

# Hidden Relationships and Networks: Financial Institutions at Risk

*An Oracle White Paper*  
*October 2009*



# Hidden Relationships and Networks: Financial Institutions at Risk

Regulations in Europe and the United States, while not specifying the hunt for hidden relationships, urge financial institutions to be on the watch for “patterns” of activity between seemingly unrelated accounts.

## EXECUTIVE OVERVIEW

This white paper describes

- The regulatory landscape and guidance on hidden relationships
- Hidden relationships and networks -- how to identify them?
- Why financial institutions need to address the problem today?
- The roles of personnel and technology in the effort to combat money launderers
- Unique technological innovations in the fight against hidden networks

## INTRODUCTION

Protecting a financial institution, its employees, customers, and assets would have been much easier if criminals were identifiable by behavior and activities. However, financial criminals and money launderers do not behave in established, predictable patterns. They use every method possible to evade detection, and where no methods exist, they create new ones.

Nowhere is this more true than in the world of money laundering, where highly trained, well-equipped teams manage the funds for organized crime, drug cartels, and terrorist groups. In an attempt to evade detection, money launderers often layer funds through a series of financial transactions or physical movements that conceal the origin of the illicit funds. The objective of performing a complex system of transactions is to make it difficult for investigators to trace the origin of the assets involved. Known as “hidden relationships” or “networks,” money launderers often establish rings of accounts that appear to be unrelated and then move assets between several of these accounts.

## REGULATORY LANDSCAPE

Regulations in Europe and the United States, while not specifying the hunt for hidden relationships, urge financial institutions to be on the watch for “patterns” of activity between seemingly unrelated accounts. In recommendation 11 of its “Forty Recommendations,” the Financial Action Task Force on Money Laundering (FATF) states:

Financial institutions should pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings published, and made available to help competent authorities and auditors.

**“Firms with more successful programs had well-trained firm personnel that were educated on what to look for when screening money movements, such as: rapid journaling of assets between related accounts, transaction patterns where no securities investments were made before funds were wired out of the account, and several ostensibly unrelated entities sharing addresses.”**

**— Lori Richards,  
Director, U.S. Securities and Exchange  
Commission’s Office of Compliance  
Inspections and Examinations**

Hidden relationships and networks, by their very purpose, have no legitimate economic or lawful purpose. Regulations in the United States and their guidance offer similar guidance to financial institutions and instruct them to look for patterns. The summary statement from adoption of the rule states:

The language in the rule requiring the reporting of patterns of transactions...is intended to recognize the fact that a transaction may not always appear suspicious on a standalone basis. In some cases, a broker-dealer may only be able to determine that a suspicious transaction report must be filed after reviewing its records, either for the purposes of monitoring for suspicious transactions, auditing its compliance systems, or during review.

While the rule language is general, the regulators give guidance on implementation in speeches, lists of red flags, and other documents. In addition, they talk about best practices and systems that have features they believe are especially effective.

Lori Richards, Director of the U.S. Securities and Exchange Commission’s Office of Compliance Inspections and Examinations, had this to say about anti-money laundering in May 2002:

Screening wire transfers: We found that reviewing individual wire transfers—in and of themselves—in many cases did not constitute a meaningful exercise. Firms with more successful programs had well-trained firm personnel that were educated on what to look for when screening money movements, such as: rapid journaling of assets between related accounts, transaction patterns where no securities investments were made before funds were wired out of the account, and several ostensibly unrelated entities sharing addresses. One firm utilized a computer system that detected patterns in wire activity and flagged accounts with multiple transfers to an unrelated account and large wires in and out with little or no corresponding securities purchases or sales.

Lastly, in support of the FATF 40 and the need to adopt new methods to counter money laundering, the U.K. Financial Services Authority (FSA) stated in its January 2005 International Regulatory Outlook:

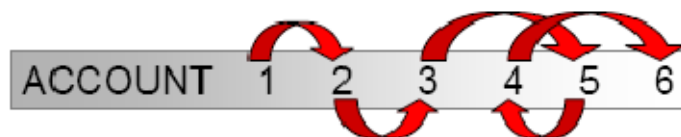
The guidance adopted by the FATF towards AML-CTF is consistent with firms adopting a risk-based approach. Such an approach is aimed at maximizing the effectiveness of risk monitoring and mitigation.

Rather than treating all transactions uniformly, it requires firms to be continuously vigilant as new criminal techniques and sources evolve and to focus on high-risk activities.

Clearly, regulators on a global scale are imploring, if not outrightly directing, financial institutions to take a closer look at relationships between accounts, and how those accounts form patterns, rings, and networks of accounts.

### **HIDDEN RELATIONSHIPS AND NETWORKS DEFINED**

What are hidden relationships? There are several types, each with characteristics that financial institutions need to consider in order to detect them. In its most simple example, consider six accounts within a financial institution. Account 1 shares a piece of information such as a phone number, address, or beneficiary in common with Account 2. Account 2 shares a different piece of data with Account 3, and so on.



**Figure 1: Example of hidden relationships**

It appears that Account 1 and Account 6 share absolutely nothing in common. However, they constitute a network through which a criminal can launder funds. Unfortunately, hidden relationships or networks are rarely that easy to define or identify.

### **PATTERNS OF FUNDS TRANSFERS BETWEEN CORRESPONDENT BANKS**

Correspondent banking is considered particularly vulnerable to money laundering. Therefore, financial institutions are expected to apply due diligence procedures and effective monitoring to their correspondent (correspondent) bank accounts. Understanding patterns in their correspondent banks' activities with one another helps improve the institution's knowledge of its customers and identify potential areas of concern. Patterns of potentially suspicious activity among correspondent bank accounts, such as high levels of activity or activity that suggests exclusive relationships between correspondent banks, indicates a hidden relationship.

### **PATTERNS OF FUNDS TRANSFERS BETWEEN INTERNAL ACCOUNTS, CUSTOMERS, AND EXTERNAL ENTITIES**

An institution's customers may have multiple accounts that span various business lines and are not linked clearly in the institution's transaction or account systems. This can present vulnerabilities to money laundering because the customer can, without detection, wire funds between seemingly unrelated accounts (which may be titled differently) to aid in the layering and integration of illicit funds. Similarly, this activity may take the pattern of potentially suspicious activity between internal accounts/customers and external entities.

Understanding patterns in client accounts and customer activity helps to improve the institution's knowledge of its customers and identify potential areas of concern.

### **PATTERNS OF RECURRING ORIGINATORS AND BENEFICIARIES IN FUNDS TRANSFERS**

A major issue in money laundering surveillance is “knowing your customers’ customers.” This is problematic in certain areas, such as correspondent banking because of the incidence of “nested bank” relationships. This occurs when relationships exist between entities external to the institution that use the institution or its correspondents as an intermediary for funds transfer activity.

These hidden relationships may present vulnerabilities to money laundering because the external entities can, without detection, wire funds between seemingly unrelated accounts at various institutions.

### **KNOWN AND UNKNOWN REMITTER AND BENEFICIARY NAMES IN CHECKS AND MONETARY INSTRUMENTS**

Financial institutions should also examine possible money laundering or fraud involving checks or monetary instruments with recurring remitters or beneficiaries or both. This activity can be the evidence of attempts to structure deposits and move funds back and forth between accounts to hide their origin. It can also indicate a fraud scheme. Riskier yet are remittances through correspondent bank accounts involving significant percentages of unknown parties.

### **JOURNALS BETWEEN UNRELATED ACCOUNTS**

Money launderers may establish several accounts within a single institution, often establishing relationships at multiple branches using aliases or slightly different identifying information. They then move their money between the accounts as part of a layering strategy, often consolidating the funds in a single account before removing them from the institution. Without a known link, institutions have an extremely difficult time identifying these relationships.

### **DETECTING HIDDEN RELATIONSHIPS**

The benefits of identifying hidden relationships go well beyond complying with domestic and international regulations. In most cases, hidden networks indicate higher-level money laundering activity or effort. As a result, hidden networks pose much greater risk to financial institutions.

By identifying hidden networks, a financial institution has a much better chance of forcing launders to either change tactics or avoid the institution altogether. That said, identifying hidden relationships is one of the most difficult AML challenges. Oracle has designed a variety of AML detection modules to address the wide variety of problems. Having a suite of detection modules allows Oracle Mantas to apply the most relevant and suitable module for solving the specific business problem being addressed. Additionally, each detection module used by Oracle Mantas fully exposes the logic and reasoning applied in finding the behavior of interest. This is accomplished by presenting all the underlying business data that

**By identifying hidden networks, a financial institution stands a much better chance at forcing money launders to either change tactics or avoid the institution altogether. That said, identifying hidden relationships is one of the most difficult AML challenges. Oracle has designed a variety of AML detection modules to address the wide variety of problems.**

contributed to the behavior detected, which might also be used by a business analyst in resolving an alert raised by the system.

Link analysis finds hidden links between accounts and pieces this information into larger webs of interrelated accounts. Once a group of linked accounts is found, their behavior can be examined as a group, which can unmask previously hidden suspicious patterns of behavior. This technology is particularly applicable for problems where “rings” of perpetrators are involved.

Link analysis and sequence matching are Level 4 detection techniques not found in AML solutions offered by other companies, and each is particularly useful in detecting hidden relationships or networks. Because criminals constantly adapt their behavior to evade existing detection systems, their problem behavior becomes ever more complex, spread out over time, and difficult to detect. Techniques such as link analysis and sequence matching expose hidden relationships and uncover what otherwise might not have been found.

## LINK ANALYSIS

Link analysis finds hidden links between accounts and places this information into larger webs of interrelated accounts. At the simplest level, consider the three accounts shown in Figure 2.

The diagram shows a table of account information with columns for ACC T #, NAME, ADDRESS, PHONE, and CELL. A mouse cursor points to the table. Arrows indicate links between accounts: one arrow points from the first two accounts to their shared address (123 Main St), and another arrow points from the last two accounts to their shared cell phone number (555-6644).

ACC T #	NAME	ADDRESS	PHONE	CELL
00000345	Mr. Ed Sender	9 00000 00	000-0000	550-0000
90455987	Mr. Ed Sender	32 First Rd	555-9096	000-0000
90553745	Ms. Sue Smith	123 Main St	555-1234	555-6765
90567345	Mr. Bob Jones	123 Main St	555-2244	555-6644
90594856	J. Evans	456 Oak Ln	555-3993	555-6644
90634121	Mr. Smith	00 00000 Rd	000-0000	555-2949
90620000	0000 000	00 000000	000-0000	000-0027

Figure 2: Example of link analysis

The first two accounts are linked by a common address. The second two accounts are linked by a shared cell phone number. Thus, all three accounts are linked together. While this example focuses on a very small (and simple) group of accounts, the principal at work is the same when vastly larger webs of accounts are detected. Accounts may be linked in much more subtle ways, such as sharing a common beneficiary, or evidence that the parties involved do business with each other, such as writing checks or wiring funds to each other. Once a group of linked accounts is found, their behavior can be examined as a group, which can unmask previously hidden suspicious patterns of behavior. This technology is particularly applicable for problems where “rings” of perpetrators are involved.

## SEQUENCE MATCHING

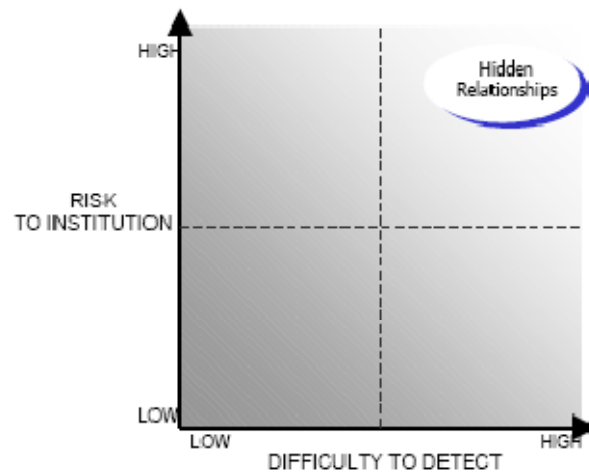
Sequence matching is employed when a particular order of events (such as those transpiring over a period of time) contains some important clue that points to a hidden relationship or relationships. For example, a stock trader who receives a large customer order may try to trade ahead of that order because she believes it will move the market and give her instant profit. Likewise, networks of accounts can be identified by examining patterns that occur over time of deposits, withdrawals, and transfers between accounts.

Sequence matching can define a problem series of events or behaviors in advance and then it searches for any occurrence of a telltale sequence among the thousands of trades and orders taking place on a particular day. Because criminals, money launderers, and fraudsters constantly adapt their behavior to get around the existing detection systems, their problem behavior grows ever more complex, extensive over time, and difficult to detect. As criminals vary their behaviors to defeat simpler and older detection methods, compliance officials at financial services firms must employ more and more sophisticated technology—such as behavior detection and techniques such as link analysis and sequence matching—in order to expose hidden relationships and uncover what otherwise would most likely have remained covered tracks.

## A MULTIPURPOSE SOLUTION

Few areas of compliance have seen the flux and flurry of activity that has become common in anti-money laundering. Institutions are tasked to address the requirements of both domestic and international guidelines in a rapidly changing regulatory environment. Moreover, financial institutions are realizing the intrinsic correlation between compliance and reputational risk. In the supercharged competition for market share, institutions simply cannot risk damage to reputation, client trust, and market capitalization that result from financial abuse and illicit activity. Based on the Oracle Mantas behavior detection platform, Oracle Mantas Anti Money Laundering monitors accounts, customers, and correspondence across business lines for suspicious activities and possible money laundering, including the detection of hidden relationship and hidden networks. The solution provides automated, comprehensive, and consistent surveillance and enables a global understanding of customer relationships and funds moving to and from the institution. The product alerts analysts to detected behaviors and provides a context of business data and historical information with which to streamline analysis and resolution.

**Sequence matching is employed when a particular order of events (such as those transpiring over a period of time) contains some important clue that points to a hidden relationship or relationships.**



**Figure 3. Identifying hidden relationships is one of the most difficult AML challenges.**

Oracle Mantas Anti Money Laundering monitors the following major areas of activity:

- Funds transfer activity, such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and Fedwire
- Demand (current) account activity, including deposits, withdrawals, and clearing of checks and monetary instruments
- Cash and cash products activity, including currency and cash equivalent products

Oracle Mantas Anti Money Laundering accepts the following types of data in accordance with formal firm data interface specifications:

- Funds transfers and electronic transactions
- Checks and monetary instruments transactions
- Cash transactions
- Accounts
- Account balances
- Customers
- Correspondents
- Employees
- Watch lists and trust or exclusionary lists (entities, geographies)
- Electronic and internet activity, including Automated Clearing House (ACH) transactions and electronic payment services

**Oracle Mantas Anti Money Laundering uses scenarios that identify behaviors of interest that indicate potentially suspicious behavior and possible money laundering activities. The scenarios can be grouped as high-risk geographies and entities; hidden relationships; anomalies in behavior; other money laundering behaviors; and institutional scenarios.**

Oracle Mantas Anti Money Laundering uses scenarios that identify behaviors of interest that indicate potentially suspicious behavior and possible money laundering

activities. The scenarios can be grouped as high-risk geographies and entities; hidden relationships; anomalies in behavior; other money laundering behaviors; and institutional scenarios.

The following list of scenarios represents a portion of the behaviors that can be identified as indicative of hidden relationships or networks.

- Patterns of funds transfers between correspondents
- Patterns of funds transfers between customers and other entities
- Recurring originators/beneficiaries in funds transfers
- Patterns of recurring remitters/beneficiaries in checks and monetary instruments
- Journals between unrelated accounts
- Networks of accounts and entities

## **CONCLUSION**

Anti-money laundering, and with it the search for hidden relationships, is an enterprise wide challenge. And each enterprise is going to approach those challenges in its own way. The tactic of hiding the true identity or purpose of an account or series of accounts will continue as long as money launders have success in utilizing this method. When this tactic begins to meet resistance, they will likely adopt new methods or will move their money laundering activity to institutions that do not make an effort to uncover hidden relationships. Financial institutions that address the issue of hidden relationships head-on stand to realize multiple benefits:

- Better understanding of the customer base and transaction flow within accounts
- Greater success and relationships with domestic and international regulators
- Reduction of the amount of illegal money laundering activity within the institution
- Positive reputation as an institution committed to ethical business

The application of industry-leading technology makes it possible for financial firms to address hidden relationships and AML in a comprehensive and proven approach. Oracle Mantas Anti Money Laundering, which leverages the Oracle Mantas behavior detection platform's link analysis, fuzzy name matching, and sequence matching technologies, is the most comprehensive and successful AML solution available.



Hidden Relationships and Networks: Financial Institutions at Risk  
October 2009

Oracle Corporation  
World Headquarters  
500 Oracle Parkway  
Redwood Shores, CA 94065  
U.S.A.

Worldwide Inquiries:  
Phone: +1.650.506.7000  
Fax: +1.650.506.7200  
[oracle.com](http://oracle.com)

Copyright © 2008, Oracle and/or its affiliates. All rights reserved.  
This document is provided for information purposes only and the contents hereof are subject to change without notice.  
This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. 1009