SAR Requirements

Key Purpose of a SAR

- Identifying Trends
- Preventative Measures – Law enforcement can have trends in financial crime.
- Investigative Tool for Law Enforcement
- SAR Thresholds

Suspicious Activity Review and SAR Decisioning Exercise

- Document the Suspicious Activity.
- Report if you would file the SAR or not.
- Write the SAR Narrative.
- Provide the Escalation Procedures followed from time the activity was deemed suspicious through the time the SAR was filed or determined not to need to be filed.

Suspicious Activity Review and SAR Decisioning Exercise

- Each table will have a Scenario
- You have 10 minutes to discuss at your table.
- Each table will have 5 minutes to report how they handled.

Scenario 1 – SAR Narrative - Regulation E Claim – Account Takeover

- *Bank is filing this SAR to report account takeover totaling $57,103 involving Customer A, age 67, of City, ST. The activity took place between 4/14/2025 and 4/30/2025. No suspect has been identified.*

- *On 5/1/2025, Customer A came into the branch with a printout of his checking account activity. He did not recognize the external transfer made on 4/30/2025 nor the Account Verification deposits on 4/29/2025. He stated that he only uses his online banking on his desktop at home and has never set up an external transfer. On 4/15/2025 there were also online transfers from his Home Equity Line of Credit ("HELOC") that he did not initiate.*

- *Additional notes on the account indicate that on 4/15/2025 a fraudster called in to Bank posing as the member from phone number 555-555-5555. Customer A stated that he had not received any suspicious calls or text messages. However, Customer A did state that he had received a pop-up stating that there was malware on his device and the software was going to clean the device to remove the malware.*
- *Review of account activity identified numerous disbursements from Customer A's HELOC into his checking account along with a bill pay transfer, and an ACH external transfer out.*

Scenario 1 – SAR Narrative - Regulation E Claim – Unauthorized Transfers

The following New Jersey IP addresses were associated with transfers and online banking activity: 11.11.111.111 and 22.22.222.222.

- *A description of the unauthorized activity is as follows:*

- *4/14/2025: $9,500 HELOC disbursement to checking account*

- *4/15/2025: $9,500 transferred from checking account to the HELOC, $1.89 moved from checking account to the HELOC, a $9,500 HELOC disbursement to checking account, and $9,500 moved from checking account to the HELOC account;*

- *4/29/2025: $0.34 ACH deposit to checking account from Person 1, a $0.46 ACH deposit to checking from Person 1, and an $0.80 ACH withdrawal from checking account from Person 1; and*

  4/30/2025: $9,500 ACH external transfer to Person 1, a $9,500 HELOC disbursement to checking account, and $9,500 moved from checking account to the HELOC account.

- *All affected accounts were closed and new accounts opened.*

Scenario 2 – SAR Narrative – Debit Card Fraud Ring

- Bank is filing this SAR to report 20 individuals that opened or attempted to open checking accounts to use their debit cards for fraudulent activity at gas stations. The activity occurred from 4/14/2025 to 6/28/2025. The majority of the individuals in this suspected fraud ring lived around 2 hours from the closest Bank branch with most living in Lumberton, Rowland, or Fairmont, NC. The individuals that were successful in opening their accounts would make a small deposit at account opening, usually in cash, to cover the pre-authorization holds gas stations may place on the card to ensure funds are available before you pump gas.

- The gas station activity took place in the same geographic area including Lumberton, St Pauls, Clinton, Fayetteville, Pembroke, Hope Mills, Stallings, Rowland, Tar Heel, and Warsaw, NC and Dillon and Hamer, SC.

- We have attached 323 transactions which include 172 $1.00 preauthorization charges and 150 posted charges totaling $29,930.37. Banks loss from this activity is $29,650.37.

- All accounts have been closed.

Scenario 3 – SAR Narrative – Debit Card Fraud

- *Bank is filing this SAR to report fraudulent debit card activity totaling $10,242.66 involving Customer A, age 20, located in Charlotte, NC. The activity occurred between 6/15/2025 and 6/20/2025.*
- *On 4/15/2025, Customer A opened checking and savings accounts. There was no activity in the accounts until 6/4/2025.*

On 6/4/2025, Customer A made a $4,000.00 cash deposit into his checking account.

Soon after the cash deposit, Customer A began making numerous and frequent debit card transactions.

On 6/11/2025, Customer A made a $1,000.00 cash deposit into his checking account.

- *Between 6/16/2025 and 6/19/2025, Customer A made numerous transactions, including Walmart and Wells Fargo ATMs. He then contacted Bank to report that the transactions were not completed or authorized by him. He received provisional credit in the amount of $5,304.00.*
- *Once the provisional credit was posted, Customer A made a cash withdraw for the full available balance of $5,304.00 on 6/20/2025.*
- *After conducting an investigation into the debit card claim, it was determined that no error occurred and Customer A was responsible for the debit card transactions. Provisional credit was reversed from Customer A's account, causing an overdraft.*
- *This fraudulent debit card dispute claim resulted in a loss of $4,912.50 to Bank.*
- *See Part I for the information we have on file for Customer A.*

Scenario 4 – SAR Narrative - Check Fraud Investigation

- *Bank is filing this SAR to report check fraud by customer/suspect Customer A, age 69, of Gibsonville, NC involving 2 checks totaling $51,917.34 deposited on 11/20/2024 and 12/13/2024. We are listing Customer A as the sole suspect in this SAR. It is believed that he is involved in obtaining funds via the internet and is being used as a Money Mule.*

- *On 11/20/2024, Banks branch received a $4,917.34 mail in deposit for Customer A. It was a bill pay check from Individual A, located in City, SC. The check was made payable to Customer A to be deposited in his checking account. The check was drawn on XYZ Bank. It subsequently returned as an altered/fictitious item. Bank gave Customer A the benefit of the doubt and closed the affected account and opened a new account for him. Due to the hold on the check, no funds were spent.*

- *On 12/13/2024, Customer A walked into Bank branch and deposited a check for $47,000.00 into his new checking account. It was from Mister and Miss Individual, located in City, KY and drawn on ABC FCU. An extended hold was placed on the check and no funds were spent. The check subsequently returned as unable to locate.*

- *Banks fraud investigator placed lockouts on Customer A's accounts and restricted him to in branch transactions only.*

Scenario 4 – SAR Narrative - Check Fraud Investigation

- *On 12/24/2024, Customer A went back to the branch and tried to negotiate having the lockouts removed. He was asked about the check for $47,000.00. He stated he received it from his online boyfriend, because his boyfriend needed help. (However, it is noted that that is not the maker on the check). At that time, he was told to stop communicating with people online and that the restrictions would remain.*

- *No funds were lost as a result of these 2 checks due to extended holds being placed.*

- *It is believed that Customer A is involved with fraud involving people he meets on the internet, and we are listing him as the sole suspect in this SAR.*

- *See Part I of this SAR for the current information on file for Customer A who has had various checking, savings, and loans since 2006 with no prior incidents.*

Scenario 5 – SAR Narrative – Check Fraud – Real Estate Investment Scam

- *Bank is filing this SAR to report check fraud involving Victim A, age 60, of City, NC. The activity took place on 4/2/25 and involved a check deposit in the amount of $179,500.00.*
- *Customer A established accounts, including loans, with Bank in May 2016. There has been no prior concerning activity for Ms. Little.*
- *On 4/2/25, Customer A visited Bank's branch in Greensboro, NC to deposit a check in the amount of $179,500.00 from the JP Morgan Chase account belonging to Individual XY of City, NJ. The check returned on 4/7/25 as altered/fictitious.*
- *Front line staff reached out to Customer A regarding the deposited check. Customer A stated that she received the check via priority mail from a prior classmate at University. She stated that the source of the funds for the check was for a return investment in New York real estate that numerous other classmates she had not spoken to in years also contributed to. Customer A confirmed that she had not spoken to her classmates in many years and had only recently been in contact via social media. Customer A provided that she felt comfortable that it was a classmate since they discussed times in college prior to discussing the investment opportunity.*
- *Customer A stated that she wired her classmate $50,000.00 for the investment, but that activity did not take place at Bank. For the returned investment, her classmate sent the check with instructions on how to distribute the funds to the other classmates that had invested.*
- *Bank educated Customer A on the scam and advised her to use caution going forward. She confirmed that she did not provide her account information to anyone.*
- *There was no loss to Bank and Bank has not identified a suspect.*

Scenario 6 – SAR Narrative – EFE

Referencing FIN-2023-PIGBUTCHERING, EFE FIN-2022-A002

- *Bank is filing this SAR to report elder financial exploitation and suspected pig butchering involving customer/victim Customer A, age 74, of City, NC. Customer A has had various accounts and loans with Bank since 2009. The suspicious activity we are reporting started on 1/12/2025 and runs through 7/1/2025. The activity involves the use of Customer A's home equity line of credit ("HELOC"), a home equity loan, and Edward Jones Investment funds for $373,652.32 used for suspicious outgoing wires, cash withdrawals deposited into bitcoin ATMs, a suspicious debit card purchase at Food Lion, and suspicious Uphold, Cash App, and likfli.us transactions. No suspect has been identified. Customer A shared that the scammers reached out to him via WhatsApp and telegram messaging apps.*
- *Between 1/12/2025 and 2/18/2025, Customer A used 3 disbursements from his HELOC and a disbursement from his home equity loan to wire $36,620 to the ABC Credit Union account of Scammer A located in City, GA and to wire $9,000 to the XyZ Bank account of Fake Business LLC, located in Hollywood, CA.*
- *It is noted that on 2/18/2025, he took out a new home equity loan and used some of the funds to pay off his HELOC.*
- *For these transactions, he later explained that he met this person on WhatsApp and that Scammer A was like a family member with her father being a good friend of Customer A's in the 1970s although he never asked her any identifying information questions about her father. He said he wired her the funds because she was a military contractor stationed in Yemen and needed to get back to the states after her contract was complete, but she needed to buy her way out of Yemen.*

Scenario 6 – SAR Narrative – EFE

- *From 2/19/2025 to 2/24/2025, Customer A started having out of pattern Cash App and Uphold (a digital money and trading platform) transactions. He had one incoming $166.60 Cash App deposit and 19 Cash App payments totaling $520.00 out, all with his name in the description. He also had 2 Uphold transactions in totaling $1,330.87 with description UPHO*CustA and 22 Uphold transactions out totaling $2,668.00.*

- *On 2/24/2025, he wrote a personal check for $2,000 from his checking account and cashed it and then withdrew another $4,000 in cash from his checking account the next day.*

- *From 2/27/2025 to 3/11/2025, he received $16,321.14 via 3 ACH transfers from Edward Jones - Investment and withdrew $16,000 in cash over 3 withdrawals.*

- *On 4/25/2025, he sold his house. Between 4/25/2025 and 4/29/2025, he received $384,831.93 via 2 wires and one check from Real Estate PLLC for the proceeds for the sale of the home and used $281,800.00 of it to send 3 wires to the Other Bank account of Scammer Trading, located in CA. The check was used to pay off his home equity loan.*

- *From 4/30/2025 to 5/21/2025, he used some of the proceeds to withdraw $18,000 in cash via 3 withdrawals.*

Scenario 6 – SAR Narrative – EFE

- *It is also noted that he had 3 out of pattern likfli.us internet transactions totaling $46.85. A Google search has those commonly linked to fraud.*
- *For the transactions that took place from 2/19/2025 to 5/21/2025, he shared that he received a job offer on WhatsApp for a job working for Social Media and that the female he was communicating with said she was a team lead of the media department who was training a staff of 500 people to scan all incoming materials to proof and send edits back. According to Customer A, he was working closely with this woman and started dating her. He thought he was getting paid by Uphold and that the Uphold transactions he initiated out were for service fees and to keep jobs coming to him from Social Media. For the wire transfers to Scammer Trading and the cash withdrawals, the girlfriend opened bank accounts and bitcoin accounts and send him a screen shot of the new accounts. His cash withdrawals were deposited into bitcoin ATMs because he thought they were investing together and the wires were supposed to be used for a place that he and his girlfriend were going to buy in Florida. Customer A noticed that the last wire he sent went to California and didn't understand why wires would go there when his girlfriend supposedly lived in New York. He could not locate the screen shot of the bank and bitcoin accounts his girlfriend shared with him.*
- *Due to concerns that Customer A was being scammed, his checking account was closed and a new one opened on 6/13/2025.*
- *On 7/1/2025, he used his debit card for a $1,500 purchase at a Food Lion in City, NC, which indicates that he may still be involved in a scam. His account balance is now down to under $300.*
- *In summary, we believe that Customer A was the victim elder financial exploitation and possible pig butchering involving one, or multiple, scams.*
- *Transactions details attached.*

Scenario 7 – SAR Narrative – Elder Financial Exploitation/Money Mule

- *Bank is filing this SAR to report money mule activity involving Customer A, age 69, located in Asheboro, NC. The activity took place between 7/7/2025 – 8/7/2025 and totaled $368,529.99 (in actual and attempted transactions). We believe Customer A to be a willing participant in mule activity, and it is noted that Customer A has been served mule notices by law enforcement. Customer A opened accounts on 6/23/25.*

- *On 7/7/25, Customer A deposited a check in the amount of $150,000.00 from John Smith and Sally Smith, located in Hawaii. The memo on the check referenced "payment". Customer A claimed the remitter was a longtime friend whom she lent money to a couple of years ago, and the check was to pay her back and was received through the mail. However, Customer A did not know the name of her friend, the city the friend lived in, or the bank the check was from.*

- *On 7/17/25, Customer A sent a wire transfer in the amount of $70,000 to Coinbase. The purpose of the wire referenced OTHR. The wire was returned on 7/18/25 due to an invalid account number. Customer A later told a bank investigator that she wrote down the account number incorrectly by mistake.*

Scenario 7 – SAR Narrative – Elder Financial Exploitation/Money Mule

- *On 7/19/25, Customer A sent $15,000 to Uphold.*
- *On 7/21/25, Customer A sent another $15,000 to Uphold.*
- *Customer A later told a bank investigator that the Uphold transfers were done to pay down her loans.*
- *In addition to the Uphold transfers on 7/21/25, a wire in the amount of $70,000 was sent to Coinbase. The purpose of wire referenced CASH. She later told a bank investigator that the funds were going to her retirement accounts at Merrill Lynch, through Coinbase.*

Scenario 7 – SAR Narrative – Elder Financial Exploitation/Money Mule

- *On 7/24/25, Customer A visited the branch to send another $20,000 wire to Coinbase for the purpose of Bitcoin Investment. The Banks wire department canceled the wire due to suspected fraud, and Fraud Prevention placed lockouts on the account for further investigation.*

- *On 7/25/25, Customer A visited the branch to inquire about the account lockouts. She stated that her wires and transfers were to pay off some loans and credit cards. She said she does not expect to send any more money after the $20,000 wire and requested to speak to someone in Fraud Prevention. In addition, she attempted a transfer to Coinbase in the amount of $29.99, that was returned due to the account lockout.*

- *On 7/29/25, she withdrew $500 cash.*

Scenario 7 – SAR Narrative – Elder Financial Exploitation/Money Mule

- *On 7/30/25, Customer A visited the branch wanting to withdraw $28,000 in cash from her checking account for home improvements/renovations, including wood floors and new bathrooms. She stated that the contractor requested to be paid in cash.*
- *Further discussions with Customer A by the Banks investigator determined that she was involved in a romance scam. She stated that she has a boyfriend in South Africa, a contractor, that needed money to get back home; most recently $20,000.00. In addition, he gave her advice on moving money and helped her set up Coinbase and Uphold for investments.*
- *Customer A indicated that she was aware she was being scammed and stated she would stop the activity; but later returned to the branch on 8/7/25 requesting another cash withdrawal.*
- *Since Customer A received education regarding money laundering, understood the process of working with law enforcement to return the funds to the remitters of the check, admitted to falsifying the purpose of the wires, admitted to understanding she was in a sweetheart scam, and admitted to not knowing the person who sent her the original funds, she is now considered a witting money mule and we are reporting her as a suspect.*

High Risk Review & Lessons Learned

Facts of Case:

- Alerts in AML System
- ATM activity increased
- Front Line activity (e.g., cash withdrawals, ATM settlements, etc.)
- Good customer of the branch
- High Risk Review leading to Enhanced Due Diligence
- SAR filing decisioning
- Subpoenas
- Account Closing Decisioning