What to include in a SAR

- A factually accurate and concise introduction statement in your narrative about what is suspicious in the context of your business. Then focus on the who, including not only traditional identifiers but also non-traditional identifiers and digital clues.
- Summary of transactions + full listing of transactions in an attachment
- Traditional identifiers
- Non-traditional “Cyber” identifiers (See Appendix A)
- Sources of OSINT Research: If you find useful OSINT, would be great to either capture the link, screenshot it, or archive it through wayback machine, if possible. (web.archive.org). Will make our research and documentation of the OSINT much easier
- Statements or communications with account holder (Depending on the nature of the communication – might determine how its included either in narrative or as an attachment)
    - Documented discussions
    - Memorandums of contact
    - Questionnaire responses
    - Notes from phone call

- Associated accounts
    - Linked proactively by customer
    - Maybe not in the same name as subject but can be linked through investigation/research, examples:
        - use of same IP for account creation or login
        - use of similar KYC or supporting documentation
        - use of similar email accounts
        - account behavior similarities
        - cookies
        - device fingerprint
        - primary, recovery, or 2FA phone number
        - deposit or withdrawal VA addresses
- Direct contact information
    - Name, email address, and direct phone number of analyst or preparer
    - Understanding every organization works differently - if we can’t talk to the person who witnessed or analyzed the suspicious activity…at a minimum, an email address that is monitored regularly in order to request supporting documentation.
- Other Useful information (FAQs that are appropriate for the circumstances)
    - General rules that help LE understand how your operations work.
        - (Example: every account holder receives their own unique deposit address per asset vs. one deposit address for all users)

Appendix A

Non-traditional identifiers that are helpful to LE (where available)	
IP addresses w/timestamp	Digital asset tracing graphs
Digital asset addresses (withdrawal & deposit)	Digital asset transaction hashes
Domain names	Email addresses
Social media accounts	Chat application usernames
Fintech app usernames	Online monikers
Profile photos	Metadata from photos or other files submitted
Geolocation (if available)	Device IDs

IP Addresses

- A list of IP addresses and time stamps
- Great to differentiate between account creation IP vs. login IP (if different)
- Would be great if you can flag IP addresses that you know through research as being associated with a VPN or Proxy.

Digital Asset Tracing/Graphs

- If you use a blockchain analytics tool like Chainalysis, TRM, or Elliptic, and do some tracing – it would be great to include your graph as an attachment to the SAR (ideally in native format – or can also do .png if small enough)

Digital asset addresses

- Inbound and outbound addresses (withdraw to/deposit from)
- Any other known digital assets associated with account holder
- Include transactions hashes where available

Domain names

- Usually when we're talking about frauds or investment scams
- What sites are victims going to.

Email addresses

- Primary and recovery (if available)
- Others used to contact customer service

Social media account IDs

- Tiktok

- Snapchat
- FB
- Twitter
- Linkedin
-

Chat application usernames

- Telegram
- Signal
- Jabber

Fintech app usernames

- $cashtag
- Venmo

Other online monikers

- Forums for example (reddit, bitcointalk, etc.)