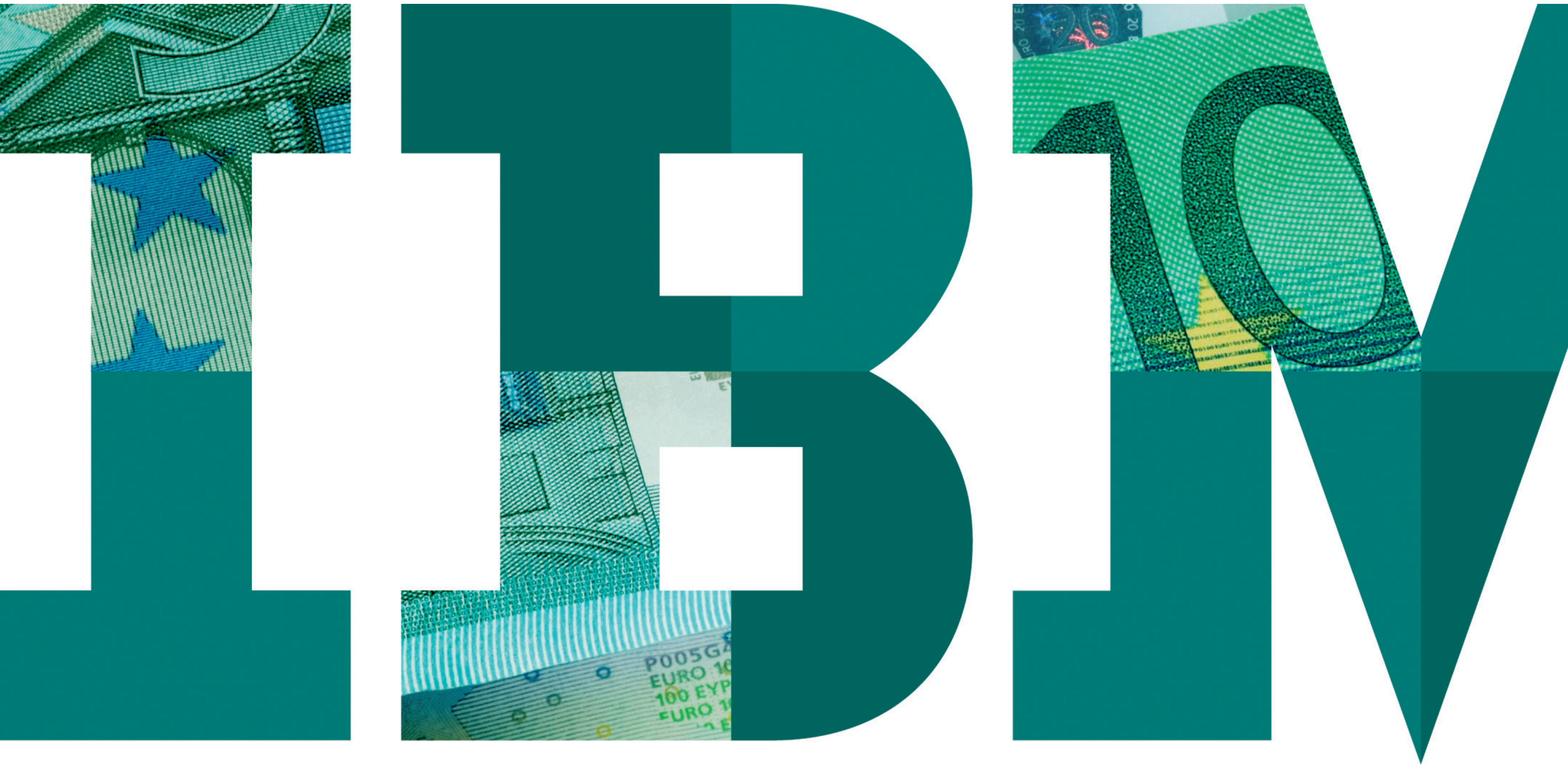
IBM Analytics
White Paper

Preventing fraud with identity and social network analysis

A guide for bank executives



Banks face a rising tide of fraud—and stringent regulations

When someone applies for a loan at your bank, you need accurate answers: Who is this person? What is their background? Is the information that they're giving us 100 percent truthful?

Answering these questions quickly and completely isn't just a good idea—it's the law. Financial institutions are subject to an array of regulatory requirements to "know the customer":

- The USA PATRIOT Act aims to detect and prosecute international money laundering and the financing of terrorism. The Act requires banks to implement customer identity verification procedures, anti–money laundering (AML) programs and other due diligence measures. Customer identification programs must describe how the bank will verify the identity of new account holders. Banks must also hold identity data for five years after an account is closed. Additionally, banks must implement procedures for determining whether the customer appears on any list of known or suspected terrorists. When they suspect or discover violations, they must file a suspicious activity report.
- The European Union (EU) implemented money-laundering directives in accordance with the EU Financial Action Task Force (FATF) recommendations. The FATF proposed 40 recommendations for countermeasures against money laundering that cover the criminal justice system and law enforcement, the financial system and its regulation, and international cooperation. In addition, it made nine special recommendations that set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts.
- Hong Kong is particularly susceptible to money laundering because of its low taxes, complex banking system and minimal currency and exchange controls. Under current legislation, financial institutions are required to know and record the identities of their customers and maintain records for five to seven years. Furthermore, remittance agents and money changers must register their businesses with the police and maintain customer identification and transaction records for cash transactions equal to or greater than HKD20,000 (approximately USD2,564).

The bottom line is that if you don't know your customer, you are vulnerable.

Meeting regulatory requirements starts with knowing exactly who you're doing business with—not always an easy task. Financial fraud, money laundering and other illicit activities are often performed by individuals acting in collusion with each other. These individuals may be related as business partners, customers or even as your employees. And while their isolated banking transactions may look insignificant, together they may illustrate patterns of suspicious activity that warrant investigation. In short, to prevent fraud, you need to know not only who is who, but also who knows who, and who does what.

This paper discusses the ways that identity and social network analysis can help you prevent fraud and enable compliance by focusing not only on transactions, but also on persons and groups and how they are interrelated. The paper also examines the requirements for a proactive fraud detection system, and describes how ongoing data analysis can alert you to the need for action.

What is identity and social network analysis, and what does it mean to your bank?

Identity and social network analysis is a technique for uncovering and analyzing relationships. It takes the form of software designed to look at entities—defined as unique persons or institutions—and analyze their relationships to detect collusive activities. With identity and social network analysis, you can see relationships both within and outside of your bank, showing the extended social, business or relational network of an entity. The resulting view provides the insight you need to take swift preventative action. In a recent report, Forrester Research, Inc. highlighted the value of an entity-based approach, saying, “Since fraud is committed more and more by fraud rings that quickly attack your business from various channels (web, call center, branch, ATM, POS, etc.), you will have to protect your business from fraud by moving beyond transactions to entities, looking across multiple channels in near–real time.”[1]

The identity and social network analysis process includes a series of techniques performed in sequence:

1. Identity matching
2. Relationship network analysis
3. Transaction analysis

Let’s look at how each step builds progressively to uncover fraud.

Identity matching detects aliases

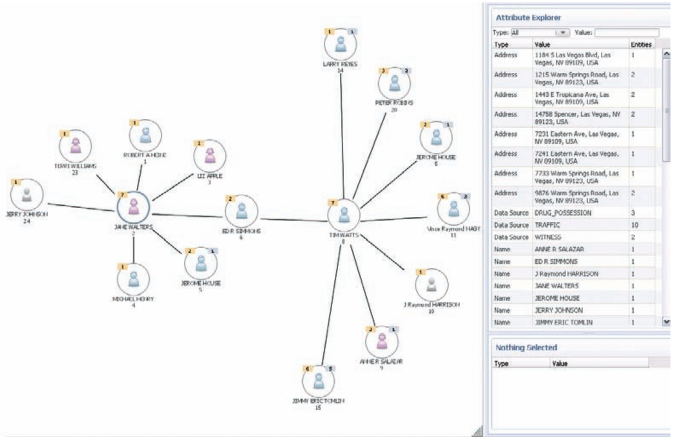
Identity matching—also called identity resolution—shows who is who. Fraudsters will try to hide their identities by using an alias, by using different cultural variations of their name, or by using a manufactured or stolen identity. They may cite the same address with different spellings, or give different phone numbers. If one individual can convince you that he or she is actually two different people, then that person has taken the first step necessary to carry out fraud.

Identity matching uncovers multiple aliases and collapses them to a single entity. By determining when seemingly unique entities are actually the same person, group or company, you can begin to build a network map.

Relationship network analysis detects collusion

After aliases and other duplicate identities have been accounted for, relationship network analysis looks for connections between persons, groups or organizations (see Figure 1). Some of these connections will be known or declared relationships, such as two people sharing a joint account.

By comparison, undeclared or nonobvious relationships are more likely to indicate fraud. A bank might suspect fraud, for example, when a customer is found to have a relationship with an organization on a watchlist for financial crimes. Collusion might also be suspected if a loan applicant shares an address with an employee in the loan processing department. Once the relationships are identified, the bank can determine the need for further investigation.



Attribute Explorer

Type: All Value:

Type	Value	Entities
Address	1184 S Las Vegas Blvd, Las Vegas, NV 89109, USA	1
Address	1215 Warm Springs Road, Las Vegas, NV 89123, USA	2
Address	1443 E Tropicana Ave, Las Vegas, NV 89109, USA	2
Address	14758 Spencer, Las Vegas, NV 89123, USA	2
Address	7231 Eastern Ave, Las Vegas, NV 89109, USA	1
Address	7241 Eastern Ave, Las Vegas, NV 89109, USA	1
Address	7733 Warm Springs Road, Las Vegas, NV 89123, USA	1
Address	9876 Warm Springs Road, Las Vegas, NV 89123, USA	2
Data Source	DRUG_POSSESSION	3
Data Source	TRAFFIC	10
Data Source	WITNESS	2
Name	ANNE R SALAZAR	1
Name	ED R SIMMONS	1
Name	J Raymond HARRISON	1
Name	JANE WALTERS	1
Name	JEROME HOUSE	1
Name	JERRY JOHNSON	1
Name	JIMMY ERIC TOMLIN	1

Nothing Selected

Type	Value

Figure 1. Relationship network mapping charts declared and undeclared relationships.

Transaction analysis looks at activities

The final step in identity and social network analysis maps a person or group to the activities they conduct. At this point in the analysis, you already know whether seemingly distinct entities are really the same, and you know how those entities are related. Now you're ready to shed new light on their interactions with your institution.

For example, suppose that five individuals each transfer USD9,000 to an offshore bank account within a 24-hour period. In isolation, each transaction looks perfectly ordinary. But if you know that the five individuals are actually all the same person, you may have detected a money-laundering operation.

Five requirements for successful identity and social network analysis

For identity and social network analysis to provide real value to your bank, the underlying software engine must be properly designed. While the algorithms involved can be complex, there are several essential characteristics of well-designed identity and social network analysis, which can be defined as the five rules for success. Let's take a closer look at these rules:

1. Assume no clue is too small

Identity and social network analysis starts from the assumption that fraudsters are actively trying to hide, and that any data that doesn't match up potentially indicates an active threat. That means all clues are important, no matter how small. For example, if the system looks only for exact matches in data, it may miss intentional misspellings designed to throw investigators off track. Likewise, if the system looks for name variations in only one culture, it may miss cross-cultural matches that could indicate international fraud. Many clues may seem insignificant at first but yield great meaning when viewed together in a larger context.

2. Operate in real time

To prevent fraud before it happens, your identity and social network analysis must operate in real time or near–real time. You can't wait for a new load of data to process overnight—by then it might be too late, and undoing the effects of fraud after the fact can be far more expensive than prevention.

3. Move beyond transactions to people and groups

Some fraud detection systems look only at transactions. That's a mistake. Stopping fraud before it happens requires that you focus on the individual attempting fraudulent activity. For example, opening an account is a routine activity that would not ordinarily raise suspicion. But if you know that someone has opened up several accounts and is transferring money between them, you might want to take a closer look—especially if you also know the accounts are owned by the same person using seemingly different identities. If that individual is related to another person engaged in the same pattern of banking activity, you may have discovered a fraud ring.

4. Look for links across banking channels

Fraud rings often attack an institution in several ways at once. For example, one member of the ring may specialize in account opening, another in check fraud and another in money laundering. Detecting these groups requires software designed to look for connections across channels of banking activity.

5. Adapt to changes in fraud tactics

As fraudsters adopt new tactics—changing the recipient and frequency of money transfers, for example—identity and social network analysis software must have the built-in capability to evolve. The ideal system also allows quick customization to incorporate software changes.

Solution profile: IBM InfoSphere Identity Insight

The IBM® InfoSphere® Identity Insight solution uses identity and social network analysis to provide true insight for threat and fraud analysis. It is designed to give you the context necessary to catch fraud rings before they catch you, by answering key fraud detection questions and embodying the essential rules of successful identity and social network analysis.

Answering the three key fraud detection questions

For data to be useful, it must be put into context. InfoSphere Identity Insight is a powerful identity and social network analysis platform that combines pioneering identity and relationship disambiguation technology with innovative event-processing capabilities to quickly and automatically provide that context. By examining relevant individuals, their relationships and their actions, InfoSphere Identity Insight enables your bank to have a complete picture of who a person is, who they know and what they do (see Figure 2).

Who is who—The first step is identity matching. Once InfoSphere Identity Insight determines that two or more identities are the same, it integrates the multiple records into a single entity and assigns a unique identifier. All of the data about the person or organization stays with this new identifier. The platform can even tell you which source records provided the original information.

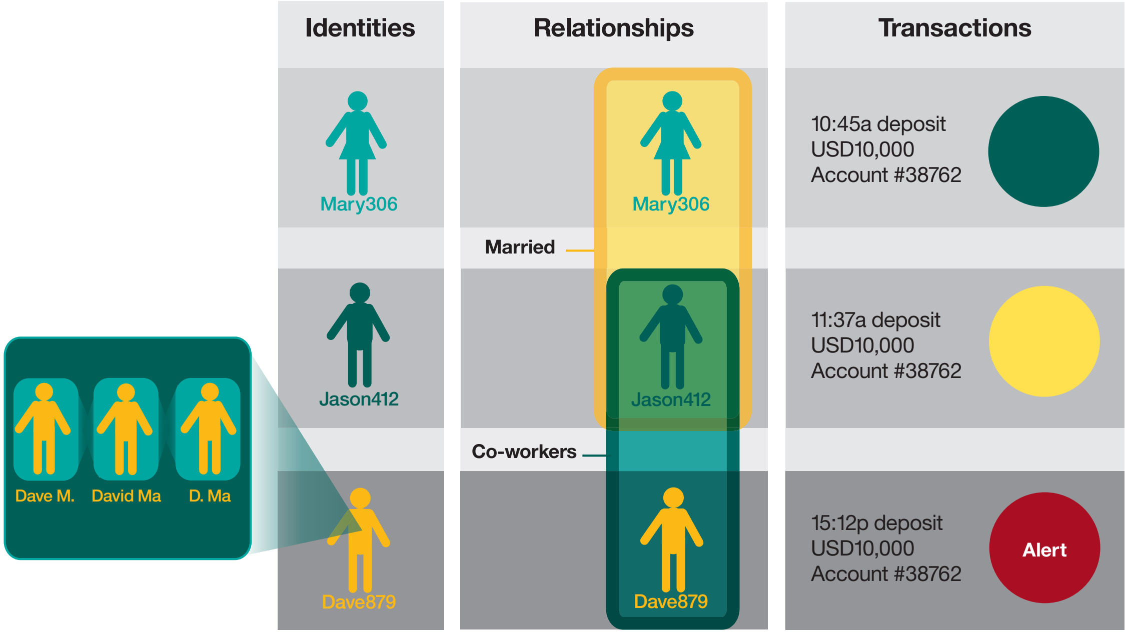


Figure 2. InfoSphere Identity Insight establishes unique identities, uncovers relationships and tracks transactions in context to help detect potentially fraudulent activity.

Who knows who—Next, the InfoSphere Identity Insight platform performs a thorough relationship network analysis. It uses the entity data generated during the previous step to learn whether people are, or ever have been, related in any way.

Who does what—InfoSphere Identity Insight uses an advanced transaction analysis method called complex event processing to gain a clear picture of how an entity is interacting with your bank. The process is designed to mine the overall information landscape, bringing to light all of the associations and occurrences involving the same person or group. If fraud is detected, the system proactively generates alerts.

Relationship network analysis might reveal that someone on a fraud watchlist shares an address with some of your customers and a phone number with others, indicating the potential existence of a sophisticated fraud ring.

Delivering on the five rules of fraud detection success

InfoSphere Identity Insight uses patented entity-resolution technology and innovative event-processing methods to set the bar for intelligent, automated fraud detection. With each new activity, the platform builds context based on what it already knows—for example, remembering how people and organizations relate. Intelligent algorithms mitigate false positives, making the platform highly efficient for banking staff. Built-in security enables data to be securely shared within and among departments.

Assume no clue is too small—Are multiple records really describing different individuals, or are they actually records for a single identity? The InfoSphere Identity Insight platform uses even small clues to uncover the truth. For example, IBM InfoSphere Global Name Recognition searches for names based on linguistic, phonetic and specific cultural variation patterns. This technology, built from analysis of over 800 million names, gives InfoSphere Identity Insight more power to discover matches. Also, Identity Insight uses a technique called full attribution to maintain a complete profile of an entity that includes not only current information, but also related details such as an email address used on a prior alias, a past phone number, or alternate names and birth dates. These pieces of information often become the clues that link two seemingly independent entities together.

Operating in real time—InfoSphere Identity Insight operates constantly and dynamically in the background, taking in new information and performing *perpetual analytics*. Whenever new data appears, the system immediately evaluates it, recategorizing the affected entities and then determining the impact on any potentially related entities. For example, a new piece of information may reveal that a single entity named Robert Smith is actually two entities: father and son. InfoSphere Identity Insight will instantly recalculate all relationships and entities tied to Robert Smith Jr. and Robert Smith Sr., giving you a more accurate picture of who you're dealing with.

Moving beyond transactions—Is a fraud ring trying to hide transactions greater than USD10,000 by spreading the transfers across multiple accounts with different names? InfoSphere Identity Insight is designed to find out by going beyond identity and relationship disambiguation to match events to identities using advanced algorithms to untangle complex events.

Looking for links across channels—Multiple contacts from a fraud ring can appear quickly in different departments or geographical locations of your bank. The InfoSphere Identity Insight platform is built to detect fraud across channels, whether through different lines of banking, different branches or different forms of electronic communication. It supports a variety of integration methods that allow data from disparate source systems to be centrally analyzed while maintaining links to the source data.

Adapting to change—InfoSphere Identity Insight is rules-driven, and can thus be easily adapted to meet changing criminal tactics. For example, match rules can be exact or approximate and used in nearly limitless combinations. You may start by configuring InfoSphere Identity Insight to consider a birth date match as more important than a name match. Later, you can alter the hierarchy as you discover that other data—such as addresses or passport numbers—is more reliable. Or, you may begin by flagging online accounts opened within a 24-hour window by related entities—and then expand or contract that time period as criminals change their methods.

Case in point: How financial institutions are using InfoSphere Identity Insight

International payment provider

An international payment provider built an integrated fraud and compliance environment with InfoSphere Identity Insight as the analytics engine. As a result, the company can analyze relationships in context rather than simply analyzing each transaction in isolation. The IBM system first confirms the identity of each individual entered into the system, resolving the data against internal and World-Check watchlists. Then the system validates whether the transaction made by the individual passes business and regulatory rules, taking into account all other transactions involving that individual. With InfoSphere Identity Insight at the core, the company can focus both business and IT operations around a single, robust fraud detection solution.

U.S. regional bank

A large regional bank made InfoSphere Identity Insight a cornerstone of its anti-money-laundering and “know your customer” solution. The IBM system analyzes all customer data to check each individual across channels and identify relationships of interest. During this analysis, the system validates names against internal and external watchlists. Any alerts are sent to the bank’s case management system, and identities and relationships are made available to the bank’s data warehouse to support business intelligence reporting—providing an added benefit to the bank.

Global money transfer organization

A global money transfer organization integrated InfoSphere Identity Insight into its existing analytical platform. While satisfied with the organization’s business rules engine, managers realized they lacked a comprehensive view of the customers. With the IBM technology’s ability to uniquely resolve identities, the organization is better able to know its customers, becoming more alert to problems while fostering relationships of value. The IBM system is set up to operate in near–real time within transaction streams. This enables the system to verify the customer identity for each transaction as it comes in, providing the basis for all further analysis.

Help stop fraud before it happens with InfoSphere Identity Insight

The days when bankers knew all of their customers personally are long past. Today’s banks may have thousands of clients scattered across the globe. Have your fraud detection systems kept pace with the changes? With InfoSphere Identity Insight and identity and social network analysis techniques, you can examine individuals and groups, their activities and their relationships, to identify potential fraud before it affects your bottom line.

Fraud strategies—and the criminals who perpetuate them—are more insidious than ever before. Make sure that you’re asking the right questions and getting the right answers about your level of risk. After all, it’s much better to read headlines about fraud cases than to be part of them.

For more information

To learn more about using IBM InfoSphere Identity Insight to help your organization combat fraud, contact your IBM representative or visit: **ibm.com**/software/data/identityinsight-solutions

Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2017

This document is current as of the initial date of publication and may be changed by IBM at any time.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates. Offerings are subject to change, extension or withdrawal without notice. All statements regarding IBM future direction or intent are subject to change or withdrawal without notice and represent goals and objectives only.

[1] Forrester Research, Inc. "Market Overview: Fraud Management Solutions." August 25, 2010.

Please Recycle