Fighting Economic Crime with a Resolved Identity Platform

John Slitz,
Chief Executive Officer
SRD

Abstract

Risk management and fraud prevention is serious business, and the IT, investigative, and legal persons whose mission it is to prevent these activities know there is no off the shelf, whole product solution to this problem. As veterans they have the experience, resources, and fire power to build their own CIP processes, as well as access to best-of-breed case management and workflow solutions to assist them in their efforts to harden their organizations from attack and fraudulent manipulation. In large part these systems are successful in their mission, but increasingly in larger banks they have begun to reach the extent of their identification capabilities. The problems are not in the applications or systems. It runs deeper than that, to the underlying identity data and the need to successfully consolidate that data regardless of where it resides, and determine whether the data contains inconsistencies, errors, or deliberate attempts to mask or misrepresent an identity.

The challenge is to build an identity platform that recognizes an individual despite deliberate attempts to mask, shield or misrepresent his true identity, sees beyond a seemingly benign identity to links or relationships to threatening entities, and facilitates the seamless, secure, and privacy compliant exchange of bad guy data across the banking and financial service provider industry

Achieving this new level of identity recognition means the system must maintain the full attribution of each data element, i.e. not discard or purge any information, allowing the system to conjoin or disjoin identities as new information enters the system, and giving investigators an immutable audit trail that can trace each data element back to the source system from which it came. The system should be able to facilitate changes to an identity at the moment the data enters the system in order to defeat masking attempts as they occur at the system entry point. It should also be able to perform "link analysis" to connect seemingly benign identities to not-so benign outside threats and do so in real time. Data should be anonymized for cross company, department, and industry sharing, as well as cross referencing against OFAC and government watch lists. This technology should be easy to integrate into existing AML, CIP, and anti-fraud programs with minimal re-engineering, as well as support existing industry standards and future, as yet to be disclosed, missions.

Such a system does exist and is actively in use within the federal government. This article discusses its application within the financial service industry.

Introduction

Fraud, a growth industry: Low entry cost high profitably

Amidst the economic downturn there is an industry that continues to expand at hypergrowth rates. It is multinational in nature and crosses the line between the public and private sector. The cost of entry is very low – there is no need for extensive educational backgrounds or Fortune 500 resumes. Start-up costs are reasonable; all that is required is a PC, phone line or a cooperative friend in a trusted position. The rewards are great – from the hundreds to the hundreds-of-millions. Market players are highly adaptive to ever changing conditions and introduce innovative new approaches and processes at a steady cadence.

The industry is fraud and the main targets are banks and financial institutions.

Financial service providers (FSPs) have been in a pitched battle with money launderers, identity thieves and crooked brokers for the better part of the last century. What have changed are the motivations of the groups who perpetrate these crimes. From al-Queda to the Russian Mob, these are no longer the days of chasing Frank Abagnale Jr. for a few forged checks; these are the days of multiple individuals, multiple identities, and multiple channels of business, and crimes that fund international crime, drugs and terror. FSPs have had a head start in managing this challenge, but the number of individuals and methods for committing fraud is growing at an exponential rate, taxing the operational risk missions at even the largest banks.

Accurate identity recognition is the key to preventative measures. FSPs need new tactical systems that allow them to create highly accurate views of individuals, not just across their organizations, but also when individuals are deliberately trying to mask or misrepresent their identities. Investigators must be able to go beyond a single identity, which may appear to be clean, to uncover any links to nefarious individuals, groups or governments.

Strategically, the industry must find more effective ways to fight fraudulent activity cooperatively, including ways to share information resources that do not expose proprietary customer data, but allow organizations to combat their mission at hand, preventing economic crime.

The Roaring 90's and Beyond

Strong economy, M&A, new products & channels converge to create new opportunities for financial criminals

With the convergence of deregulation and technology, FSPs have seen explosive growth over the past several years. The Internet, World Wide Web, and various links to networks, intranets and extranets, have delivered enormous benefits to the financial industry. New online platforms provide the perfect delivery channel for many new products and services, from online banking, trading, and money

transfer, to the large and complex financial networks major banking institutions use to manage accounts and the activities of their clients. These channels enable new levels of flexibility and economy previously unheard of and have given the individual consumer options that would have been impossible only a decade ago.

This transformation has resulted in the migration of new financial service opportunities, from business-to-business offerings to more direct business-to-consumer models. As tens of millions of consumers come online, the giant "money center," banks have made retail banking a strategic imperative. This, combined with investor pressure on smaller banks to compete with the likes of Citigroup and the new JP Morgan Chase, is fueling a new round of merger and acquisition activity[1]

The very same factors that have helped drive the exponential growth and profitability of the financial service industry have also resulted in the rise in fraud and financial crimes.

Teams tasked with managing the operational risk mission of major FSPs are like veterans on the “Eastern Front.” They have been successfully handling their own anti-fraud missions for years and satisfying the standards of the Bank Secrecy Act. Most have built their own “Customer Identification Processes” (CIPs) and have deployed best of breed case management and workflow solutions in their efforts to harden their organizations from attack and fraudulent manipulation. In large part these systems have been more than adequate to address their identification requirements. But increasingly, especially in larger banks, they have found that, no matter how many financial, technological, or human resources have been thrown at the problem, unless the data that fuels this mission is managed in a manner that is resistant to disparity, misrepresentation, and latency, the chances of internal and external threats will increase exponentially.

September 11th and the New Environment

The day Americans changed their perception of financial crimes

In the aftermath of September 11th investigators discovered that much of the money that funded the hijackers was laundered through American banks, using both actual and stolen identities. FSPs suddenly found themselves under intense scrutiny from the federal government, media, and court of public opinion about how the American financial system was used against us. The federal government reacted by passing the bipartisan Patriot Act, which introduced a new regulatory framework designed to protect America’s financial system and provide enhanced checks and balances to identify misuse specifically involving the financing of terrorism and terrorist activities.

[1] Which Bank Will Be Next? J.P. Morgan Deal Adds Urgency As the Big Institutions Scramble To Strengthen Retail Operations By MITCHELL PACELLE and GREGORY ZUCKERMAN Staff Reporters of THE WALL STREET JOURNAL

The new regulations compelled banks to weed through customer records to separate legitimate customers from those with false identities and to work with the federal government on uncovering potential terrorist threats. Specifically, the Patriot Act requires FSPs to:

- Maintain Customer Identification Programs to verify the identity of new customers.
- Check new customers against terrorist watch lists and money laundering.

These measures, in conjunction with the existing Bank Secrecy Act and Office of Foreign Asset Control (OFAC) regulations, were designed to harden America's defenses against fraud, illegal drug activity, and the funding of international terrorism.

Raising the Bar on Operational Risk

New identity requirements and anti-fraud initiatives increase expectations

Moving forward in the post 9/11 environment, FSPs had to re-examine the investigative and technological ability of their systems. No longer could their mission be solely to reduce financial loss from financial crime; their new mission now included the war on terror.

Identity played a large part in the failures that led up to that day, both the in-ability to recognize the falsification of identity and the inability to flag individuals, who were using their real names, which, amazingly, were already on international terror watch lists. New emphasis would have to be put on technologies and processes capable of recognizing an individual using a false or misrepresented identity, and persons using actual names that appear on internal or government watch lists. New systems would have to be based on 360-degree identity data constructed from internal FSP data sources and public and third party enhancement data, then cross-referenced in real time with government watch lists. These systems would be able to flag known criminals using real identities, as well as those using phony ones.

Unfortunately a 360-degree identity isn't enough. Given the conspiratorial and collusive personality of the most dangerous fraudulent activity, banks and FSPs must also be able to recognize a benign identity acting as a front, or "Wolf in Sheep's Clothing," for a nefarious organization bent on criminal activity.

Political Backlash

Consumer advocates and civil libertarians react to new focus on identity

A byproduct of this emphasis on identity requirements has been the ire of consumer advocacy groups and civil libertarians, fearful that the use of technology to establish identity could be used for applications beyond economic crime and homeland security and thus, violate consumer privacy. The pressure

had already been building on FSPs as a result of the Graham Leach Bliley legislation enacted in 2001 that required banks to provide notification to customers when their personal information was to be shared with non-affiliated financial institutions. Compliance required customer record consolidation, as the notification provision of this law could not really be accomplished unless the FSP could establish a complete single identity regardless of inconsistencies or disparate systems.

The Patriot Act and its "Know Your Customer" (KYC) provisions upped the ante on identity, positioning it as the first line of defense against financial criminals and funding of acts of terror. FSPs are now required to share customer level data with the federal government and regularly cross-reference customer lists with federal watch lists. Suddenly FSPs find themselves in an identity tug of war. On one side, they have privacy advocates, ranging from liberal groups to traditional conservative libertarians, united in their view that the use of U.S. persons data in this quest is problematic from a privacy standpoint.

> No use of computer data or technology anywhere at any time for national defense, if there's the slightest possibility that a rogue use of that technology will offend someone's sense of privacy[2]

On the other side are counter terrorism officials within the Federal Government, who believe that some measure of privacy must be sacrificed in the war on terrorism.

Traditional Identity Technology Falls Short

Standard approach focused on direct marketing, not catching bad-guys

FSPs have struggled with creating the 360-degree identities necessary to manage operational risk. Part of the problem is that the technology on which they rely was not built to catch bad guys; rather it was created to increase the effectiveness of direct marketing campaigns or transform data to build data warehouses.

The standard approach to data cleansing and consolidation falls into two categories: Extract Transform & Load (ETL) tools and Customer Data Integration (CDI) processes. Both technologies struggle with the complex identity resolution requirements of an FSP's operational risk missions. FSPs need to know absolutely who their customers are with the highest degree of accuracy. The quality of raw citizen or customer level identity data is usually very low. There is an extreme analytical difference between three individuals each with a single bank account and one individual with three bank accounts. Traditional approaches are usually based on comparing two identity records and using data survivorship rules to create a single "clean" record. But, often the data that

[2] Wall Street Journal - The 'Privacy' Jihad, By HEATHER MAC DONALD, *April 1, 2004; Page A14*

survives is not the most accurate and the information about that identity is compromised.

9/11: Funding a Combination of False and Real Identity

> The 9/11 hijackers opened 35 American bank accounts without legitimate Social Security numbers. The hijackers relied most heavily on 14 accounts at SunTrust Banks, moving upwards of $325,000 through accounts opened in Florida and actually taken out in the names of many of the hijackers whose names also appeared on international terrorist watch lists.
>
> - The hijackers used visas issued through Saudi Arabia or the United Arab Emirates to open bank accounts, with an average amount of $3,000 to $5,000, within 30 days of entering the country.
> - None had a Social Security number, and the addresses they used changed frequently.
> - All of the accounts were basic checking accounts with debit cards, which they used to make a high percentage of withdrawals. Few checks were written. No safe deposit boxes were opened.
> - The hijackers tended to open their accounts in groups of three or four individuals. Some of the accounts were held jointly with other hijackers.
> - Twelve of the hijackers had accounts at the same bank, which wasn't identified. They also opened their accounts at branches of large, well-known banks, which also weren't named.
> - Three of the hijackers opened foreign checking accounts and credit card accounts at banks in the UAE. All bought traveler's checks overseas and brought them to the United States.
> - The accounts were funded mainly by cash and overseas wire transfers from foreign countries, such as the UAE, Saudi Arabia and Germany. [3]

Large FSPs tend to have heterogeneous environments, with multiple platforms and many different types of data sources. This is compounded with each new acquisition. Since most ETL and CDI technologies rely on batch processing and lack a real-time capability, there is a serious problem with degenerative data accuracy between systems refreshes. In environments with a high degree of complexity (more than three-to-five data sources, complex business rules, and a combination of different platforms), most banks have struggled to provide the

[3] "Hijackers used accounts at U.S. banks, debit cards." Jeannine Aversa, Associated Press, Februay 12, 2002.

depth and accuracy of identity data necessary to know who is who, never mind, who knows whom. This certainty of knowing with whom you are doing business is not possible in many of today's homegrown environments.

Knowing Who Is Who through Identity Resolution

Accurate identity is foundation for operational risk

Knowing your customer was much simpler in the brick and mortar days of the banking industry. With only a few products and services available and supplied through human channels, the local bank could identify customers because they actually knew them. Today banks have millions of customers and hundreds of millions of customer records. They have multiple products and services, delivered in virtually every fashion. Applicants can access services from the secrecy of their own living rooms. Individuals are free to misrepresent themselves on online credit or loan applications by simply changing the way they spell their name, or by using a false or stolen identity.

Identity Resolution (IR) techniques address traditional record linking shortfalls of standard ETL and CDI solutions and provide new levels of context about individuals. Rather than employee data survivorship rules, Identity Resolution (IR) maintains the "full attribution" of the data, i.e. no data loss. The so-called bad or un-clean data, the redundant data, and the out-dated data, normally purged with older technology, is maintained and used to create greater accuracy in building identities.

Problems with Traditional Approaches

The vendor pile on: The technology industry moves to exploit hype cycle

The technology industry, still reeling from the evaporation of Y2K revenues and the Dot-com/E-Commerce bust, was all too eager to capitalize on this new opportunity. What followed was a cadence of anti-fraud products, applications, and services. Financial institutions were finding vendors, with whom they had dealt for years in the business intelligence and warehousing business, suddenly claiming they were in the business of compliance and risk management. Predictably, once the hype died down, there was no silver bullet, and the FSPs discovered that the persons and technology most suited to manage this problem lay in their own IT departments. Risk management and fraud prevention is serious business and had been long before the government and public found out its by-products could include funding acts of terrorism. Financial Service Providers lose millions of dollars a year to economic crimes. The IT, investigative, and legal persons whose mission it is to prevent these activities know there is no off the shelf, whole product solution to this problem.

Customer Data Integration (CDI) had always been associated with the marketing departments of large banks and service providers, whose primary use for these technologies was to reduce redundant mailing costs and improve marketing

efficiencies. September 11th took this problem from the mailroom to the board room, as identity became a strategic imperative and the lynchpin to managing operational risk and compliance.

Almost immediately, traditional data quality vendors tried to reposition themselves as purveyors of homeland security solutions. They enlisted retired military officers as lobbyists and board members, and rebranded and repackaged CDI technologies as anti-fraud/anti-terrorist solutions. Offerings came from vendors as diverse as data aggregators, data quality, and hygiene to ETL, and DBMS vendors. The problem is, no matter how you repackage or rebrand a warehouse or direct marketing solution, it cannot solve the unique integration challenges FSPs face in preventing fraud.

Standard CDI/DQ/ETL is sufficient in building a 360° view of an individual based on information directly attributable to that individual. The integration challenges they are designed to correct are:

- Accidental (transposition errors);
- Disparate (incompatible systems applications or data sets);
- Redundant (multiple names and addresses, same person).

Though they claim they are able to facilitate real-time matching, it is more often than not batch or trickle, allowing ample time for bit-rot and latency between each refresh. The matching and cleansing is primarily done using merge/purge processes, whereby the system would employ data survivorship rules to "vote" on which data, name, address, and/or telephone number is most accurate and purge the remainder. Once purged, that data cannot be reclaimed. By their very nature then, these technologies are ill-equipped to seek out deliberate attempts to mask an identity or to adjust in real-time when such an attempt is made, because prior data histories are erased. What happens when a suspected fraudster and an innocent customer share the same first and last name? What happens if your system merges their identity into a single entity and purges valuable intelligence about a criminal in the process? How do you get it back? You can't.

As previously stated, traditional re-packaged CDI marketing solutions are not up to the challenge of managing operational risk, but perhaps worse, the solution providers from this industry are squarely in the crosshairs of consumer privacy advocates. Certain matching technologies they employ are based on the aggregation of huge consumer data banks. They also deploy pattern-based Data Mining technologies and are thus subject to significant privacy challenges and the attendant adverse publicity. This may also raise a strategic dilemma for FSPs: it may well be the case, that after expensive deployment of such solutions, privacy advocates could succeed in persuading Congress that such approaches should be illegal and thus, their use would be prohibited.

Identity Resolution significantly expands the accuracy and scope of the intelligence the system is capable of producing. This approach is self healing and regulating in nature and can facilitate changes to an identity at the moment the data enters the system, to defeat masking attempts as they occur at the system entry point.

Central Identity Resolved Repository
A resolved identity platform to manage the operational risk mission

Most FSPs do not have centralized identity repositories that contain all of the information about their customers. Therefore, they do not know the difference between five people with five accounts and one person with five accounts. This makes it almost impossible to find people who are disguising or misusing their identities to perpetrate a crime.

An enterprise-wide single identity repository would help solve all identity recognition needs, such as validating who people are and determining patterns of activity to prevent an organization from having to catch the same individuals twice. Tied to national and international security, federal watch lists, and external data sources, the system could also contain information about accounts that were closed for cause or were under investigation or had queries against them. The self correcting, self healing capabilities of Identity Resolution would insure that the accuracy of the identities that populate the repository would be updated or refreshed in real time, as additional conjoining or disjoining data entered the system, so that investigators would not have to be concerned with data latency between refreshes.

A central repository would also be able to detect “bust outs,” whereby someone establishes good credit with a credit card, then obtains access to more and more credit, with the intention of taking out as much cash as possible and then declaring bankruptcy.

Who Knows Who
Gauging Risk by Association

More daunting than the lone individual engaged in fraudulent activity are financial crimes committed by groups of people conspiring together. This high-risk activity, which results in the most damaging instances of financial crimes, is extremely difficult to detect. Traditional CIPs, which were designed to verify the identity of a single person, do not go far enough. Unless an individual turns up on an internal or government watch list, they will pass into the system unchecked. What if that same person shares an address with a known money launderer or an individual on a banned customer list? What if they have also made three trips to Bogotá, Columbia in the past year and have received four wire transfers from anonymous individuals in a pooled account? What if they are the front to an international money laundering operation selected because their background would raise no

flags? How would traditional systems and processes detect them? Most often, it is the people lurking in the background, behind the account, that present the largest threat. These individuals are also the most difficult to recognize.

This same truth applies to the bank employees and contractors with permissions granting them access to sensitive data stores and the commercial networks which FSPs use to manage the accounts of their clients.

FSPs would benefit greatly from a system that would allow them to determine who knows who by identifying obvious and non-obvious relationships between individuals. The system should combine the highly accurate Identity Resolved internal data about individuals, with aggregated publicly available data sources or other collections of external data, watch lists, OFAC, etc, to establish links between a subject and a suspect, location, or other piece of applicable information, be it other individuals, locations or things. With this system, FSPs would be able to uncover and connect the dots between individual identities and external relationships, and gauge the risk by association of each individual.

September 11th Conspiracy Map

> **Direct Links—Watch List Information**
> **Khalid Almihdhar** and **Nawaf Alhazmi**, both hijackers of American Airlines (AA) Flight 77, which crashed into the Pentagon, appeared on a U.S. government terrorist watch list. Both used their real names to reserve their flights.
>
> **Ahmed Alghamdi**, who hijacked United Airlines (UA) Flight 175, which crashed into the World Trade Center South Tower, was on an Immigration and Naturalization Service (INS) watch list for illegal or expired visas. He used his real name to reserve his flight.
>
> **Link Analysis—One Degree of Separation**
> Two other hijackers used the same contact address for their flight reservations that Khalid Almihdhar listed on his reservation. These were **Mohamed Atta**, who hijacked AA Flight 11, which crashed into the World Trade Center North Tower, and **Marwan Al Shehhi**, who hijacked UA Flight 175.
>
> **Salem Alhazmi**, who hijacked AA Flight 77, used the same contact address on his reservation as Nawaf Alhazmi. The frequent flyer number that Khalid Almihdhar used to make his reservation was also used by hijacker **Majed Moqed** to make his reservation on AA Flight 77.
>
> **Hamza Alghamdi**, who hijacked UA Flight 175, used the same contact address on his reservation as Ahmed Alghamdi used on

his. **Hani Hanjour**, who hijacked AA Flight 77, lived with both Nawaf Alhazmi and Khalid Almihdhar, a fact that searches of public records could have revealed.

Link Analysis—Two Degrees of Separation
Mohamed Atta, already tied to Khalid Almihdhar, used a telephone number as a contact number for his reservation that was also used as a contact number by **Waleed Alshehri**, **Wail Alshehri**, and **Abdulaziz Alomari**, all from AA Flight 11, and by **Fayez Ahmed** and **Mohand Alshehri**, both from UA Flight 175.

Public records show that Hamza Alghamdi lived with **Saeed Alghamdi**, **Ahmed Al Haznawi**, and **Ahmed Alnami**, all hijackers of UA Flight 93, which crashed in Pennsylvania. Link Analysis—Three Degrees of Separation[4]

Data Sharing Across Organizations

Employing technologies to anonymize data for secure sharing

Data sharing is a sticky issue for FSPs. The emergence of the Patriot Act and its "Know Your Customer" provisions raised the bar on identity, positioning it as the first line of defense against financial criminals and funding of acts of terror. FSPs are now required to share customer level data with the federal government and regularly cross-reference customer lists with federal watch lists. The challenge lies not so much in the act of sharing the data with the government, but in how to reduce corporate exposure to privacy violations that can occur through this sharing. Beyond this, the industry is also searching for ways to safely facilitate data sharing among multiple organizations for due diligence and anti-fraud missions, that does not expose critical customer characteristics to competitors.

A new technology is emerging to address these concerns. It will allow data to be converted into an anonymous form so that it can be shared with other organizations without compromising security or privacy. This selective revelation capability creates a secure barrier between private data and the investigator and provides a control mechanism regarding what data can and cannot cross that barrier to the analyst.[5] Anonymous data sharing promises not only to reduce the privacy concerns with corporate and federal data sharing missions, but to increase the ability of organizations to share data to reduce fraud and other operational risk factors.

Identity Resolution using anonymized data will allow for more secure data sharing and cross referencing prior to a major acquisition. Combined, it will enable the acquiring FSP to conduct customer verification on high-risk customers

[4] "Data Mining and Data Analysis for Counterterrorism." By Mary DeRosa. CSIS. March 2004.
[5] ISAT Security With Privacy/13 DEC 02

of the "to be acquired bank," while only having access to the data pertinent to the due diligence mission.

J.P. Morgan Chase was recently in the news for violating the Know Your Customer rules of the Patriot Act as a result of their association with Beacon Hill, an unlicensed money transmitter. On the outset this would seem like a KYC issue, but, in fact, Beacon Hill was a client J.P. Morgan had acquired from its acquisition of Chase Manhattan Bank, which had inherited Beacon Hill from its merger with Chemical Bank. Banks would take heed to recognize M&A's need to not only be driven by customer acquisition and market expansion, but by the exposure they may be subjecting themselves to from nefarious customers whom they also acquire in a merger.

Deploying Identity Resolution, NORA and Anonymous Data Sharing to Fight Financial Crimes

A centralized identity platform that combines Identity Resolution with NORA (Non-Obvious Relationship Awareness) and anonymous data sharing provides huge benefits to FSPs in reducing their operational risk, by decreasing operating losses and enhancing due diligence for security and privacy compliance. Below are several examples of how these technologies could be used to benefit FSPs in their efforts to reduce credit card fraud, money laundering, collusion and other illegal activities, and to increase compliance.

Credit Card Fraud

42 percent of all id theft is credit card fraud.

Last year in the United States alone,161,819 cases of identity theft occurred, with losses of more than $343 million. Of that, 42 percent was credit card fraud. The major areas of credit card fraud include account takeover and fraudulent applications[6]. Once a criminal has obtained the target's personal information, he or she will contact the credit provider, posing as the unsuspecting customer, and request a change of address form. Then, additional charge cards and new PIN numbers will be requested to facilitate cash withdrawals. Fraudsters may also use information such as a valid name, date of birth and SSN to open new accounts using their own P.O. Box as an address. Identity Resolution and NORA, applied to this type of financial crime, would allow FSPs to significantly harden their internal command and control mechanisms.

Identity Resolution can be performed using internal data sources such as customer service, direct marketing, and internal banned customer lists with industry, law enforcement and federal watch lists to conduct full identity verification when, for example, a customer tries to change an account address

[6] Credit Card Industry and Identity Fraud, John Schettino, VP Security and Risk Management, MasterCard International, October 28 2003 ECI Conference

over the phone. NORA could also be used on the new address to determine if it has any associations with nefarious third parties.

Know Your Customer

Illegal money laundering accounts for $600 billion to $1.8 trillion of the world's annual economic activity.[7]

The Bank Secrecy Act was enacted by Congress to combat money laundering and make it a federal crime. KYC processes are supposed to uncover illegal money transfers (money laundering) before they become a problem. FSPs must determine the source of customer deposits, i.e. the identity of the customer, classify them according to established “profiles," and monitor account activity that may raise suspicion. The problem they face is establishing a consolidated identity on which to base that monitoring. If they are monitoring what they believe to be three separate individuals, when in fact it is just one, their analysis will be false. FSPs that have struggled with recognition problems and reducing the operational risks associated with money laundering are now subject to penalties under the Patriot Act of no less than twice the dollar amount of a money laundering transaction, up to one million dollars for each violation.

The use of a central repository of resolved identity data, combined with sources such as banned customer lists, Regulatory Data Corporation (RDC) data, federal watch lists (OFAC and the Politically Exposed Person list), as well as other external data sources, would allow FSPs to screen new accounts in real time, as they touch the system to determine their true identities. This same repository could also employ link analysis to determine relationships among the new applicants, whose individual data may pass muster, but whose associations may well signify potential trouble.

The FSP industry could use anonymized data that would selectively reveal only identifiers critical to the anti-money laundering mission, to construct a real-time cross bank repository of combined customer data, that could be analyzed for patterns suspicious to criminal activity and cross referenced in the KYC process. Because the data would be anonymized, the FSP would not have to be concerned with revealing sensitive information or violating individual privacy.

Know Your Employee

Almost half of all fraudulent activity involves collusion between insiders and outsiders.

Collusive relationships between employees and third parties in 2003 accounted for more than 48 percent of all fraudulent activities. It is critical for FSPs to vet applicants for sensitive insider positions before they become employees, and

[7] U.S. agents investigate money trail / Financial profiles of hijackers used to find funding sources / By Brian Tumulty / *Gannett News Service*

mitigate insider threats by periodically screening existing personnel who have access to sensitive personal data such as customer SSNs, addresses and account numbers. In 1994, one of America's largest banks had an incident of employee collusion that involved a third party with a laptop computer, who broke through the bank's firewall in the cash management system and transferred $12 million dollars to an outside account. Despite the bank's denials, fraud experts concluded that the only way the perpetrators could have received the codes was from someone on the inside[8].

Identity Resolution can be used to resolve the multiple data sets a potential employee would be screened against in the hiring process, including academic records, credit history, criminal records, internal banned customer records, and international, federal, and state watch lists, to verify the applicant's identity and background, despite attempts to misrepresent their identity information. Link analysis could then be utilized to determine if a potential employee shares an address with a known financial criminal or if an existing employee shares a post office box with an organized crime boss.

Watch List Consolidation
Industry wide anonymous data sharing to find bad guys

The banking and finance industry could develop an "excluded customers" watch list with names of individuals who are on internal bad guy lists for questionable or illegal activities. NORA could be used to search through massive databases to find associations between, for example, a person seeking a job at a brokerage house and a person on a federal watch list. Perhaps the applicant once roomed with, sold a house to, or used as an employment reference, a person who is on a watch list. This information could be used by the financial services industry to focus its investigatory resources

Compliance
Meeting the demands of national security and privacy

Deferring operational risk and reducing loss is at the heart of anti-fraud activities at most major banks. However, FSPs are also required to comply with anti-money laundering regulations. Identity is the key to compliance. Before a bank can comply with the KYC provisions of the Patriot Act or Bank Secrecy Act, they must first be able to consolidate their proprietary customer information into an accurate, comprehensive view, across the multiple representations, disparate systems, and poor quality of raw identity data.

Identity Resolution provides a powerful identity platform on which to manage compliance issues including homeland security, bank secrecy and consumer privacy. Once identities are resolved, they continue to be updated with each new piece of identity data that enters the system. The new data can enhance an

[8] Forget cops and robbers: it's age of the inside job/American Banker ▪ Friday, May 23, 1997/By Sarah Yavorsky

existing identity, challenge a previous identity resolution, and/or create a new identity. Since Identity Resolution occurs in real time, there is no chance for data latency between refreshes and no window for false or contradicting identities to pass into the system unchecked. Banks can build a central repository with internal resolved customer identities and combine them with industry, federal and state watch list data. The information can then be used as a tool to verify new and existing customer identities at the point of contact.

NORA extends customer knowledge by enabling investigators to see beyond the client, to with whom that client may be doing business or sharing a residence. Customer associations, depending on their characteristics, can signify deeper problems that may jeopardize compliance efforts.

Anonymized customer lists can be cross referenced with the OFAC, or the Politically Exposed Person lists. The selective revelation capabilities will protect customer privacy while fulfilling the compliance requirements of the federal government.

Conclusion

There is no silver bullet in sight to ending economic crime. FSPs must concentrate on leveraging new identification technologies to sniff out threatening individuals and organizations, while reducing exposure to privacy violations. Investigators must leave the old notion of what constitutes a 360-degree identity behind and embrace the next generation of identity resolution technology that extends beyond 360°. In doing so FSPs will extend the recognition capabilities of anti-fraud solutions to:

- See through an individual attempt to mask identity;
- Link a seemingly benign single customer to a nefarious individual, organization, or foreign government;
- Share and cross reference customer data stores protecting personal data and revealing only information critical to the mission.

In raising identity recognition to this level, FSPs will find themselves well armed to confront and manage the booming fraud industry.

About the Author

John Slitz is chief executive officer of SRD Software. SRD Software provides identity recognition software to financial services companies and other commercial and government customers needing customer and citizen insight that goes beyond the traditional 360-degree view. SRD's solutions are based on its proprietary Identity Resolution technology, which is the result of 20 years of research and development and extends insight beyond existing identity

integration technologies by incorporating non-obvious relationships and anonymous data sharing.