A person in silhouette stands in a large, curved, blue-lit tunnel or atrium. The person is positioned in the center-left of the frame, looking towards the right. The tunnel's walls are curved and feature a pattern of light blue, wavy lines. The floor is dark and reflective. The overall atmosphere is futuristic and high-tech.

BUILDING A BETTER RISK MANAGEMENT SYSTEM WHILE SAVING MONEY AND FIGHTING FRAUD

November 2006

A WHITEPAPER BY:
RICHARD W. HARMS, PH.D.

Table of Contents

Table of Contents 2

Executive Summary 3

The General Context of Anti-Fraud/AML/ATF-CFT Risk Management 4

The Core of the Solution – ARMS (AML/ATF/Anti-Fraud Risk Management System) 6

“The Heart of ARMS is Entity Resolution” 6

What is meant by “entity resolution” and why is it critical? 6

Traditional Identity Technology Falls Short 6

Is entity resolution involving individuals different than entity resolution involving businesses/corporations? 7

When are we interested in the linkages an entity has to networks of other entities and objects? 9

How ARMS and Entity Resolution Relate to the Key Components of AML/ATF/Anti-Fraud Risk Management 11

Establishing and maintaining relationships = all aspects of know-your-customer (KYC) 11

Monitoring for and reporting suspicious/unusual activity 13

Managing cases and investigations 15

Responding to specific government requests 16

Managing changes in key government and other authoritative lists of high-risk entities 17

Summary of ARMS Opportunities 18

Cost Savings and Cost Avoidance in Customer ID Verification and Enhanced Due Diligence 18

Process Improvements in Responding to Government Requests 19





Managing the Risk Associated with Doing Business with High-Risk Entities (HREs)	20
Improved Case/Investigation Speed, Efficiency, & Effectiveness	21
Steps to Take to Reach ARMS Functionality	22
Conclusion	23
About the Author	24

Copyright November 2006

Executive Summary

This white paper summarizes the challenges faced by the financial services industry in meeting the diverse and ever-changing requirements of the battle against money laundering and terrorism funding. Financial services businesses are increasingly becoming the “front line” of this battle, and any form of failure brings dire consequences. We believe that this battle overlaps significantly with the on-going fight financial services businesses wage against fraud. While there are various significant, requisite components in every comprehensive risk management system, without question, the most important is a comprehensive information technology (IT) program.

Doing the right thing involves a precarious balancing act – making certain you catch what you need to catch without jeopardizing innocent relationships or overwhelming your staff with chasing thousands of false positives. This paper gets at the heart of this quandary.

After summarizing the major components involved in managing the risks associated with fraud, anti-money laundering (AML), and anti-terrorist finance (ATF, also known as combating the funding of terrorism (CFT) in the EU), this paper demonstrates that the “glue” that can best hold together the disparate requisite IT components of a comprehensive risk management system is a solution/process we call ARMS (AML/ATF/Anti-Fraud Risk Management System). The key to the success of ARMS is its ability to recognize entities and their relationships. We refer to this as “entity resolution”, and its nature and criticality are described in detail.

We then describe how ARMS and entity resolution relate to each key component involved in AML, ATF/CFT, and anti-fraud risk management. While part of the task may involve almost real-time transactional analysis (e.g., interdicting funds being transferred electronically by entities on which government authorities are focused), we make the point that the function of ARMS extends far more deeply than that. The requirements for real-time matching are, in fact, somewhat simple – does a name on a wire transfer match a name on a government list. ARMS, on the other hand, carries the concept to its full extent – is there any way that we can recognize relationships with or linkages to an entity in question. Throughout, we present examples of risk management failures that could have been mitigated if ARMS had been deployed.

Lastly, we offer first steps and a generic roadmap for the implementation of ARMS.

The General Context of Anti-Fraud/ AML/ATF-CFT Risk Management

Globally, financial institutions and financial service businesses of all types face a huge task at present and into the foreseeable future meeting AML and ATF/CFT challenges. At the same time, these businesses face the assault of evermore sophisticated fraudsters whose sole objective is to take money from the institutions and/or their customers. Performing these tasks poorly or incompletely leads to direct financial losses as well as fines, penalties, damage to reputations, and decreased shareholder value.

Who can argue this point in light of recent history? In this white paper, we will refer for illustrative purposes to a number of glaring failures on the part of financial institutions. Some, perhaps all, of the situations could have been mitigated by the approach described herein. These examples include:

- ✦ The payment of \$80 million in fines by a Dutch bank for, among other things, taking on Latvian bank business without proper controls;
- ✦ The payment of \$25 million in fines by a US bank for violations of anti-money laundering laws in dealing with foreign embassies;
- ✦ The involvement of a major US bank in the laundering of the funds of Raul Salinas de Gortari (brother of former Mexican President Carlos Salinas);
- ✦ The loss by a major UK bank of millions of dollars as the result of fraud perpetrated by one of its senior managers;
- ✦ The discovery of billions of dollars in fraud against one of China's largest state-owned banks, much of it involving insider complicity;
- ✦ The reputation damage to a number of international banks due to the facilitation of the laundering of the ill-gotten gains of former Latin American and African dictators.

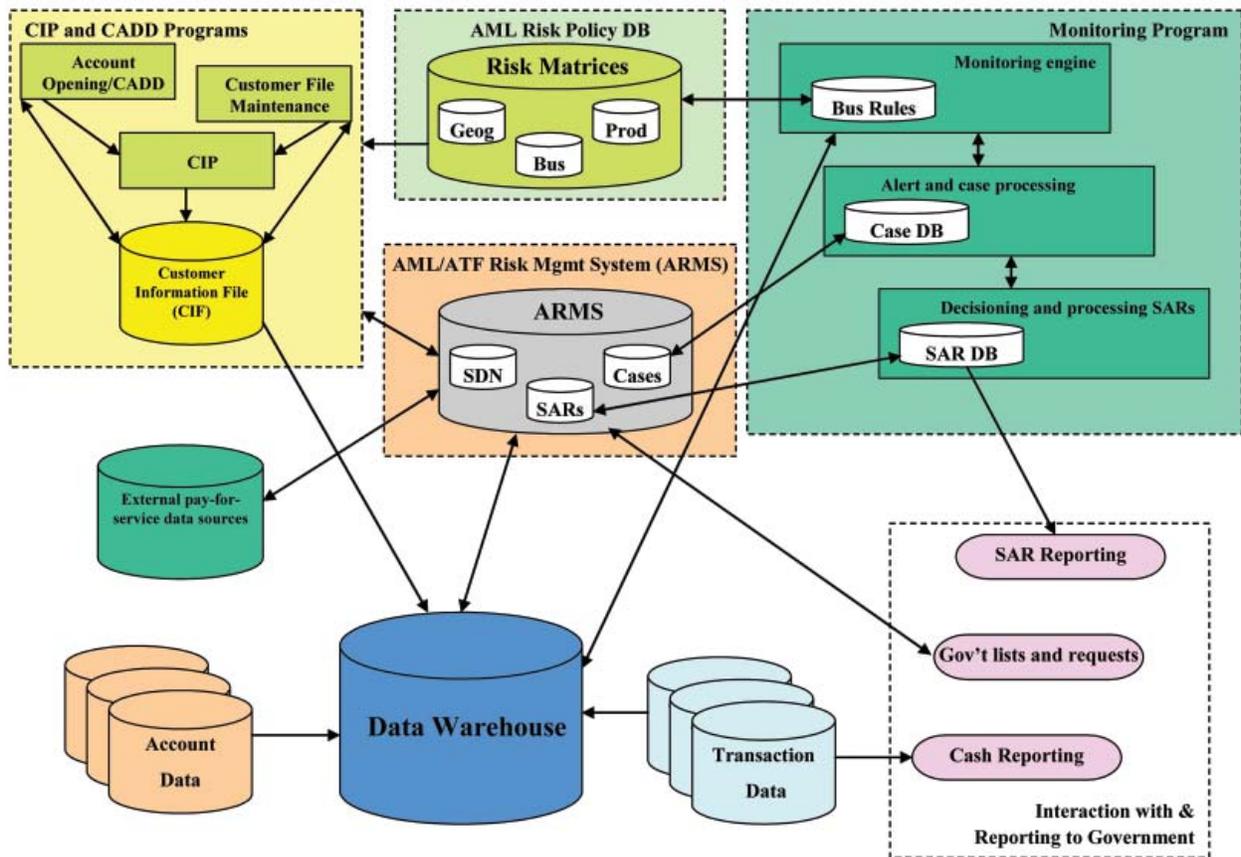
The complex and overlapping AML, ATF/CFT, and Anti-Fraud tasks involve both (a) compliance requirements levied by laws and regulations in most countries and (b) fundamental risk management obligations. With this in mind, we have identified the following primary functional areas of a comprehensive risk management system:

- ✦ Customer Acquisition Due Diligence/Customer Identification Programs (CADD/CIP, collectively often referred to as Know-Your-Customer or KYC) at account opening
- ✦ Customer file maintenance or updating during the course of a relationship
- ✦ Suspicious activity monitoring and reporting
- ✦ Additional reporting and record keeping requirements (e.g., cash transactions, purchases of monetary instruments, international wire transfers)
- ✦ Management and use of information on High Risk Entities (HREs -- e.g., public figures, entities on US, UK, or other government hot lists, and entities on which a financial institution has filed SARs, opened case, received subpoenas, closed accounts, incurred significant losses, etc.)
- ✦ Maintenance and use of the AML risk policy (e.g., the AML geographic, product, and business/entity risk matrices that drive risk-based processes).

The following inputs are generally involved in fulfilling the above obligations:

- ✦ CADD/CIP data and Customer file maintenance data (collected during the building of Customer Information Files or CIFs)
- ✦ Data on high-risk transactions (e.g., wires, cash transactions)
- ✦ Account metrics (data on debits and credits, balances, numbers and values of different transaction types)
- ✦ Business rules used in AML/ATF/Anti-Fraud monitoring
- ✦ Internal data mining and analysis of trends and patterns in alerts, cases, and Suspicious Activity Reports (SARs)
- ✦ Issuances on AML/ATF matters of concern (e.g., from authoritative government sources such as FinCEN, FATF, US State Department, OECD, UN, Bank of England)
- ✦ Government laws, regulations, and guidance.

Given the volume of data and the complexity of the requirements and their interaction, information technology **must** play a key role in the success of any comprehensive risk management system. The following diagram illustrates the manner in which these requirements and the systems that support them interact with one another.



The Core of the Solution – ARMS (AML/ATF/Anti-Fraud Risk Management System)

ARMS is the physical and figurative center of the diagram above. In the following subsections we discuss the operation, risk management performance, and value proposition of ARMS.

The Heart of ARMS is Entity Resolution: What is meant by “entity resolution” and why is it critical?

For ARMS to function, we must be able to recognize entities and possible relationships with them. In the simplest terms, “entity resolution” (or “entity recognition”) is the process of identifying that different representations of an entity (a person, a trust, a small business, a large corporation, etc.) are, in fact, the same entity. This process is necessary in order to answer the question, “Do we already know an entity [of interest]?” This question is critical in the following circumstances:

- a) At account opening, can we identify that an entity is already a good, fully identified customer, who is simply applying for other services?
- b) During the account opening, employment, and/or merger & acquisition due diligence process, can we discover that an entity is a person or business with whom we cannot, should not, or do not wish to do business?
- c) As the result of AML or fraud monitoring, what do we know about a highlighted entity?
- d) When governmental agency requests information about possible relationships we may have with an entity, can we respond quickly and completely?

Situation (a) represents an opportunity to save money during the account-opening process. Situations (b) – (d) represent the opportunity to avoid financial losses as well as possible fines, penalties, and reputation damage.

Traditional Identity Technology Falls Short: Why Entity Resolution Is Unique To Supporting ARM

FSP’s have struggled with creating the 360-degree identities necessary to manage operational risk. Part of the problem is that much of the current recognition technology was originally designed to support Customer Relationship Management (CRM) or data warehousing missions, not Anti-Fraud.

Technologies such as Data Quality, Customer Hubs, & ETL can be found in most large banks supporting direct marketing and operational effectiveness programs, but these technologies were not designed to independently address the complex entity resolution requirements of creating a true ARM system.



In most banks the quality of raw customer level identity data is very low. There is a fundamental analytical difference between three individuals, each with a single bank account, and one individual with three bank accounts. Traditional approaches usually compare two identity records and use data survivorship rules to create a single “clean” record, (De-Duplicating To A Single Representation).

The traditional 360 degree view of the customer driven by direct marketing follows the road of de-duplication or merge/purge. Using this approach, the system employs data survivorship rules to make a judgment on what is the most accurate representation of an identity, and then proceeds to delete or purge the other representations of identity from the system. This approach creates a thin identity with a very limited set of attributes, usually name and address. This “Thin Identity” or Snapshot is given a unique identifier and is used across departments when marketing, sales, accounting, etc need a single customer view.

This merge/purge approach is sufficient for direct marketing where the largest concern is address validation to reduce costs associated with direct marketing. However, it is insufficient for threat and fraud efforts where analysts and investigators need to know not only who the entity is today, but who the entity was last week, last year, etc.

Entity Resolution **should not employ merge/purge, data survivorship, or data fusion processes** in resolving identities. Unlike the direct marketing-driven approach, an anti-fraud focused approach must maintain all of the identity data (i.e. provide all versions of truth) about an individual, regardless of the determined quality of that data is. For example, if the entity Resolution process was to determine that a single unique identity was made up of 16 independent records, attributes, etc., your process should apply a persistent key to the 16 data pieces so you know that they were “all moving together”. This is a capability that is fundamental to the success of any Anti-Fraud, Anti-Terrorism Funding risk management system.

Is entity resolution involving individuals different than entity resolution involving businesses/corporations?

The simple answer is distinctly “yes.” Successful entity resolution of both individuals and businesses requires both names and attributes (for example, address, tax ID number, passport number, driver’s license number, date of birth, phone/fax number). It is impossible to distinguish one “John Smith” from another (or one “ABC, Inc.” from another) without unambiguous additional information.

Therefore, once we have specific attribute information about individuals, we must have the ability to handle:

- a) Culturally based name variations;
- b) Aliases;
- c) Nicknames; and,
- d) Prefixes (e.g., Dr., Rev., Mr., Mrs., Miss, and their equivalents in numerous languages).

(a) Culturally based name variations are important whenever we are dealing with a diverse population of customers, particularly when that population includes customers whose native languages are character-based (for example, Arabic, Korean, Japanese, Chinese, and Indian). Without any attempt at obfuscation, the interpretation of character-based names into Western alphabet can yield widely diverse representations. We must be able to discern these variations when determining if we “know” an entity.

The following example clearly illustrates this point:

The Arabic name محمد ابراهيم عبدالرحمن شريف has the following four of many possible transliterations/permutations, depending on which part of the Arabic world is interpreting the characters:

- Mohammed Ibraheem Abd al Rahman Shareef
- Mhd Brahim Abderrehmane Charife
- Mohamad Ibrahim Abdul Rahman Sharif
- Mohd Abraham Abdelrahman Sharaf

(b) Knowledge about aliases comes into play primarily when we are contending with politically exposed persons (PEPs) or high-risk entities (HREs). Criminals, in particular, have histories of adopting different identities during their career in order to disguise themselves. If a government were to ask if we had a relationship with former Chilean dictator Augusto Pinochet Ugarte, it is important to know that his aliases include “Daniel Lopez” and “Jose Ramon Ugarte.” Thus, a “Daniel Lopez” with the same address or date of birth as “Augusto Pinochet Ugarte” may be the same person. Or, if one were asked about accounts previously held by Yasser Arafat, it is important to know his alias (Abu Amar) and the name on his birth certificate (Mohammed Abadul-Raouf Qudwa Arafat Al-Husseini). In these situations, it is unquestionably worthwhile to realize and then investigate further and resolve each of these possibilities.

(c) It may seem simplistic to raise the issue of nicknames, but most of the formal given names people carry on their passport, driver’s license, or taxpayer identification documents have numerous informal versions that we must be able to recognize. “Richard” can become “Rick,” “Dick,” “Rickey,” “Dickey,” “Rich,” “Ritchie,” “Richart,” “Rico,” or “Ricardo.” Furthermore, “Rick” or “Rickey” can be a nickname for “Frederick,” which itself can also become “Fred,” “Freddie,” or even “Fritz.” To a significant degree, this idea of nicknames overlaps with the concept of culturally based names, because informal representations of given names vary significantly around the world from culture to culture.

(d) It may also seem simplistic to raise the matter of prefixes, but given the numerous linguistic variations of Dr., Mr., Mrs., Miss, etc., the situation can be confusing. How many bank tellers around the world might mistake the following as given names: “De Heer” or “De Vrouw” (“Mr.” and “Mrs.” in Dutch), “Vater” (“Father” in German), or “Ingeniero” (“Engineer” in Spanish, a common prefix in Spanish-speaking countries for people with engineering degrees)?

When dealing with businesses/corporations, we must have the ability to deal with:

- Doing-business-as representations
- Parent companies
- Subsidiaries
- Company officers and principal shareholders
- Beneficial owners (if not included above)

Under the circumstances in which business entity resolution is important, our interest in an entity must extend to the relationships noted above. For example, if a government inquires about a relationship with a specifically named small business (for example, Harms Family Pizza), we must assume that they are interested also in East Norwalk Partners LLC (as in East Norwalk Partners LLC DBA Harms Family Pizza). Similarly, if our AML monitoring system highlights Harms Family Pizza as being involved in unusual activity and we ultimately determine that we must file a SAR on that entity, it stands to reason that we must know (and thus implicate) Richard W. Harms (CEO of East Norwalk Partners LLC).

When are we interested in the linkages an entity has to networks of other entities and objects?

Under most conditions, a financial institution simply needs to know whether it can recognize the different representations of an entity in order to decide whether or not to enter into a relationship with that entity.

However, there are circumstances that justify the effort, indeed sometimes demand the effort, to look into the networks that surround an entity of interest. Following are examples of those circumstances:

- When an entity has been highlighted by a monitoring system or internal control process
- When an entity is seeking a private banking relationship and high-risk factors are involved (such as, a high-risk jurisdiction and/or a high-risk type of business or source of income)
- When an entity is associated with a merger or acquisition target
- When an entity is being considered for a key position of trust in an organization [Note: It could be argued that all entities being considered for employment or as vendors could be reviewed in this manner. On the other hand, there can be no argument that entities being considered for key positions of trust must have their relationships inspected.]
- When an entity may be involved in fraud
- When the government requests information about an entity

If an individual is targeted as structuring cash deposits apparently to evade the cash transaction reporting threshold, we may very well be interested in any other individuals associated with the target's address and in the financial activity of these additional people. The individual targeted initially may be the "tip of the iceberg" of an organized structuring (also known as "smurfing") gang.

Further, if an individual is seeking to establish a high-net-worth relationship (typically with the private banking business of a financial institution) and that individual resides in, has a passport from, or has income derived from a high-risk jurisdiction and/or high-risk business, we are probably going to perform additional due diligence on

that individual. For instance, it is worth the effort to inspect all aspects of a wealthy individual from a high-risk jurisdiction who purports to derive his income from an import-export business and whose initial deposit involves wire transfers from known drug-source jurisdictions.

More pointedly, if the government submits a request for any relationships with former “President of the Federal Republic of Yugoslavia Slobodan Milosevic and close associates,” it is essential that we consider his spouse, his children, his siblings, former Yugoslav government officials with whom he was closely tied, and businesses with which he is linked. For example, the UN War Crimes Tribunal specifically identified the following individuals as members of Milosevic’s “joint criminal enterprise”:

- Borisav Jovic;
- General Blagoje Advic;
- Jovica Stanisic;
- Tomislav Simovic;
- Milan Babic;
- Radovan Stojicic;
- Vojislav Seselj;
- General Veljko Kadijevic;
- General Aleksandar Vasiljevic;
- Franko Simatovic;
- Milan Martic;
- Goran Hadzic;
- Zeljko Raznatovic;
- Momir Bulatovic.

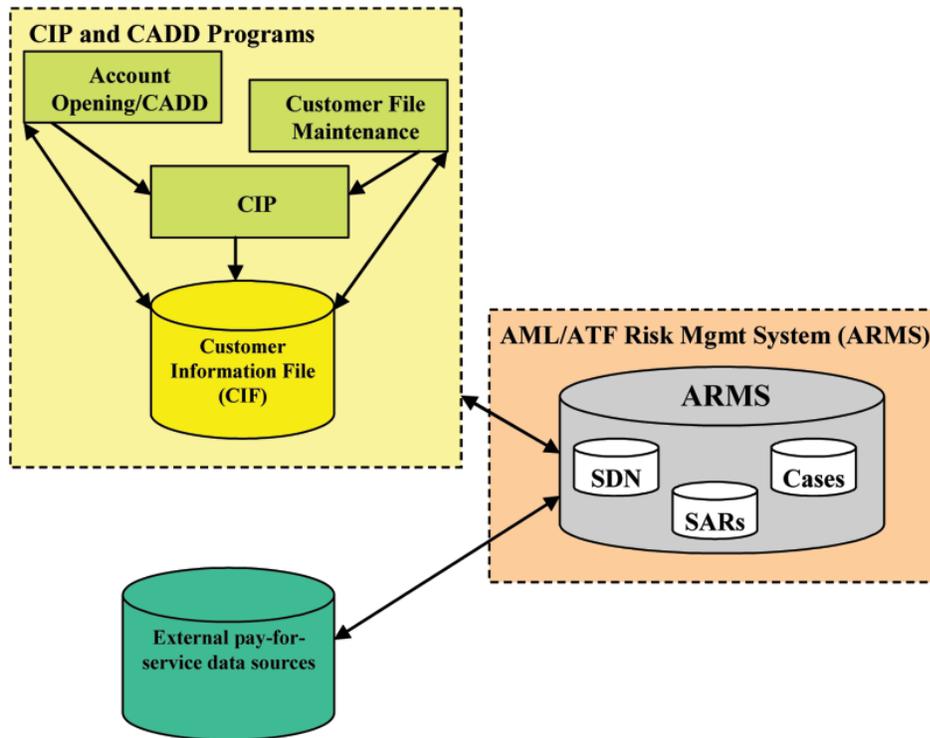
Lastly, two recent examples of significant fraud losses experienced by major banks illustrate how entity resolution and a sophisticated process to recognize relationships/linkages could have come into play to detect the fraudulent pattern and possibly prevent, or at least greatly lessen, the losses. In one case, a major UK bank was defrauded by a senior manager, who concocted fake loans over a period of four years that totaled in excess of £20 million. ARMS may have been able to highlight early on the pattern of fictitious loan applicants (and their attributes) as well as associated transactions.

In the other situation, Chinese authorities announced that illegal loans totaling \$3.5 billion, primarily in car loans and home mortgages, had been uncovered at one of China’s major state-owned banks. At that same bank, 51 cases of criminal wrongdoing involving 157 individuals had been identified by government examinations. The bank itself may have been able to avoid this public embarrassment if it had proper controls and systems, including ARMS, to detect unusual patterns and networks.

How ARMS and Entity Resolution Relate to the Key Components of AML/ATF/Anti-Fraud Risk Management”

To see how ARMS operates, the main components of AML/ATF/Anti-Fraud Risk Management are inspected in detail separately.

Establishing and maintaining relationships = all aspects of know-your-customer (KYC)



When involved in the process of accepting a prospective customer, we have basic obligations both prescribed by statute and imposed by basic risk management principles. In the simplest terms, we must “know” with whom we are dealing. At present, it is simply unacceptable to enter into anonymous relationships. There is no responsible financial institution that does not adhere to the principle of “know-your-customer” (KYC). KYC extends to include the following areas:

- ✦ Basic account opening requirements for even the most elementary of relationships – these would normally include name of account holder, name of beneficial owner (if different than account holder), address, and taxpayer identification number, as well as possibly phone number, date of birth, and/or additional ID number (passport, driver’s license, etc.).
- ✦ In some jurisdictions (or required globally by some multi-national financial institutions because of requirements in their home country), identity verification procedures are expected. In the U.S., this actually involves the establishment of formal Customer Identification Programs (CIPs), which involve either documentary verification (viewing actual documents showing reported address and taxpayer ID number) or non-documentary verification (third-party, pay-for-data services that verify the association between an entity and a reported address or taxpayer ID number).
- ✦ Under many circumstances, additional (or “enhanced”) due diligence (EDD – meaning extra effort, analysis, investigation) are called for. This can involve phone calls to references, site visits to homes and places of business, internet research, and obtaining detailed business reports.
- ✦ Lastly, during the course of a customer relationship some degree of information maintenance or updating should occur. Normally the frequency and extent of such maintenance will be dictated by risk factors. Information on higher risk customers, according to risk factors such as association with high-risk jurisdic-

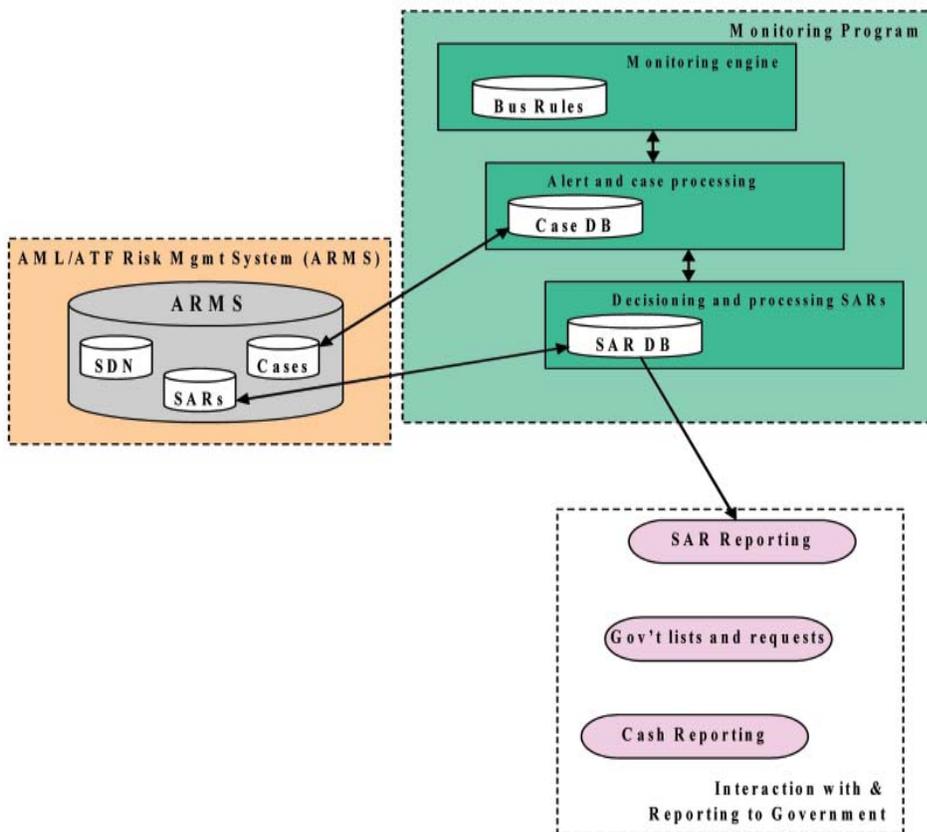
tions, types of businesses or usage of high-risk products, should be updated more frequently than on lower risk customers.

In each of these situations, it is necessary to perform some degree of entity resolution, especially as it relates to recognizing entities that we cannot, should not, or do not wish to do business with. Is the “Jeffrey Skilling” seeking a new private banking account the convicted Enron executive or not?

More commonly, the question is whether or not we already know the entity of interest through another of our businesses and that entity has already been identified, been verified, and has had EDD performed. In such cases, it is not necessary to duplicate what has already been done – that is, paying for verification information that has already been purchased and/or redoing research that has already been completed.

A valid question in the above situation concerns whether or not entities have been added to a high-risk entity list after we have already cleared them. Actually, staying abreast of changes in such lists (either internal or external) is an integral function of ARMS – see section on “Managing changes in key government and other authoritative lists of high-risk entities.” All changes (or “delta”) in any list are treated as “new” entities and are checked against all existing relationships. Thus, a heretofore “clean” customer, who has been added to the US Office of Foreign Asset Control’s Specially Designated National (SDN) list and/or the Bank of England’s list as a known money launderer, will be highlighted by ARMS during the ingestion of the updated SDN list.

Monitoring for and reporting suspicious/unusual activity



In most jurisdictions, financial institutions and financial services businesses have an affirmative obligation to report suspicious activity to government authorities. Even without this requirement, it is important for these businesses to be able to identify and counter fraud in their midst. Monitoring for fraud and monitoring for other unusual activities that are unusual (and may also be suspicious and reportable) involve information technology. These automated monitoring systems are augmented by other control processes (e.g., staff training to observe unusual behavior, internal audit, external audit).

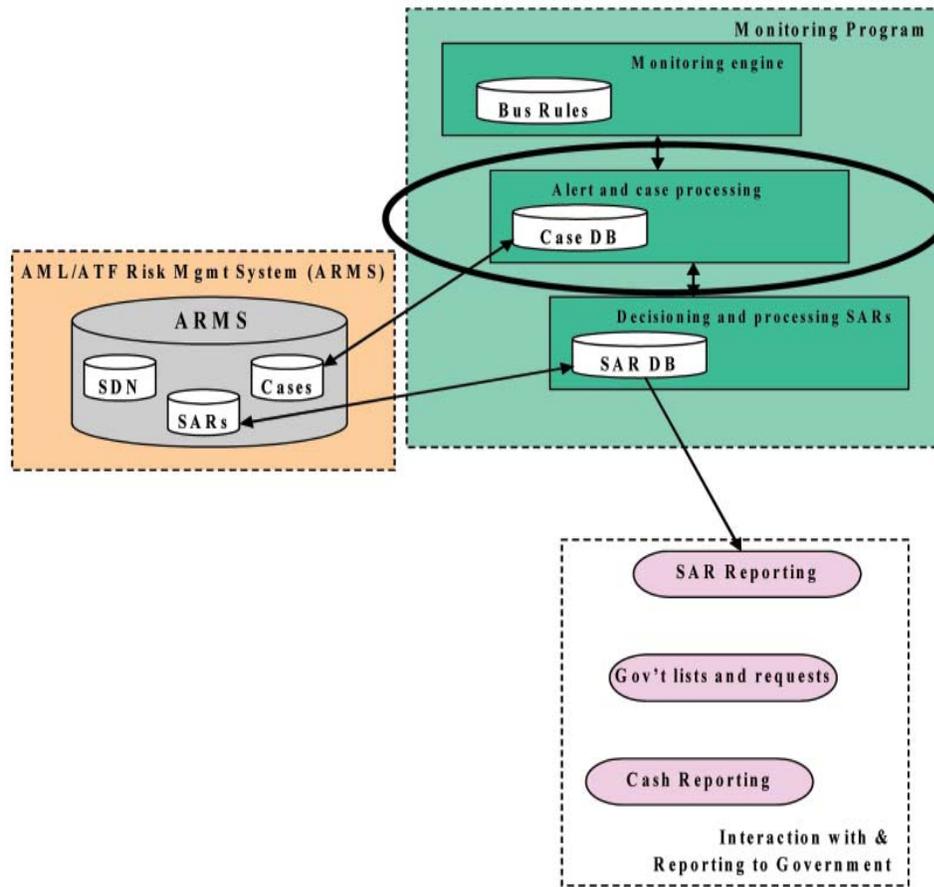
The following circumstances can lead us to become interested in a potentially suspicious entity and its activities:

- Alerts are generated by automated monitoring software
- When matters of interest are identified by staff vigilance
- The media reports criminal convictions
- Colleagues from other financial institutions legally share target information
- During examinations, the regulators specifically identify entities on which they would like additional information
- Internal or external auditors raise questions about entities they believe should perhaps have been investigated

It is important however, to point out that transactional monitoring software is not designed to resolve entities. Rather it is designed to monitor activity attached to an account. Problems and blind spots are inevitable if the perpetrators are conducting transactions using multiple identity packages attached to multiple accounts. Without sophisticated identity resolution systems that resolve identities across multiple identity misrepresentations, packages, etc., to a single entity (account holder), these technologies will not reveal a complete view of the attempted transaction.

When we focus on an entity for the above reasons, we are distinctly interested in entity resolution. We can leave no stone unturned in these circumstances.

Managing cases and investigations

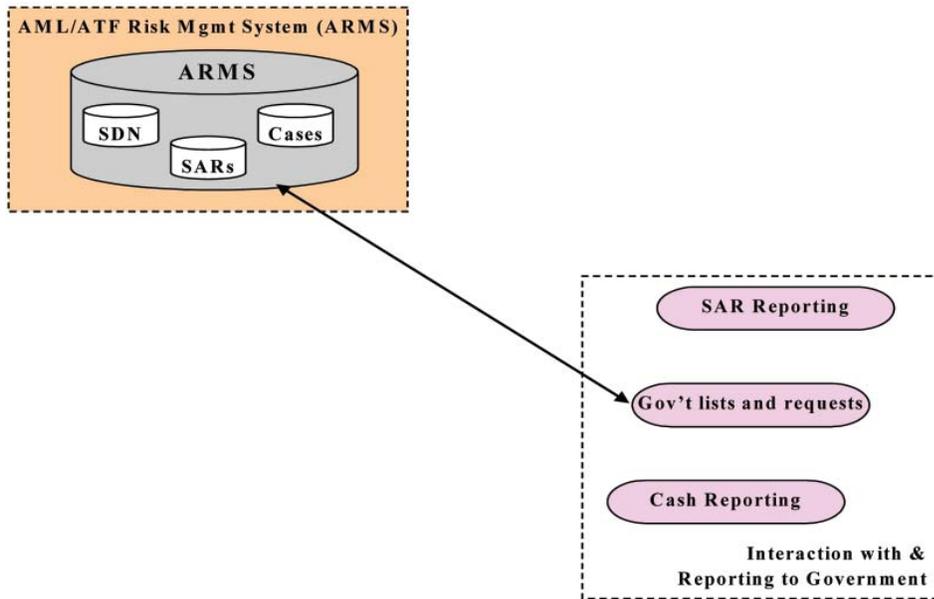


This component of the overall AML/ATF/Anti-Fraud information technology context overlaps with the preceding “monitoring” component. For example, once an entity truly becomes an object of interest, most often a formal “case” is opened in a case management system. These case management systems vary in their complexity from fairly simple databases (that store information on the entity as well as notes on the investigation) to sophisticated software systems (that track all enquiries conducted during the investigation, attach all documents and other items surfaced during the work, and can automatically display complex link diagrams).

Investigations that require full entity resolution as well as the identification of associated links and networks are most commonly initiated by:

- ✦ AML/ATF analysts
- ✦ Anti-fraud investigators
- ✦ Security staff involved in merger & acquisition due diligence

Responding to specific government requests



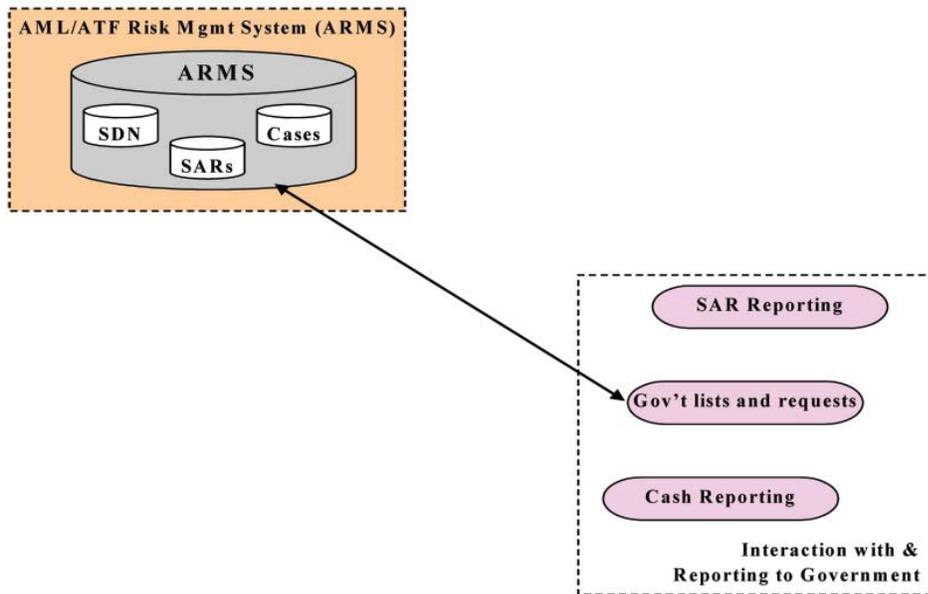
Government authorities have a number of processes by which they can legally require financial institutions to provide information on customer relationships. These include:

- Subpoenas issued through judicial authorities
- Special requests from duly authorized government officials – such as those issued by the US Department of Treasury, requesting information on possible relationships with Augusto Pinochet Ugarte, Yassir Arafat, Sani Abacha, or Slobodan Milosevic
- In the US, the bi-weekly lists issued by the Financial Crimes Enforcement Network (FinCEN) under Section 314(a) of the Patriot Act

When the government submits such a request, we are obligated to respond, typically within a specified period of time. In addition, it is in our best interest to respond as completely as possible. Full entity resolution and network detection become key factors in accomplishing this task.

For example, when we receive an official government request to “identify relationships with [former Liberian dictator] Charles McArthur Ghankay Taylor and close associates,” we must be able to discern not only Taylor’s aliases (and possible relationships under these false identities), but we must also identify relationships in, among others, Taylor’s son’s name and aliases (that is, Charles McArthur Emmanuel aka Chuckie Taylor, Jr., Dankpannah Charles Ghankay Taylor, Dankpannah Charles Ghankay Macarthur) and Taylor’s company’s name (that is, Lone Star Company, a cell phone distribution business).

Managing changes in key government and other authoritative lists of high-risk entities



We previously covered the obligation at account-opening to make certain that we have not entered into a relationship with an entity that we cannot, should not, or do not wish to do business. Among the most important relationships we must avoid are those with entities posted on high-profile, well-known “black” lists – such as, the US Treasury’s Office of Financial Assets Control (OFAC) Specially Designated Nationals (SDN) list of drug traffickers, money launderers, and terrorists and the similar list issued by the Bank of England.

After we have done due diligence during account opening, and we know that we have no watch listed entities among our customers, we will constantly get updates of undesirable entities from OFAC, the Bank of England, and other authoritative sources. When such updates occur, we must know expeditiously whether or not a heretofore low-risk entity has become a high-risk entity. Once again, entity resolution is key to the completion of this task.

Further, when we confirm that we now have a high-risk entity in our midst, we have businesses to notify internally (to take action) and government officials to notify. Failure to completely and promptly accomplish these tasks significantly increases our vulnerability to fines, penalties, and reputational damage.

Summary of ARMS Opportunities

We have provided details on the operation and risk management performance of ARMS. One can justify the expenditure and effort to create ARMS based on risk management principles alone. On the other hand, would it not be advantageous if the enterprise that undertakes to establish ARMS can also experience cost savings and cost avoidance totals that help ARMS pay for itself?

Cost Savings and Cost Avoidance in Customer ID Verification and Enhanced Due Diligence

We previously described the circumstances at account opening when customer identification verification and/or enhanced due diligence are required. Related to individuals, customer identification verification often involves reaching out to pay-for-data sources (such as Axiom, Choicepoint, Experian, etc.) that charge on a per transaction basis, to verify that an address, phone number, and/or ID number are associated with a prospective customer. Vis-à-vis businesses, verifying bona fides often involves reaching out to other pay-for-data sources (principally Dun & Bradstreet reports) to verify the circumstances and good standing of a prospective customer.

In large, complex financial institutions, which emphasize cross-selling, the likelihood exists that disparate businesses in the corporate family are duplicating CIP and EDD costs. One business may have no way of knowing that a sister business has just paid for and filed information that clears a prospective customer. As a result, they conduct and pay for this duplicate activity and information separately.

With ARMS, such duplication of effort and cost can be eliminated. With account opening systems “checking with” ARMS as a first stop early in the customer acceptance process, a business has the ability to know that the enterprise already “knows” the entity in question as a good, fully identified customer, who is simply applying for other services and products. For documentation purposes, data and reports that have already been paid for can be made part of the customer files of these additional businesses.

To estimate the potential savings derived from avoiding these duplicate costs, an enterprise can perform the following calculations:

- (1) For individuals,
 - a. Estimate the number of new customer relationships annually in which a relationship with more than one service/business is involved,
 - b. Multiply this number by the transaction cost of verifying ID, address, etc. (usually less than \$1 per inquiry).
 - c. If, for example, 250,000 new customers per year seek products in at least two different businesses and the cost of the ID verification is \$0.75, the direct cost saving is \$187,500 per year.
 - d. Consider the additional savings if successful cross-selling generates additional relationships for these new customers in three or four different businesses.
- (2) For businesses/companies,
 - a. Estimate the number of new customer relationships annually in which a relationship with more than one service/business is involved,
 - b. Multiply this number by the cost of obtaining requisite business reports. (usually on the order of \$5-\$10 per report).
 - c. If, for example, 200,000 new companies per year seek products in at least to different businesses and the cost of a full business report is \$7.50, the direct cost saving is \$1.5 million per year.
 - d. Again, consider the additional savings if successful cross-selling generates additional relationships for these new customers in three or four different businesses.

A more difficult to quantify but no less-important consideration is the time savings generated by the operation of ARMS as noted above. This process should result in a faster account-opening process – that is, a business receives a quicker “green light” to enter into a revenue-generating relationship with a new customer.

Process Improvements in Responding to Government Requests

Most financial enterprises have legal and/or operational staffs dedicated to responding to subpoenas, FinCEN 314(a) lists, and special government requests. The personnel devoted to such tasks can involve considerable size and cost. Without ARMS, personnel given the assignment to identify possible relationships with targeted entities must contend with (a) incomplete knowledge about the entities' aliases and relationships, (b) multiple customer/account databases to check, and (c) often simplistic and variable name-matching capabilities in these various databases. Single name inquiries spread across multiple businesses and databases can involve considerable effort and cost.

Furthermore, the result of the interaction of the above factors yields conclusions in which we cannot have supreme confidence. Does it make sense to expend great effort, incur considerable cost, and take a significant amount of time to generate questionable findings?

ARMS offers the opportunity (a) to have a single database to query, (b) armed with a uniform, sophisticated name-matching capability that can account for culturally based names and aliases as well as key linkages and that (c) can achieve results in a short period of time. The results of the above include:

- ♦ potential to reduce the size of the staff dedicated to these activities, and/or
- ♦ opportunity to focus on increased thoroughness in the analysis of results.

To estimate the scale of potential savings that result from the above process improvements, an enterprise must first understand all the direct costs involved in processing subpoenas, responding to the bi-weekly FinCEN 314(a) lists, and answering special requests. A more difficult to quantify but no less-important consideration is the much higher confidence in the results provided by the operation of ARMS. This confidence is of significant value to the enterprise and the law enforcement officials and regulators making the requests.

As an example, if we have twenty (20) staff members dedicated full-time to the above activities (20 full-time equivalents of FTEs), and an analysis of process improvements due to ARMS indicates that we can reduce the current processing time by 40%, we can either reduce FTE by 40% (8 employees), focus the staff on better, more thorough analysis, or some combination of both. If we opt for staff reduction (and assuming that fully-burdened costs per employee are between \$50,000 - \$100,000), this option may yield savings of between \$400,000 - \$800,000 per year.

Managing the Risk Associated with Doing Business with High-Risk Entities (HREs)

Savings based on process improvements (e.g., quicker, more thorough processing) are encompassed in the previous section. Generally, it is difficult to quantify direct savings from the use of ARMS to successfully manage the risks associated with high-risk entities. However, financial institutions can avoid fines, penalties, and regulatory disruption by ensuring:

- (a) we do not enter into relationships with certain types of high-risk entities (for example, SDNs or known criminals)
- (b) we know and treat appropriately our relationships with senior public officials (SPFs, also known as PEPs or Publicly Exposed Persons)
- (c) we can quickly identify and react to a situation when a previously low-risk customer becomes a high-risk customer.

Moreover, we can avoid the stigma and embarrassment associated with unknowingly entering into such relationships. This is a key component of reputation risk management. A financial institution's reputation is a priceless asset, which when damaged, generally results in a loss in shareholder value.

Riggs Bank is a perfect example of the criticality of this process. It is no exaggeration to state that their relationships with Augusto Pinochet Ugarte (and close associates) and Teodoro Obiang Ngeuma Mbasogo, the dictator of Equatorial Guinea, resulted in the demise of Riggs Bank. In addition to \$25 million in civil penalties for AML program failures, the reputation damage to Riggs and the disruption caused by the Senate investigations and OCC regulatory actions resulted in the sale of Riggs Bank to PNC Bank in 2004 and the disappearance of the Riggs Bank brand name. This damaged reputation and the resultant fallout destroyed an institution with a storied history dating back to 1836.

Improved Case/Investigation Speed, Efficiency, and Effectiveness

We previously discussed the ways in which entities typically become the focus of cases/investigations – that is, as the result of AML or fraud monitoring, internal control processes, and merger & acquisition due diligence. ARMS has the ability to put analysts and investigators rapidly in touch with key information on the entities of interest. For example:

- previously filed SARs
- other cases/investigations in other businesses
- networks associated with the targets
- all account relationships (and potentially employee, vendor, supplier, etc., relationships)

When dealing with situations that may result in the filing of SARs and the closing of accounts, ARMS speeds up the process and increases the thoroughness of the analysis/investigation. It can be difficult to quantify what these process improvements yield in cost savings although their savings are real and significant.

On the other hand, when we are dealing with situations involving possible fraud, ARMS can rapidly provide a fraud investigator with all relationships across the enterprise. This allows the investigator to understand the full potential exposure to a fraudster and thus identify and close avenues to further fraud. In almost all current situ-

ations, at best a fraud investigator requires hours, perhaps days, wading through numerous disparate systems to accomplish this task. At worst, the fraud investigator does not have access to all the information he/she requires and can never fully identify the exposure.

While it is difficult to quantify potential reductions in fraud losses with a definite degree of accuracy, consider the possibilities when fraud investigators have almost immediate access to all the information they need to prevent additional losses. Information about actual fraud losses experienced by financial institutions is typically closely guarded. However, for illustrative purposes, consider a financial institution that experiences fraud losses of all types (e.g., check fraud, wire fraud, mortgage fraud, insurance fraud, credit card fraud, identity theft, etc.) totaling \$50 million per year. If ARMS can help reduce these losses by a mere 1% (a hyper-conservative estimate), the savings represent \$500,000 of real money saved per year. Now consider using ARMS to reduce fraud losses by as much as 10% (a moderately conservative estimate). The savings represent \$5,000,000 of real money saved each year.

Steps to Take to Reach ARMS Functionality

1. Start with Names – Names are the most basic identifiers for both individuals and businesses. Good name resolution systems include:
 - a. A database of names from most countries around the world
 - b. Intelligence for applying localized conventions or standards based on the region or country where the transactions are being analyzed.
2. Expand to Identities and Resolve Entities – In addition to names, an identity, such as an individual, is composed of other elements, such as addresses, phone numbers, government ID numbers, date of birth, employers, etc. Good identity resolution systems:
 - a. Should accommodate an unlimited number of identity elements
 - b. Must keep a history of all identity elements to assure the greatest ability to detect fraudulent or suspicious identities
 - c. Track both individuals and businesses, since business linkages are critical to fighting fraud
 - d. Must be both real-time to prevent fraud when possible and transactional for on-going analytics
3. Expand to Networks of Identities and Resolve Relationships – While individuals can cause serious financial losses, significantly more damage is done by networks of criminals working together. Good relationship resolution systems:
 - a. Must be linked to the identity system that is maintaining a history of all known identities' elements.
 - b. Must be able to detect both obvious relationships (for example, a potential client living at the same address as someone on the OFAC watch list), and less obvious relationships (for example, a potential client who previously lived at the same address as someone who shares a phone number with someone on the OFAC watch list).
 - c. Must be open-standards based so they can be integrated to a variety of front-end applications and watch lists, as well as integrated to a variety of target “output” investigation tools and applications.

Conclusion

We have presented a comprehensive perspective on fraud, AML, and ATF-CFT risk management challenges and the critical role that information technology must play to meet these challenges. Further, we have provided details on what we view as the most critical component of the IT solution, what we refer to as “ARMS” (AML/ATF/Anti-Fraud Risk Management System), as well as its key function, “entity resolution.”

We provide a number of examples of costly risk management failures that ARMS could have been instrumental in preventing. In no way do we imply that the implementation of ARMS is a simple and cheap undertaking. However, the endeavor is clearly worth the required effort. We also demonstrate that the deployment of ARMS has both direct and indirect cost savings and potential loss reductions that more than justify the requisite expense.

Ultimately, the answer to the question of “Should we use ARMS to build a better risk management system while saving money and fighting fraud?” may lie within senior executives’ willingness to face government officials, or their own shareholders, after front-page exposure reveals the sort of preventable risk-management failure we describe.

About the Author Richard W. Harms, PH.D.



Rick Harms has over 22 years of experience in domestic and international anti-money laundering work. After twelve years as a college professor, Rick began his career in anti-money laundering work in 1983 by joining the U.S. Customs Financial Intelligence Branch. He became the director of that unit, and when the U.S. Treasury Department created the Financial Crimes Enforcement Network (FinCEN) in 1990, he was a member of the task force that planned and created the unit and he became an original assistant director. In 1992, he began work as a consultant with the Australian Transaction Reports and Analysis Centre (AUSTRAC), for whom he worked until 1995, developing money laundering detection and suspicious transaction reporting systems. In 1995, he returned to FinCEN as a senior

advisor, focusing on work with the world's growing number of other financial intelligence units and participating in the development of the Egmont Group.

In 1997, he joined PricewaterhouseCoopers, where he directed AML work for gaming, banking, insurance, securities, asset management, and corporate clients in the U.S., Mexico, South Africa, Australia, the Caribbean, and Europe. He was primarily responsible for making recommendations for reducing risks and establishing "best practices" in money laundering deterrence and compliance, including implementing know-your-customer profiling and monitoring solutions.

Rick Harms joined Citigroup in December 2001 to enhance the company's AML risk policy, manage the expansion of Citigroup's global AML analysis capabilities, and help implement a unified AML IT strategy.

Specific Experience

- ✦ Served as contracting officer for the Customs Artificial Intelligence System, one of the first computerized, rule-based systems in law enforcement.
- ✦ Directed the inter-agency steering group for AUSTRAC that developed an automated system to identify criminal targets (including bank fraud, securities fraud, and narcotics-related money laundering) from cash transaction and international wire transfer data from financial institutions, gaming establishments, and corporations.
- ✦ Served as FinCEN's Training Coordinator and the Training Steering Group Coordinator for the Egmont Group, the organization formed by the world's financial intelligence units (FIUs) in 1995.
- ✦ Presented domestic and international training and lectures for 20 years on the topics of money laundering and the use of technology to combat money laundering.
- ✦ Consulted with foreign government agencies on the most effective and efficient processes involved in the formation of national anti-money laundering units (financial intelligence units - FIUs).
- ✦ For a number of domestic and foreign financial institutions facing possible legal action related to money laundering, directed the auditing and analysis of the facts and circumstances of allegations and the identification of shortcomings and vulnerabilities to money laundering in policies, procedures, business processes, and transactions.
- ✦ Directed money laundering vulnerability assessments for gaming, banking, insurance, securities, asset management, and corporate clients in the U.S., Mexico, South Africa, Australia, the Caribbean, and Europe and made recommendations for reducing risks and establishing "best practices" in money laundering deterrence and compliance, including implementing know-your-customer profiling and monitoring solutions.



Education & Credentials

B.A. University of California Berkeley (1969) - Geography

M.A. University of California Berkeley (1970) - Geography

Ph.D. University of California Berkeley (1983) - Geomorphology

M.S. University of Oregon (1992) – Curriculum and Instruction

Contact Information

RICHARD W. HARMS AML

36 Calf Pasture Beach Rd.

Norwalk, CT 06855

(203) 853-1982 - phone

rharms001@optonline.net