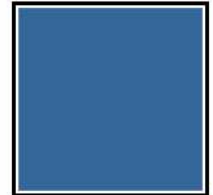
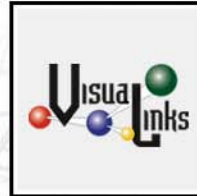


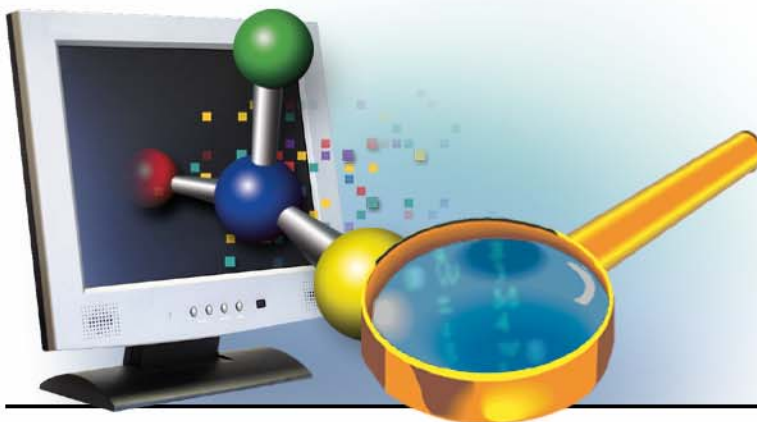


VISUAL ANALYTICS INC.



# To Catch a Thief

White Paper



## ABSTRACT

To catch a thief, spy, money launderer, insider trader, tax evader, narcotics trafficker or anyone exhibiting patterns of "non-compliant" behavior can be effectively performed using a combination of strategic (proactive) and tactical (reactive) analytical techniques. The exact definition of a non-compliant pattern will vary according to the activities occurring within the domain for which it is being applied. In many instances, the methods used to identify a pattern will change depending on the situation-the challenge to the investigator is to discover what associations in the data constitute a reliable and valid pattern. This paper overviews several methodologies used to identify patterns of non-compliant behavior across multiple and disparate data sets (e.g., financial crimes). Real world examples utilizing an operational visual data mining application targeted at money laundering operations are presented to show exactly what conditions were used to identify different types of behaviors based on a set of transactional events (e.g., the activities).

## Introduction

In relational data-management systems, or any electronic media for that matter, data is usually taken at a face value, that is, without trying to understand much about how and what is being represented. We typically gather information and store it into buckets (e.g., database tables and fields) so we can recall it at some future point in hopes that it may be useful or provide value to an ongoing case or investigation. In the law enforcement community, there are enormous volumes of information that are being collected and stored in this fashion without regard to how it will ever be used. Thus, there are huge repositories of information that exist and most likely may never be effectively utilized. This is due in part because there are no established means (technologies or methodologies) by which to easily understand what is contained in them. Thankfully initiatives supported through government sponsorships and commercial initiatives have provided new approaches to help law enforcement organizations better understand, manage, and present their data. Furthermore, these advances are applicable across a wide range of functional areas.

## Understanding Data

The goal of many law enforcement investigations is to find associations or establish relationships among the targets or suspect entities. Associations can be made not only based on the name of a person or organization but also through addresses, identification numbers (including licenses, passport, or social security numbers), telephones, vehicles, accounts, and most importantly activities. Activities represent the phone calls, border crossings, cash deposits, and meeting contacts associated with the illicit conduct being analyzed. A single occurrence of any activity, in and of itself, is not ordinarily considered of interest. However, when taken as a collective whole, a much different set of patterns emerges.

The behavior associated with activities (also called events) can be exposed using several different approaches. The goal is to take advantage of the similarities to understand the underlying behaviors associated with the activities being reviewed. Depending on the nature of the application, the behaviors will indicate different types of patterns that, once known, can then be identified and exploited according to the specific needs of the investigative agency. An analysis of activities can expose general trends or very specific patterns. Whether you are looking for temporal sequences or spatial dependencies, all information is contained within the activities themselves.

## Descriptive Data Models

Virtually all data modeled in an analysis may be characterized as either: descriptive or transactional. Descriptive data describe objects such as people, places, or things via attributable values (e.g., the location of a burglary, the subscriber of a phone, the color of a vehicle, etc.). The attributes of any descriptive object are unique to the object and are also considered a one-to-one

mapping - an attribute should only support a single value.

Descriptive data typically represent "state-based" knowledge that is considered true or believed until replaced by a different value. Once replaced, the old value is usually not maintained nor is it used within any subsequent analyses. See Figure 1 for a sample of descriptive data elements.

Figure 1. Descriptive Data Examples



Descriptive data tend to represent information such as organizational structures, credit report headers, driver's licenses, last known addresses, parole terms, account ownership, and so on. When various classes of declarative information are used in a model, one can show that relationships exist among them. The models are the explicit translations or mappings of the raw data into a primary object representation (e.g., what are objects, what are attributes, and what are defined to be the relationships).

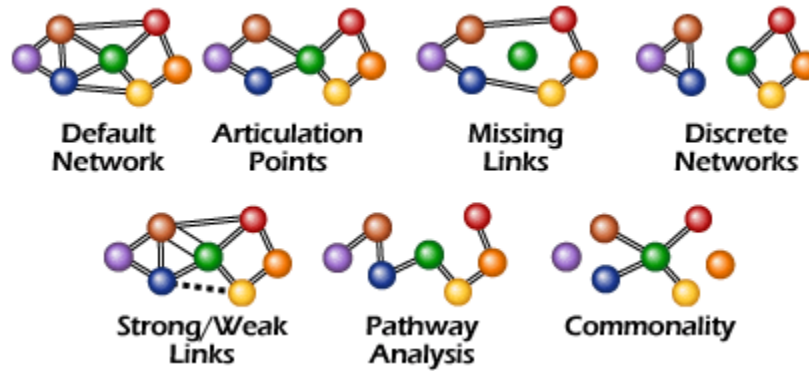
For example, you might have a model in which there is a class of objects corresponding to people and another class corresponding to vehicles with relationships between them indicating who owns which vehicles. Descriptive models tend to outline the overall structure of the relationships between the different objects contained within a data set. Descriptive data are useful for looking at networks and frequencies of connections, but are very difficult to use if the goal is to describe behaviors or events.

The networks that form from the definition of descriptive data can be used to expose a wide range of important data patterns. Since the goal of most law enforcement investigations is to establish relationships, descriptive data is a perfect representation format for supporting these tasks. The following depicts but a few of the structures that can be derived from the use of declarative data sources. Of course their exact meanings and usage will be dependent on the context in which they are used.

- **Articulation Points** - look for bottlenecks where one particular entity connects two or more sub-networks. These entities represent potential vulnerabilities and can be exploited, targeted, or used to the benefit(s) of the investigating organization.
- **Missing Links** - expose entities that are detached or unconnected from the main network structure. The investigator needs to determine why the entities are isolated and if there are missing data that would tie them in with the rest of the data.
- **Discrete Networks** - identify all the isolated sub-networks contained in the data. These groupings can be used to focus resources and help expose the extent of an investigation.
- **Strong/Weak Linkages** - see the strength of relationships within the network. Those entities with multiple (strong) relationships can be subject to transactional (behavioral) analyses.
- **Pathway Analysis** - determine if a series of linkages will connect a tuple of entities including the shortest path. Finding indirect relationships among suspects is vital in law enforcement applications.
- **Commonality** - look for entities connected to or that share common elements. These situations help identify additional targets as well as show the overlap of known resources.

Figure 2 shows a small network diagram for each one of these situations. Keep in mind that there are many different permutations and variations on the descriptive data pattern theme. The investigative domain largely defines the interpretation. For example, the patterns identified for telephone toll analysis will be different than those for identified for narcotics investigations.

Figure 2: Network Patterns



**Transactional Data Models**

Transactional data, in contrast to descriptive data, contain episodic information about time and place of events. Much of the information within database systems used by law enforcement represent transactions of some sort. The structure of transactions remains fairly static, that is, the content or values stored in transactional structures is what varies among instances. In general, transactional data contain a date/time component that can be used as a primary key to distinguish each discrete transaction (e.g., the transaction itself is what is unique).

To get a feel for transactional representations, consider the use of your telephone. No matter how many transactions (phone calls) are recorded for your telephone, the structure of the representation remains consistent. There is always a destination number, time, duration, and a date. What makes each telephone call unique are the values which are applied to each of these attributes for every transaction. Even when you call the same telephone time and time again, each transaction will be unique just from the fact that it occurs at a different time and date. Figure 3 shows some domains that are heavily based on the use of transactional data.

Figure 3: Examples of Transactional Data



Since every transaction can be distinguished from every other by its assigned values you can start to perform an analysis to look for explicit transactional patterns and related behaviors.

In a transactional model, you can typically use links between object classes to represent traits or conditions of the event contained within the transaction. Thus, all of the conditions associated with the event can be applied to the link since they were derived as a result of the event. What this means is that any attribute applied to any link generated between any pair of objects derived

using a transactional model can justifiably support any of the information used to describe the transaction.

Is it not true that the amount, time, or date of a financial transaction can be used as an attribute to describe the link created between the transactor and the account as well as the link between the address and the business? Also, the existence of many links between two objects indicates that many separate transactions occurred between them and each is represented in the data set.

In a descriptive model, on the other hand, each of the links can have its own unique value used to describe the relationship between object classes. Thus, an individual person in a "people" object class might be connected to an "address" in another class because the information was listed in a credit application. However, that same individual can have a link with a particular automobile in a "vehicles" object class for a completely different reason, defined by a completely different set of conditions. This flexibility occurs in a descriptive model because the information that is used to specify the conditions of the relationship is distinct to the objects of interest. In a transactional model, the conditions represented in any relationship are generated from the transaction record and so are more focused on the event itself.

Thus, we could immediately look at the results to determine whether there are any trends of interest with regard to these behavioral questions. You should note that although the transactional model is the most powerful alternative for examining behavior, it comes with a price. Transactional models often involve the proliferation of large numbers of objects and links that must be managed.

On the whole, there are not tremendous differences in the qualitative nature of individual transactions. For example, all phone calls share certain traits or attributes in common. What is important in the analytical environment is that this episodic information that can be used to distinguish one transaction from another. That is, you may not be so interested in what happened (since all events are fairly similar to one another) as you are in when, where and how often it happened. In contrast, semantic or descriptive representations may or may not contain the same attributes. Patterns of interest within descriptive knowledge structures often center on similarities and differences in these attributes.

When an investigation is initiated you will need to decide whether you are dealing with descriptive data, transactional data, or a combination of both. The type of data will determine the analytical models that can be used. If your data are descriptive your analyses will be confined to the use of descriptive models. Transactional data, on the other hand, may be represented in either descriptive or transactional models. The types of results that you will be able to glean from your analyses depend largely on the kind of model you select.

### **Show Me The Money!**

Financial crimes are a lucrative business for both criminals and the law enforcement organizations that pursue them. There has been a good deal of literature in recent times describing new and innovative ways of detecting money-laundering operations.

The regulations imposed on banks and other financial institutions were designed to generate a trail that could be used to track the path of money as it moves through the system. There are several different types of forms that must be filed when a cash transaction of currency for more than \$10,000 is conducted. Banking related industries are required to file an IRS Form 4789 - Currency Transaction Report (CTR).

Businesses such as car dealerships, jewelry stores, and any other retailer dealing with large dollar merchandise are required to file IRS Form 8300 - Report of Cash Payments over \$10,000 Received in a Trade or Business. Additionally, casinos need to file IRS Form 8362 - Currency

Transaction Report by Casinos, and any international travelers file Customs Form 4790 - Report of International Transportation of Currency or Monetary Instruments.

Finally, those people who maintain foreign bank accounts are required to file Treasury Form TD F 90-22.1 - Report of Foreign Bank and Financial Accounts (FBAR). There is even a special form called a Suspicious Activity Report (SAR) TD F 90-22.47 that is submitted by financial institutions for any suspicious financial transactions, including those under the \$10,000 trigger.

Figure 4. A CTR Form 4789

Figure 4 shows an example of a CTR form, of which there are well over 100 million stored in various database systems throughout our state and federal agencies

To effectively understand all of the behaviors associated with this type of data, its format must be understood. Naturally, the information contained on a CTR can be viewed using either a descriptive or transactional data model.

Using a descriptive model, there are all sorts of information that can be exposed. The primary data objects used in this model typically represent people, organizations, identification numbers, accounts, banks, and tellers. From here a variety of structural patterns can then be viewed to look for various financial crimes. Depending on the agency, the structures will expose different patterns.

Figure 5 shows a set of objects where a central entity has connection to two different entities. Their interpretation is based on the context in which they are being analyzed.

Figure 5. Descriptive CTR Models



For example, when one person is connected to two different social security numbers it may indicate a non-compliant tax situation to the IRS. Alternatively, two people connected to a single

id-number may show deceitful behavior where they are trying to avoid detection. Multiple addresses for any one person might lead investigators to suspect illicit activities are ongoing. The combinations are virtually endless.

When looking at the transactional CTR models, for brevity, let's assume that the only information to be modeled represents the subjects conducting the transactions (e.g., transactors) and the CTRs (e.g., the transactions) themselves. Remember that the attributable information that is contained on the transaction itself (e.g., the CTR) can be used to expose the underlying behavior associated with moving the money. The following represents only some of the detail required for filling out a CTR.

- Account Type
- Amount Cash In/Out
- Bank Location
- Bank Name
- Date of Transaction
- Occupation Type
- Teller/Official Name
- Transactor Address
- Transactor ID
- Transactor Name

The goal is to provide a well-integrated picture of all of the known cash transactions for a transactor when money is moved in or out of a financial institution. Once a pattern has been identified, law enforcement can take appropriate actions to prevent, circumvent, or interdict the targets based on their known behavior.

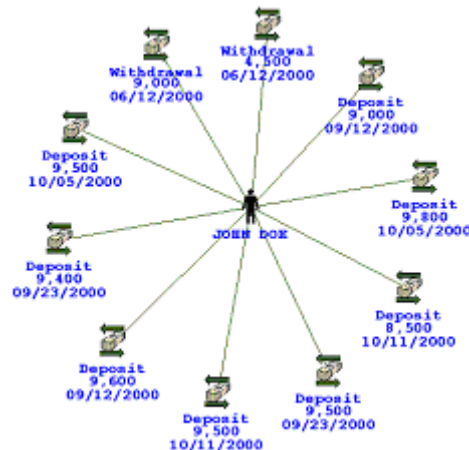
**Transactional Examples**

To make better sense out of what the transactional patterns would look like in a real world financial crime application, several hypothetical examples have been created to demonstrate the concepts. Typically no single display indicates there is something suspicious, the investigators must look at all the dimensions and come up with an overall evaluation of the situation.

The diagrams generated for these examples were created using the VisualLinks® data visualization software. However, it is the concepts and methods that are important to understand, and not the specific presentation technique.

Figure 6 shows a transactor who has been involved with a number of CTRs. The transactor appears at the center and is linked to each of the transactions that are shown in the display. The links are created to make the relationships explicit even though the value of the transactor is an attributable value in each of the CTR objects. The links make the display look more consistent and are useful when more than one transactor is being investigated.

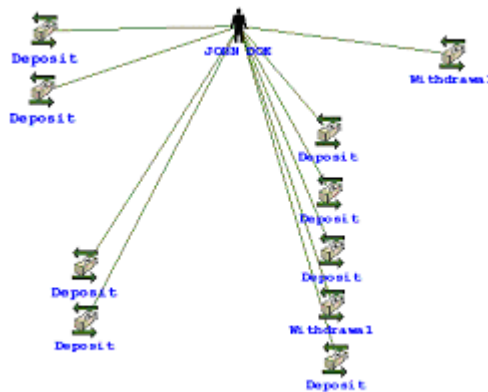
Figure 6. No Prior Audits/Reviews



For these purposes, a highlight-color for any CTR object can be defined to reflect certain values. In this case it was set to show if this transactor has ever been previously reviewed by any other law enforcement agency. As it turns out, there are no prior reviews which potentially means he maintains a well-established pattern (e.g., relationship) with the banks. Of course this also means he may be very good at avoiding these situations or perhaps the bank has already been subject to infiltration or corruption.

Figure 7 shows another example of the same transactor where the CTRs have been clustered (e.g., grouped) according to the particular branch where the transaction took place. As can be seen, there are now four discrete clusters for the CTRs. The majority of transactions have taken place at one particular branch as is seen by the larger cluster. However, the presence of the other three clusters may indicate there is potentially an ongoing "structuring" pattern.

Figure 7. Multiple Branch Activity



It is illegal to "structure" a series of transactions to avoid the \$10,000 threshold. For example, you cannot knowingly manipulate a financial institution into failing to file a CTR report by making three deposits of \$9000 instead of one \$27,000 deposit. Using multiple branches to move large cash deposits is not consistent with legitimate behavior.

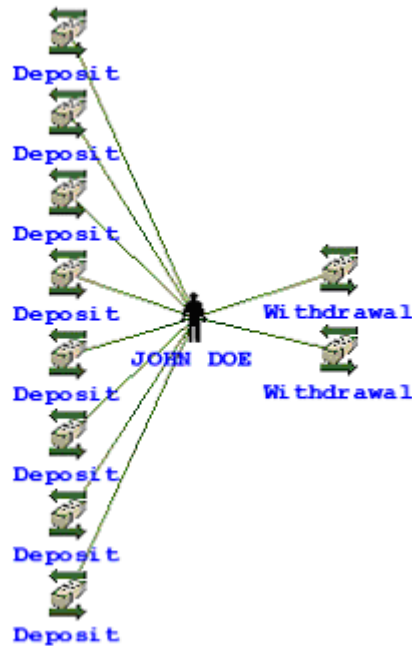


Figure 8. Bias for a Teller

Figure 8 represents a situation where the CTRs have been clustered based on the teller who has performed the transaction on behalf of the filing institution (e.g., the bank). In this example there is an overwhelming bias for a specific teller.

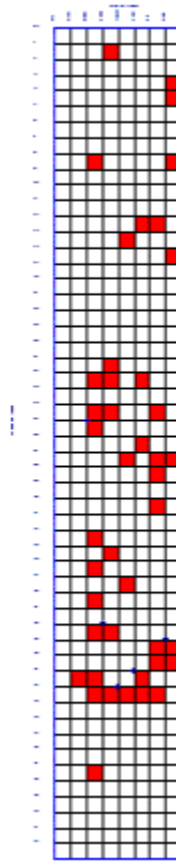
A possible explanation for this situation might include that the bank has one designated official who authorizes these types of transactions and therefore, by default, his or her name or identification number is listed on all the CTR forms. Much more likely is that there is collusion with one of the tellers. This is also reflected in the link colors (not shown in the B&W diagrams) where the teller is shown to have operated at more than one branch location when the transactor has made deposits. Notice that this teller performs all deposits and another teller performs all withdrawals.

This type of diagram can be used across a wide range of the attributable values present on the CTR form. Figure 9 depicts a slightly different display configuration where the CTRs are laid out according to the date when they occurred. This format is considered to be an "absolute" placement.

The placement of CTRs according to their dates can be extremely powerful, especially when dealing with larger quantities of information. Patterns are more readily detected using this type of display since there are so many dimensions being displayed at one time.

Within this display the CTRs are presented using a 7x52 placement algorithm. Dates associated with a CTR can be used to determine the day-of-week (1-7) as well as the week-of-year (1-52). The resulting matrix definitively presents the temporal filing patterns associated with the transactor. It is very clear due to the time-gaps that the transactor does not follow a regular pattern which implies there is no steady income nor is the exhibited pattern consistent for any known occupation codes (a required field on the form).

Figure 9. Irregular Filing Dates



There are all sorts of variations on this theme, especially when dealing with times and dates. Since transactional patterns are structurally consistent, the same type(s) of patterns can be derived from telephones, border crossings, travel events, email, web-site visits (cyber-crime), or just about anything else with a temporal value.

Ideally when dealing with financial crimes, the ultimate goal is to seize the assets associated with the money laundering operations. Thus, if a temporal pattern can be identified and confirmed, then the law enforcement agency has a better chance of actually obtaining a "cash" assets forfeiture because they can predict when the funds are going to be moved or when the accounts are full.

**Conclusions**

There are good people - and there are bad people. The bad people cost the good people a significant amount of monetary and resource losses (measured in billions of dollars) through the liabilities incurred from fraud, theft, espionage, embezzlement, public corruption, and proliferation. In many cases the malpractice and malfeasance succeed because people do not know how to interpret their data sets or recognize the telltale symptoms. The majority of wrongdoing is carried out in a large number of relatively small exchanges. A large percentage of crimes such as money laundering are perpetrated through a series of frequent transactions with relatively small amounts of money being processed on any one occasion. This sort of activity is of course subtle and not directly detectable through usual methods of oversight. To catch a thief, or any wrongdoer for that matter, one must lock onto a behavior pattern. Data mining and visualization approaches can be applied to these sorts of problems with great success at relatively low cost.