MIs, digital asset ramps, shell-company counterparties
- EDD: contracts, invoices, tax/payroll, inventory, employees, patient/service legitimacy
- SAR: HCF keyword/field and all relevant money laundering boxes

How to decide whether activity makes sense.

- Compare revenue to payroll, rent, inventory, licenses, suppliers, and operations
- Identify whether owners or counterparties are unrelated to health care or recently formed
- Map ACH deposits to rapid movement and ultimate beneficiaries
- Look for shared identifiers across other health care providers
- Document whether the bank can reasonably understand lawful purpose

Source: FinCEN FIN-2026-A001, Health Care Fraud Schemes, Mar. 30, 2026.

Mini case study: ACH search for student aid refund patterns

Refunds can look legitimate until you connect source, control, and exit activity.

- Search ACH originator names for schools, education-related payment facilitators, refund processors, and repeated credit patterns
- Identify shared addresses, phones, emails, online-banking devices/IPs, opening locations, beneficiaries, or organizers
- Trace exits: cash withdrawals, P2P transfers, checks, wires, ATM activity, or transfers to a common third party
- Compare activity to a real student profile: tuition, housing, books, meals, transportation, and ordinary living expenses
- Escalate when refund funds funnel quickly with little education/living activity or indicators of identity theft, straw students, or organizer control

Concerning activity:

- Multiple customers linked by same contact information, device/IP, opening location, beneficiary, or organizer
- Rapid movement of refunds with little education, housing, food, books, transportation, or normal living activity
- Customer statements inconsistent with school, payment source, enrollment, or use of funds
- Prior fraud claims, identity theft reports, returned items, disputes, or law-enforcement contact
- Related SARs or 314(b) information showing a broader refund-fraud ring

Source: FinCEN FIN-2026-Alert004, Federal Student Aid Fraud, July 24, 2026.

Mini Case Study: Human Trafficking

Trigger: account shows multiple late-night ATM deposits, P2P receipts with vague memos, and immediate transfers.

- Frontline: capture behavioral observations and avoid confrontation
- Cash/ATM: time, location, gas station/hotel/event proximity, deposit/withdraw pairing
- P2P/card: vague memos, multiple unrelated payors, three rapid sequential payments, travel/lodging/prepaid cards
- EDD: possible victim, trafficker, facilitator, or business account with no payroll/essential-needs pattern
- SAR: FIN-2026-HTWORLDCUP and field 38(h) when related to the Notice

What the SAR needs to make the activity useful

- Locations and timing: branches/ATMs/merchants, dates, late-night or event-related concentration
- Parties: account holders, payors, beneficiaries, phone numbers, online ad contact if known
- Control facts: who appeared, who directed, who transferred funds, who benefited
- Transaction pattern: cash/P2P/card/prepaid/travel/essential-needs gaps
- Law enforcement/hotline contact and internal escalation details

Source: FinCEN FIN-2026-NTC1, Human Trafficking During the 2026 FIFA World Cup, May 11, 2026.

Human trafficking: Teach cues to frontline

Customer-facing staff may be the only people outside traffickers who interact with victims.

- Coach staff not to confront suspected victims or traffickers; escalate internally and contact law enforcement as appropriate
- Look for third-party control, coaching, lack of possession of documents/cards, fear, or inability to answer independently
- Use host-city and event timing only as context—not as a standalone reason for suspicion (nor a requirement for suspicion)
- Train tellers, call center, branch managers, security, and fraud teams on escalation paths
- Capture factual observations in case notes without speculation

Source: FinCEN FIN-2026-NTC1, Human Trafficking During the 2026 FIFA World Cup, May 11, 2026.

YOU can do this.

The future of AML is not about replacing judgment. It is about strengthening it.

Technology can help find the trail.
But YOU are the TRACER.

- **Ask good questions**
- **Follow the money**
- **Understand the WHY**
- **Tell the story**

Effective AML still depends on curious people who know how to think.

Thank you — Kristen J. Stogniew, Esq., CFE, Partner | Saltmarsh | kristen.stogniew@saltmarshadvisors.com

The TRACER workflow

This is the spine of the workshop: start with the threat and end with a useful SAR.

T — Threats (also Trigger): What threat is emerging and how would it appear here?

R — Reprioritize: What deserves attention now—and what can be dismissed or postponed?

A — Analyze: Which records reveal identity, source, movement, purpose, and network (related accounts, counterparties, owners, geographies)?

C — Comprehend: Does the activity make sense for this customer? Lawful purpose? Outlier to peers?

E — Exchange: Who else can supply a missing piece—fraud, operations, another FI, or law enforcement?

R — Report: What narrative, linkage, fields, and keywords make the SAR useful?

See the threat. Follow the trail. Understand the why. Tell the story.