

# Anatomy of a Financial Crime

Christopher Westphal  
Visual Analytics Inc.  
20010 Fisher Avenue, #200  
Poolesville, MD 20837  
[www.visualanalytics.com](http://www.visualanalytics.com)

## **Abstract**

Each day millions of financial transactions occur throughout our banking and finance systems. Whether people are writing checks, depositing cash, wiring money, or using ATM machines, their transactions are logged and recorded. All major banks, thrifts, savings & loans, credit unions and financial institutions are required to have certain protocols, reviews, and detection systems in place for exposing suspicious behaviors. The example depicted in this paper provides the realistic background and description of a single money laundering scenario. There are literally thousands of different combinations, variations, and factors involved in detecting, analyzing, and investigating financial crimes. This paper does not attempt to articulate an all-encompassing approach or solution for addressing financial crimes; rather it presents several facets and indicators that can help expose criminal endeavors.

*Keywords: money laundering, analytical tools, link analysis, structuring, suspicious reports, visualization, criminal investigation*

## **Introduction**

As he has done for the past ten months, John walks into a bank with a thick envelope full of money, mostly in worn ten and twenty dollar bills, to make his semi-weekly deposit of about \$8,500. It was a busy week for John who distributes methamphetamines in a neighborhood located about 20 miles from the bank. He has been using this particular bank for almost a year as he does not want to deal with banks closer to his apartment because he is concerned the tellers may learn about his drug dealings and will wonder how he got the money and ultimately ask too many questions.

John has told the tellers at this bank that he runs a courier service and most of his clients pay him in cash. The tellers know John by name and warmly greet him when he enters the bank. John started his drug dealings back in college where he met his current suppliers and established a small, but reliable, client base. Over the past several years, John has expanded his operations to afford him a very comfortable lifestyle.

John lives in a rented apartment in a neighborhood near where he deals his drugs. Although John does not use the drugs himself, he has been in jail a few times for possession with intent to distribute. John prefers to sell methamphetamines because they are synthetic stimulants that are easy to produce and can be highly addictive. Common street names for meth include crystal meth, crank, speed, and shabu – to name a few. John prefers using the term “ice.” What was once considered a drug only used by students cramming for tests or truck drivers on a long haul is now commonly used across all facets of society. John’s clients include housewives, businessmen, cab drivers, chefs, and even a local newscaster.

One factor that contributes to wide-spread meth consumption is the availability of its ingredients – they can be readily purchased at any hardware store, grocery store, drug store, or convenience mart. Meth is straightforward to make using a variety of materials including antifreeze, battery acid, drain cleaner, starting fluid, and pseudoephedrine (from common cold medications). Although meth production is fairly simple, John does not manufacture his own drugs because it adds more risk to his operations, and his supplier has always been timely with his deliveries. The street price John charges for his “ice” is about \$800/ ounce,

depending on the quality he gets from his supplier.

John completes his transaction at the bank without a hitch; the money is accepted by the teller, credited to his account, and he receives a receipt for the transaction. John likes to keep the amounts he deposits between \$8,000 and \$9,000 because once, when trying to move more than \$10,000, he was told that forms had to be filed with the government detailing the nature of the transaction. The teller indicated that under the Bank Secrecy Act (BSA) of 1970, all regulated filing institutions are required to submit a Currency Transaction Report (CTR) for any deposits or withdrawals accumulated throughout a business day that exceed \$10,000. So, for good measure, John structures his transactions to be less than \$10,000 to avoid the mandatory CTR filing requirements.

Unknown to John, the bank has previously checked his references and can't confirm any of his business operations. They have also checked his credit report and residence history and know that he does not have any viable means of employment supporting the volume of cash he deposits. In fact, this transaction, as all of the previous transactions conducted by John at this bank, is being recorded on a special form created in 1996, called a Suspicious Activity Report (SAR).

### ***Suspicious Activity***

By law, the bank is prohibited from disclosing that they are submitting a SAR on John, so he thinks everything is fine and his transactions are going "undetected" by the government. All of transaction details are recorded including his name, address, social security number, date, dollar amount, and a descriptive narrative written by the bank's money laundering compliance officer. Since this is not the first time the bank has filed a SAR on John, the compliance officer includes a reference to the past reports they have filed.

The bank reports this transaction as a BSA Structuring / Money Laundering violation. It is a violation of Title 31 - Money and Finance ? Structuring Transactions to Evade Reporting Requirement Prohibited, to be involved in the following:

*Any person who, for the purpose of evading the CTR reporting requirements,*

- (1) *cause or attempt to cause a domestic financial institution to fail to file a report;*
- (2) *cause or attempt to cause a domestic financial institution to file a report that contains a material omission or misstatement of fact; or*
- (3) *structure or assist in structuring, or attempt to structure or assist in structuring, any transaction with one or more domestic financial institutions.*

This statute strengthens the ability of law enforcement to detect and prosecute crimes involving the laundering of money. In this case, since John is purposefully structuring his deposits under \$10,000 so CTR forms are not filled out, he is violating this federal statute. Furthermore, because he is knowingly transacting with money derived from illegal means (drug dealing), the violation becomes 18 USC 1956, Money Laundering. Under this statute, law enforcement can pursue a criminal investigation and ultimately seize his assets.

The SAR form submitted by the bank is sent electronically to the Detroit Computing Center (DCC), the U.S. Government's clearinghouse for all BSA data. At the DCC, the SAR is loaded into the Currency and Banking Retrieval System (CBRS), a large-scale mainframe database, where it resides with millions of other BSA records.

CBRS contains all SAR and CTR forms in addition to filings by casinos (SAR-C, CTR-C), retail organizations such as car dealerships, jewelry stores, and real estate brokers (8300), declarations to Customs at U.S. borders (CMIR), and reports of Foreign Bank and Financial Accounts (FBARs). More recently, CBRS has housed the SAR-SF data submitted by the financial services industry including brokerage houses, trading companies, and stock brokers as well as the SAR-MSB collection for all of the money service business reports detailing suspicious activity at the MSBs.

John's SAR is uploaded, processed, and posted in CBRS within ten days of receipt from the bank where it is accessed by federal, state, and local law enforcement agencies involved in assisting with anti-money laundering and financial crime investigations.

## Link Analysis

The most recent SAR on John is picked up by an analyst looking for suspects with SAR filings near the CTR threshold (\$10,000). John was one of several hundred potential targets meeting the query requirement. The analyst presents the initial findings in a link-chart diagram as shown in Figure 1.

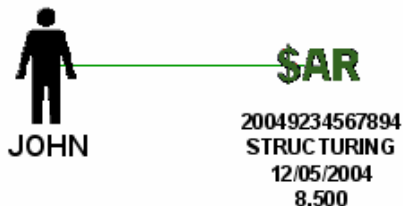


Figure 1

The label on the SAR icon shows the DCN (a unique document control number), violation type, transaction date, and the amount of money involved.

Next, the analyst pulls all of John's records and shows that he has a total of 11 SARs spanning a 12 month period, as is shown in Figure 2.

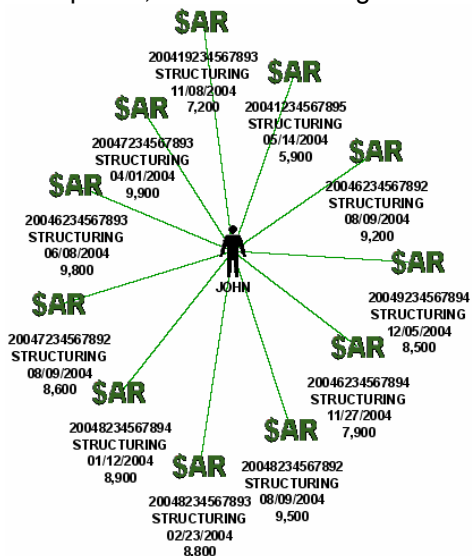


Figure 2.

The analyst does a quick re-cluster on this data to expose the number of different accounts. Often a person who is trying to avoid raising suspicion at a bank will distribute their activities across several different accounts. As can be seen in Figure 3, it appears that John generally makes regular use of 3 accounts.

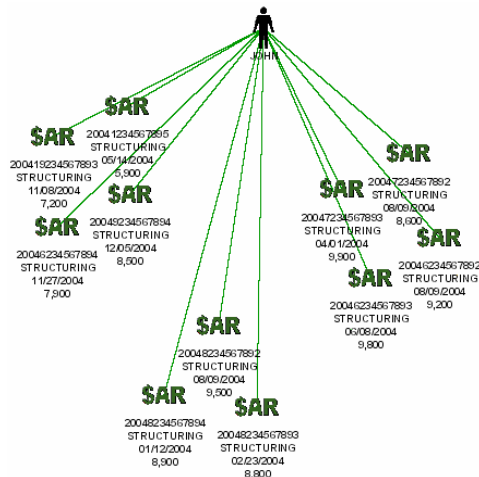


Figure 3

At this point, the analyst decides to merge each cluster to better manage the data and help clean up the display. Part of this process is to provide a unique descriptor for each merged object and in this case, the number of transactions, the account number, and the total transaction amount are listed in the label, as shown in Figure 4.

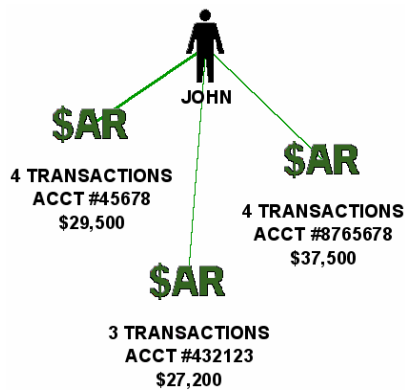


Figure 4

In the next step, the analyst expands the network to see any other relevant data listed on the SARs. The most important data that can be displayed includes: other subjects, businesses, addresses, ID numbers, social security numbers (SSNs), phones, and accounts. As shown in Figure 5, John has an address, a single SSNs, a driver's license, and two phone numbers (which are very similar).

The thicknesses of the links in this analytical system depict the frequency of the same data being reported on different SARs; the thicker the link, the more times that data element appears

in the data. The analyst checks a few external sources (e.g., Google) for more detail on the phone number and finds out it represents John's home phone. John was very diligent about ensuring he could be contacted by the bank should something happen to his money.

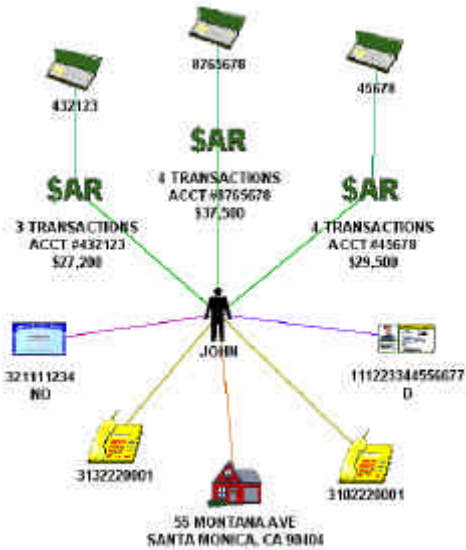


Figure 5

The analyst wants to see if there is any more data connected to any of these objects. The analytical system reveals the results shown in Figure 6.

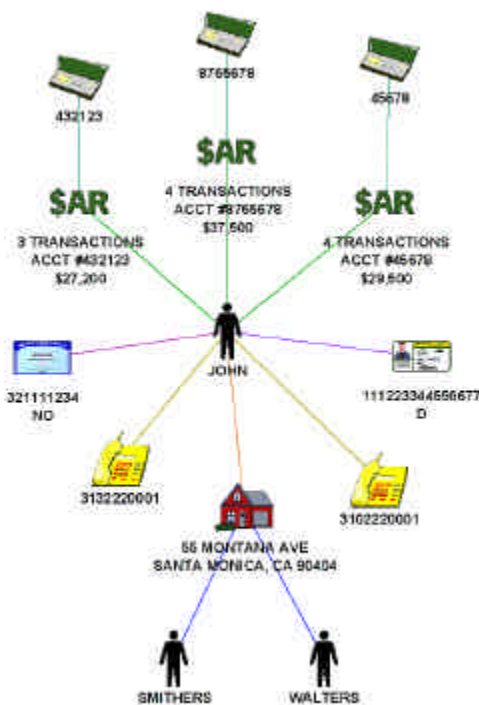


Figure 6

The address shows a relationship to two other subjects. Once again, the analyst expands the network to show 5 additional SAR reports as depicted in Figure 7. The analyst makes notes that several of these SARs list both subjects.

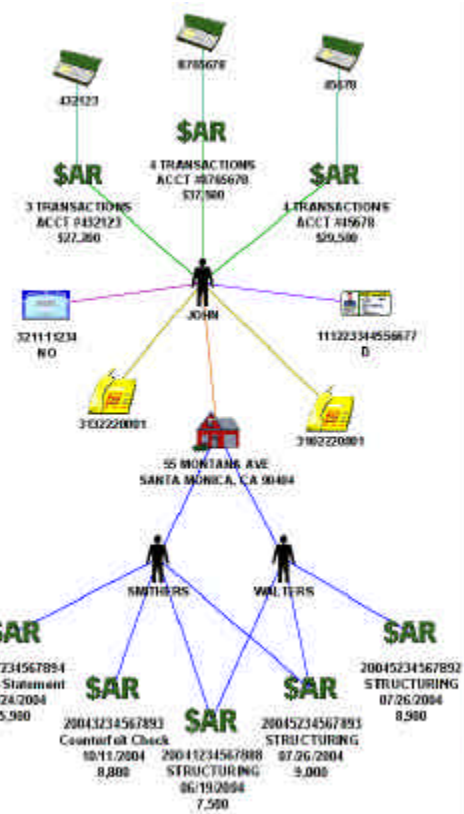


Figure 7

The analyst reads the narrative description for each of these SARs to see why the banks thought the transactions were suspicious. They all indicate that the subjects are believed to be involved in some type of illegal drug activity. From here the analyst expands the SARs an additional level, as shown in Figure 8, to show all the other subjects involved in the transaction. Immediately, the analyst recognizes ADAMS (highlighted in the red-circle) as a person who has been in the news for a recent drug bust.

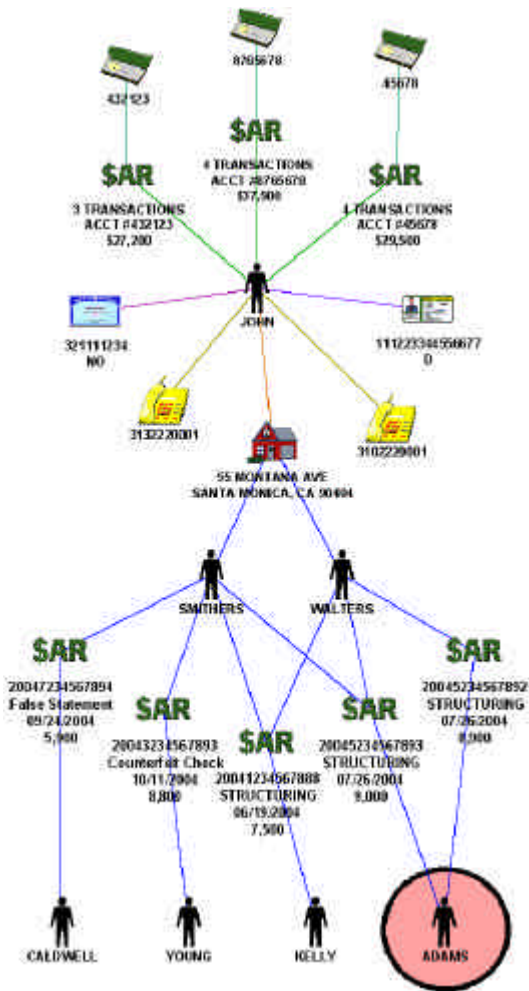


Figure 8

At this stage, the analyst contacts a Special Agent in the Criminal Investigations division of his organization and schedules a briefing. He brings to the briefing link charts, spreadsheets, maps and timelines so they can both clearly understand what the analyst has found. Based on solid reasoning and defensible assumptions, the investigator agrees that this target is worth pursuing.

### Conclusion

The anatomy of a financial crime can be quite diverse, complex, and detailed. There is no single method or query that reveals all types of money laundering behavior. Rather, the patterns are exposed through a number of indicators contained in the data.

People launder money because they are involved in criminal enterprises such as gambling, narcotics, embezzlement, fraud, or

even terrorism. Many want to avoid any type of government oversight or detection and, therefore, structure their transactions to minimize the paper trail. Regardless, if someone is involved in a specified unlawful activity and causes or attempts to cause a financial institution to fail to file a report, they are in violation of federal statutes and will be prosecuted accordingly.

There are always exceptions to the rules. Dirty data can lead to unexpected results, short circuits, invalid links, or dead ends. Of course, there are also exceptions to the exceptions. Many times when people intentionally misrepresent their identities to avoid detection – by varying the spelling of their names or transposing numbers in their IDs or addresses – they actually are establishing a different pattern than those where honest mistakes are made.

New ways of laundering money are conceived each day as are the proactive discovery of these patterns by the intelligence and law enforcement communities.

### Acknowledgement

The author would like to thank Kevin S. Hohn, Special Agent, Internal Revenue Service (IRS), Criminal Investigations Division (CID) and Andrew Shankman, Senior Analyst, Financial Crimes Enforcement Network (FinCEN) for their input and feedback on financial crimes and money laundering activities.