Risk Intelligence Solutions (RIS) in the social sector
September 2007

IBM **Information Management** software

Reducing improper payments in social services and social security

How IBM's Risk Intelligence Solutions improve eligibility decisions by identifying fraud, abuse and error before payments are made.

by Bryan Chong
David Dyda

Contents

2 Summary
2 Key message
3 Introduction
3 How are problems of identity and eligibility managed today?
4 Example scenarios
7 Data matching techniques and requirements
11 Introduction to the RIS solution
18 Scenarios revisited with RIS
25 Conclusions
27 For more information

Summary

This whitepaper presents IBM's Risk Intelligence Solutions (RIS) for social sector organizations to solve five problems that contribute to improper benefit payments:

- *Verify applicant identity upon intake or registration.*
- *Determine if the applicant is applying for the same benefit in more than one jurisdiction.*
- *Determine if the applicant is applying for multiple benefits across several programs whether in the same jurisdiction or across jurisdictions.*
- *Uncover hidden relationships between the applicants and other benefit recipients that if known would negate or reduce benefits eligibility.*
- *Compare applicant eligibility information across programs and jurisdictions anonymously in order to comply with privacy legislation.*

The solution presents an active, preventive approach to fraud, abuse and error detection, capable of integration with case management applications so that the right eligibility decisions are made prior to extending benefits. This is in contrast with traditional passive detection methods that look for improper payments after benefits have already been paid.

Key message

Worldwide, more than $4 trillion is expended annually for social services and social security benefits. The majority of benefits go to those deserving and to those who have contributed and are entitled. But not everyone in receipt of benefits presents true information upon application whether due to deception or to error. Not everyone is who he says he is. Not everyone discloses all sources of income, benefits, assets, accommodation or situations where related persons are receiving benefits. When the intent to deceive is successful, or when application errors go undetected, program dollars are

paid to the wrong people. This results in fewer benefits for those deserving, and the need for increased program budgets to compensate for improper payments. More effective tools are needed to prevent fraud, abuse and error.

Introduction

In this whitepaper, we start with traditional approaches social services and social security organizations use to verify identities, multiple applications for the same benefit, and applications for multiple benefits across jurisdictions. We then present seven scenarios to show how various forms of improper benefit payments can occur. This is followed by an introduction to IBM's RIS solution and its capabilities. We revisit each of the scenarios using RIS to demonstrate how the tool successfully addresses each of the issues social sector organizations typically face today with regard to fraud, abuse and error.

How are problems of identity and eligibility managed today?

Social services and social security organizations are confronted with significant amounts of ambiguous data regarding the identity of their clients, applicants and providers. This ambiguous data may be due to deliberate attempts by clients and/or providers to obtain payments or it simply may be unintentional error. The core of these social services systems is the citizen database repository which contains information such as name, address, telephone number, social security number, birth date, place of birth, marital status, mother's maiden name, and so forth. Identity is further complicated by multiple databases residing in other departments which maintain different versions of the data about a client or provider. Separate data bases may exist for specific programs such as pensions, disability, child allowance and employment insurance. These different databases are often not integrated, resulting in siloed, inflexible systems.

Under these arrangements, citizens provide the same information each time they apply for a different benefit. These inflexible systems do not share data between silos, are administratively inefficient, and do not have consistent, up-to-date data between silos. For example, when a citizen passes away, regional governments provide death data to the national government to update the identity repository where it is then shared with other benefit programs. Due to stand alone systems, inadequate data matching routines and privacy legislation, this update is prone to error and is a major cause of data integrity problems.

Social services and social security organizations share little data externally with other agencies, jurisdictions or third parties. For example, national government agencies such as, Education Savings Grants, Student Financial Assistance, Student Loans, Housing, Veterans Affairs; and non-government organizations such as Financial Institutions and Credit Reporting agencies, all utilize identity data. However, the sharing of data with other government and non-government organizations for service delivery integration and to prevent improper payments is minimal. The challenge is that sharing citizen information requires protection of data security and privacy. This is an issue today and will continue to be one in the coming years. In addition, most social sector fraud, abuse and error solutions rely heavily on after-the-fact detection rather than prevention or active detection before benefit payments are made.

Example scenarios

Here are seven fraud and error scenarios that a case worker may encounter.

Social service scenario #1:

James D. Thomas has been a receiving social assistance for 6 months. He decides to apply for housing benefits without disclosing that he is receiving social assistance. He makes sure neither agency finds out by applying with the name Jim Tomas, and provides a slightly different address and birth date (fraudsters often do this so that if caught, they can blame the anomaly on clerical error). As a result, James while receiving social assistance is now also receiving housing benefits.

Social service scenario #2:

Eric Vincent has turned 65 and is retiring. He is eligible for Supplemental Security Income. Eric's wife Janice Jones, (she use her maiden name), has been receiving Supplemental Security Income benefits for the last 12 months. Based on their relationship, Eric's eligibility for these benefits will be reduced. He does not disclose his relationship, and both Eric and his spouse are receiving full Supplemental Security income benefits.

Social service scenario #3:

Mark Hughes and his long time friend Dr. Michael O'Donnell share the same apartment. They have developed a scheme to defraud the state Medicaid program. Dr. O'Connell plans to over prescribe high valued prescription drugs to Mark. Mark would re-sell the drugs and split the proceeds with Dr. O'Connell. In addition, the two will share the reimbursement paid by the Medicaid program for Mark's medical visits.

Social service scenario #4:

Daniel Stack relocates from Florida to Pennsylvania but cannot find employment. He applies for income assistance benefits and is deemed eligible. However, he has not disclosed that he is the owner of a vacation home, a 2005 Honda Accord and a Ski-Doo watercraft, all of which are registered in Florida.

Social service scenario #5:

Susan Gance has been collecting unemployment benefits for 3 months. During her commute to an interview, Susan has an automobile accident sustaining serious injuries to her head and neck. Her doctor estimates that it will take 12 months to recover before she can work again. Susan moves back into her parent's home and applies for and receives disability benefits using her parents' address.

Social service scenario #6:

Matt Berry receives Medicaid from the state of Arizona. He is also applying for Medicaid in the state of Florida. He has applied for these benefits under the address of his recently acquired winter vacation home. Due to privacy legislation, data sharing between jurisdictions is not permitted. Matt is eligible and is now receiving Medicaid in both states.

Social service scenario #7:

Jonathan Miller, also known as Jack Miller, has passed away at 89. Jonathan's wife, Helen, notifies the regional government of his death. The regional government subsequently sends a notice to the national government. The notice does not update the system properly because Jonathan is registered for pension benefits under the nickname Jack, and no other identifier information has been provided. As a result, the national government continues to provide pension benefits to Jack which Helen continues to access via the joint account held with her late husband.

Problems in each of the scenarios

These problems are difficult to detect because identity and relationship data are stored across several systems that do not share data. Matching is further hampered by poor data quality. Data from operational systems is often fraught with typographical errors and variations in name and other identifier information such as address (James versus Jim and 111 West Tenth Ave. versus 111 10th Avenue W.) Current intake, registration and case management processes are a main cause of data problems. They are not designed to manage data integrity. Data becomes out-of-sync, incomplete and inaccurate in the organization's business applications. The result can be errors in the citizen data base repositories approaching 40%.

As well, there will be those who intentionally misspell their name to prevent data matching. Dates can be a problem too. The year, month and day format is often applied inconsistently. Social security numbers are lengthy numbers and the digits are often transposed. Numbers may be entered inconsistently, sometimes with leading zeros and other times not.

Data matching techniques and requirements

Naïve identity matching

Organizations typically employ three types of identity matching:

- *Merge/purge and match/merge. Direct marketing organizations developed these systems to eliminate duplicate customer records in mailing lists. These systems operate on data in batches; when organizations need a new de-duplicated list, they run the process again from scratch.*
- *"Binary" matching engines. This system tests an identity in one data set for its presence in a second data set. These matching engines are used to compare one identity with another single identity (versus a list of possibilities), with the output often expected to be a confidence value pertaining to the likelihood that the two identity records are the same. These systems help organizations recognize individuals with whom they had previously done business (the recognition becomes apparent during certain transactions, like checking into the hotel) or, alternatively, recognize that the identity under evaluation is known as a subject of interest—that is, on a watch list—thus warranting special handling. This identity matching system can be batch handled or real time, although real time is preferred.*
- *Centralized identity catalogues. These systems collect identity data from disparate and heterogeneous data sources and assemble it into unique identities, while retaining pointers to the original data source and record in order to create an index. Such systems help users locate enterprise content in the same way the library's card catalog helps people locate books.*

There are two approaches to record matching: 1) probabilistic and 2) deterministic. The identity matching systems use either probabilistic or deterministic matching algorithms. The probabilistic approach matches records by leveraging statistical properties of the data set while the deterministic approach generates a key (based on a rule) for each record, and matches all records associated with the same key.

Probabilistic techniques rely on training data sets to compute attribute distribution and frequency. For Example, Mark is a common first name but Rody is rare. These statistics are stored and used to determine confidence levels in record matching. As a result, any record containing the name Rody Smith and a residence in Maine may be considered the same person with a high degree of probability whereas, Mark Smith, which is more common, would not have a high degree of probability. These systems lose accuracy when the underlying data statistics deviate from the original training set. To remedy this situation, such systems must be retrained from time to time and the data reprocessed.

Deterministic techniques rely on pre-coded expert rules to define when records should be matched. One rule might be that if the names are close (Robert versus Rob) and the social security numbers are the same, the system will consider the records as the same identity. These systems fail—sometimes spectacularly—especially when the rules are no longer appropriate for the data collected. Both the probabilistic and the deterministic approaches have pros and cons. According to Gartner analysts, the best data matching software is a hybrid, combining probabilistic and deterministic approaches.

Mixture of vital requirements

Given the analysis of the potential problem scenarios and existing data matching techniques, it is clear that a successful solution requires a mixture of several vital characteristics. Chief among these is a non-obvious relationship awareness capability for resolving ambiguous identities. It has to be built on a model of identities and relationships between identities (such as shared addresses or phone numbers or other attributes) in real time. If a new identity matched or related to another identity in a manner that warrants human security the system immediately generates an intelligent alert.

- *Sequence neutrality. It needs to react to new data as that data is loaded. Matches and non-matches must be automatically re-evaluated to see if they are still probable as the new data is loaded. This capability is needed to eliminate the necessity of database reloads. (See* http://jeffjonas.typepad.com/jeff_jonas/ 2006/01/sequence_neutra.html *for more on sequence neutrality).*
- *Relationship aware. Relationship awareness is designed into the Identity Resolution process so that newly discovered relationships can generate real-time intelligence. Discovered relationships also persist in the database, which is essential to generate alerts beyond one degree of separation.*
- *Perpetual analytics. When the system discovers something of relevance during the identity matching process, it publishes an alert in real time to secondary systems or users before the opportunity to act is lost.*
- *Full attribution. Identity Resolution algorithms evaluate incoming records against fully constructed identities, which are made up of the accumulated attributes of all prior records. This technique enables new records to match to known identities completely, rather than relying on binary matching that can only match records in pairs. Full attribution improves accuracy and greatly improves the handling of low-fidelity data that might otherwise have been left as a large collection of unmatched orphan records.*

- *Extensible. The system needs to accept new internal/external data sources and new attributes through the modification of configuration files, without requiring that the system be taken offline.*
- *Knowledge-based name evaluations. The system needs detailed name evaluation algorithms for high-accuracy name matching. Ideally, the algorithms would be based on actual names taken from all over the world and developed into statistical models to determine how, and how often each name occurs in its variant form. This empirical approach requires that the system determine automatically the culture that the name most likely came from because names vary in predictable ways depending on their origin.*
- *Real time. The system has to handle additions, changes, and deletions from real-time operational business systems. Processing times are so fast that matching results and accompanying intelligence (such as persons on a watch list or a missing address on an apartment number based on prior observations) could be returned to the operational systems in sub-seconds.*
- *Complex event processing. The system has to support actions triggered not by a single event, but by a complex composition of events, happening at different times, and within different contexts.*
- *Scalable. The system has to be able to process records on a standard transaction server, adding information to a repository that holds tens of millions of identities.*

Introduction to the RIS solution

All of the above capabilities are provided in RIS. IBM's RIS is a suite of technologies that eliminate the ambiguity of provider and/or recipient identities. RIS disambiguates identities by examining the anomalies and inconsistencies in the data as well as in the network of both obvious and non-obvious relationships hidden in databases. RIS sifts through entity identification information such as name, address, phone number and so on that resides in separate databases to dynamically correlate identities. RIS also scrambles and encrypts identity information to create and to serve as a unique identifier to protect the privacy of individuals during information sharing between organizations.

RIS includes four Entity Analytics (EAS) components; 1) Identity Resolution, 2) Relationship Resolution, 3) Anonymous Resolution, 4) Global Name Recognition

- *IBM Identity Resolution is a technology which enables organizations to answer the question "Who is who?" Identity Resolution is able to distinguish whether multiple records are, in fact, records for a single resolved identity.*
- *IBM Relationship Resolution builds off resolved identities created by Identity Resolution. Relationship awareness provides answers to the question "Who knows who?" by seeking out non-obvious relationships between individuals and with organizations.*
- *IBM Anonymous Resolution allows several organizations to share and compare data in order to discover "Who is who and who knows who … anonymously?" Anonymous Resolution converts confidential information into cryptographic form enabling data owners to maintain control of what information is revealed and concealed.*
- *IBM Global Name Recognition provides advanced name matching analysis. Not only does it provide the ability to do automated name processing with English sounding names but it has advanced multi-cultural name recognition products for international governments and commercial clients worldwide.*

Figures 1-6 show how social services client records are ingested and compared to establish if these are the same or different clients applying for benefits.

In 2002 your system observes record **A**.

```
Source A-701 (2002)
Marc R Smith
123 Main St.
(713) 730 5769
DL:0001122107
```

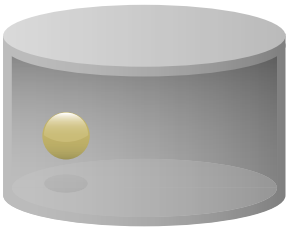

Figure 1. The identity is determined to be new.

In 2003 your system observes record **B**.

```
Source A-701 (2002)
Marc R Smith
123 Main St.
(713) 730 5769
DL:0001122107
```

```
Source B-9103 (2003)
Randel Smith
DOB: 06/17/1974
(713) 731 5577
```

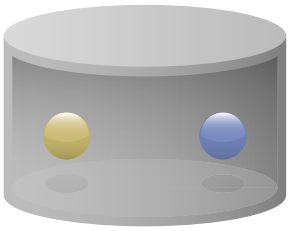

Figure 2. The identity is again determined to be new.

In 2004 your system observes record **C**.

```
Source A-701 (2002)
Marc R Smith
123 Main St.
(713) 730 5769
DL:0001122107
```

```
Source B-9103 (2003)
Randel Smith
DOB: 06/17/1974
(713) 731 5577
```

```
Source C-6251 (2004)
Mark Randy Smith
456 First Street
(713) 731 5577
DL: 1122107
```

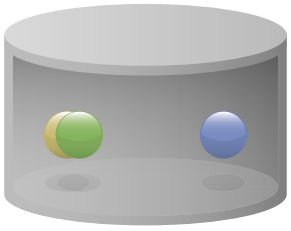

Figure 3. The identity is determined to be known.

Instantly your system recognizes **A** is **B** is **C**.

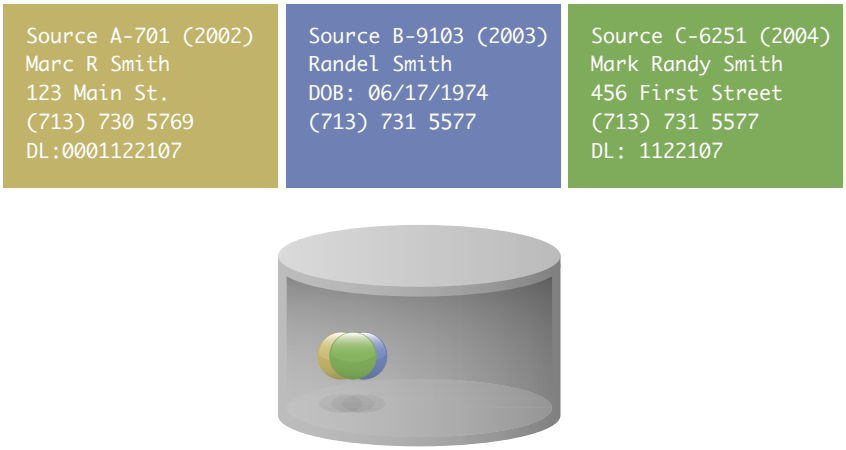

Figure 4. Sequence neutrality rules cause the two identites to collapse.

In 2005 your system discovers record **D**.

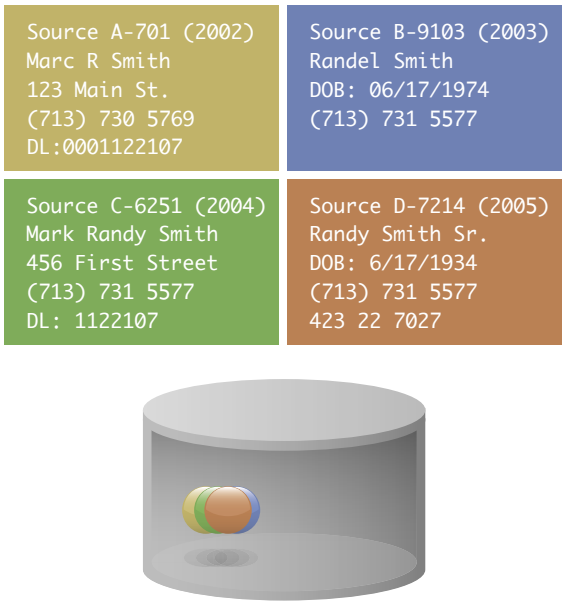

Figure 5. The identity is determined to be known.

Instantly your system recognizes **A** is **C** and **B** is **D**.

Junior

Source A-701 (2002) Marc R Smith 123 Main St. (713) 730 5769 DL:0001122107	Source B-9103 (2003) Randel Smith DOB: 06/17/1974 (713) 731 5577

Senior

Source C-6251 (2004) Mark Randy Smith 456 First Street (713) 731 5577 DL: 1122107	Source D-7214 (2005) Randy Smith Sr. DOB: 6/17/1934 (713) 731 5577 423 22 7027

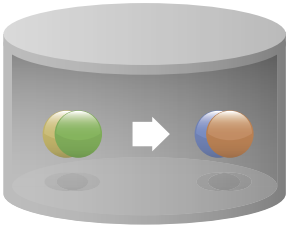

Figure 6. Sequence neutrality rules cause the identity to split.

Figure 7 shows how the data about a client accumulates for a complete and continuously updated view. With this view you see all versions of the truth about the client's identity across time.

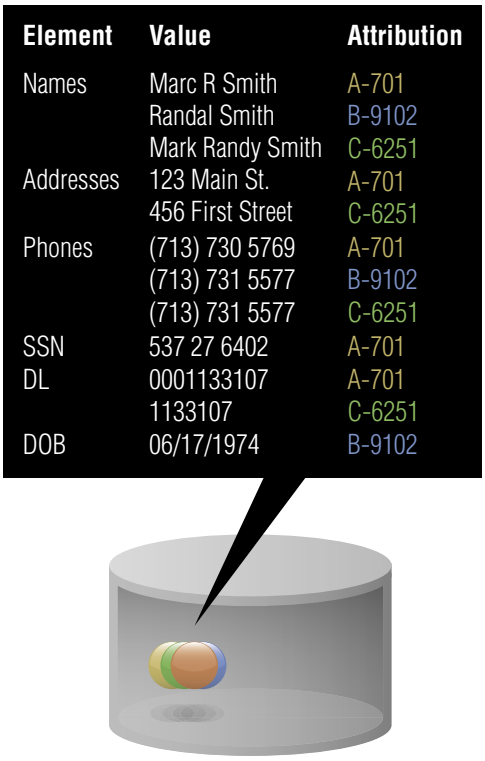

Figure 7. Behind the scenes, context is accumulating.

Figure 8 shows that data about the clients can be ingested from both internal and external sources for a more comprehensive and accurate view about them. The data about the client is compared across all personally identifiable attributes.

Figure 8. Resolve recipient identity, relationship(s) across many different personal identity attributes

Figure 9 shows that the result of the comparisons presented in figures 1-8 can be continously accumulated and updated. It can be a shared service identity repository usable by all organizations, programs for more efficient and effective government.

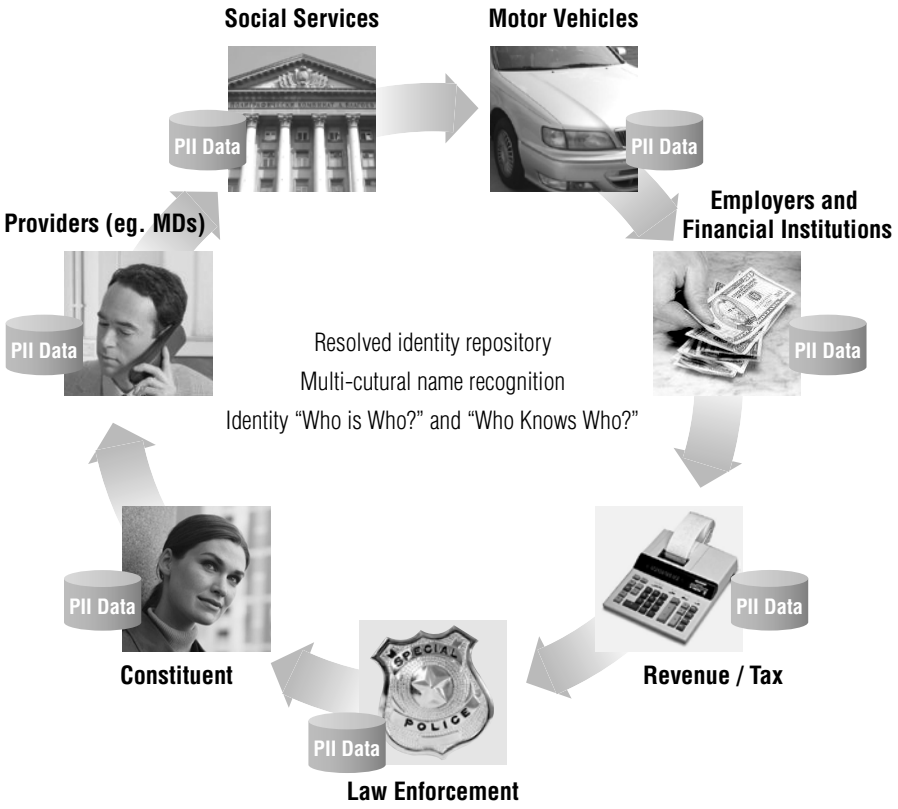

Figure 9. Create a shared constituent identity repository for an enterprise wide strategy

Scenarios revisited with RIS

Identity Resolution

IBM Identity Resolution helps social services and social security organizations solve their business problems related to recognizing the true identities of their clients and providers.

- *It turns inconsistent, ambiguous identity and attribute data into a single resolved entity across multiple data sets, even despite deliberate attempts at misrepresentation*
- *Solves the problem of recognizing "who is who?" and updates and manages client, provider identities as they evolve to meet the real- time demands of social services eligibility determination and case management*
- *Determines whether multiple client or provider identity records seem to describe different identities, even with name variations, are actually for a single resolved client or provider identity*
- *Integrates such multiple client or provider records into a single entity in a comprehensive, unified view and assigns a unique identifier called a persistent key*
- *Maintains the data's original attributes, such as information from prior client records or provider records -- even identifies the source systems that provided the original data*
- *Meets privacy regulations by offering opt-out, notification, access and security*
- *Detects and prevents fraud by recognizing multiple client and provider identities and cases, and strengthens anti-fraud efforts through identity-based verification*

Social Service Scenario #1 Revisited:

James D. Thomas first applied for social assistance in January 2006. On the application, James entered his full name, his address at 111 Bow Street, and his birth date 02/08/1942. The persistent Identity Resolution system evaluates James' personal information the instant the application is entered and determines him to be eligible for social assistance. Six months later, James decides that he is going to attempt to defraud the system. In June 2006, James submits another application. On this application, James intentionally enters incorrect or malformed data. He enters his name as Jim Tomas, his address as 111 Bowe St. and his birth date as 2/8/42. With more primitive applications, scenarios such as this are difficult to identify but with the capabilities of Identity Resolution, they can be resolved quickly and accurately.

In this case, the Identity Resolution component of the system receives James' second application, evaluates it, and this time returns an intelligence alert. What James did not know is that the Identity Resolution system can recognize that Jim is a variation of James and that Tomas may be a typographical error or a cultural name variation. The same applies for the variation in address, 111 Bow Street versus 111 Bowe St. Furthermore, Identity Resolution also recognizes dates with transposition errors: 02/08/1942 versus 2/8/42. The subsequent intelligence alert would prompt caseworker/management scrutiny and a follow up with James' file.

Relationship Resolution

IBM Relationship Resolution provides a new level of identity awareness for social services and social security organizations. This technology solution finds out "who knows who" to determine the potential value or risk associated with relationships among clients, providers and other external forces.

- *Built on the IBM-proprietary Entity Resolution™ process to maximize the accuracy of baseline identities before relationship analysis is performed*
- *Cross-references data from multiple formats in internal siloed social services systems and external publicly available sources to determine non-obvious relationships*
- *Designed to flag suspect relationships, even those hidden or disguised, and send real-time alerts based on a user-defined rules engine to case and risk management applications*
- *Enables a social services organization to look beyond the bounds of data directly attributable to an individual client or provider to see their "network value" or "network risk"*
- *Used for detection and prevention of fraud and abuse to enable social services organizations to better recognize and prevent improper payments*

Social service scenario #2 revisited:

This scenario is a classic example where Relationship Resolution would play a direct role in determining the eligibility of a social assistance applicant.

Eric Vincent has decided to apply for Supplemental Security Income (SSI). Janice Jones, Eric's wife, (she kept her maiden name at marriage), has been a SSI recipient for the past 12 months. During the application process, Eric, in error, fails to indicate that his wife is a current SSI recipient. Although this particular case is not fraudulent, the fact that Janice is currently receiving SSI benefits can potentially reduce or negate Eric's eligibility. In this situation, the underlying relationship between Eric and his wife may elude the Supplemental Security Income program due to the difference in last names.

As a component of the identity matching algorithm, Relationship resolution will recognize the situation and generate an intelligence alert regarding the marital status between Eric and Janice. Subsequently, Eric's eligibility for Supplemental Security Income will be correctly and fully evaluated based on the recently acquired information.

Social service scenario #3 revisited:

This scenario is a more unusual case where Relationship Resolution would prevent continued fraudulent activity. This scenario involves Mark and his roommate, Dr. O'Connell. The long time friends have developed a scheme to deceive the Medicaid health program. The plan is for Dr. O'Connell to over prescribe medications for Mark. Mark would then sell the medications and share the proceeds with Dr. O'Connell. As well, the two plan to share the reimbursements paid by the Medicaid program for Mark's excessive medical visits.

Mark and Dr. O'Connell's plan is simple but would be difficult to detect. Relationship Resolution plays a huge role in uncovering their arrangement. This scenario can play out in two ways. Assume that the Medicaid program has become suspicious due to increases in the frequency of Mark's medical visits and the amount of medications prescribed. Due to patient privacy legislation, the Medicaid program is unable to determine whether the increased visits and medication are a result of a legitimate worsening illness. If their investigation is supported by Relationship Resolution, the system will be able to detect the relationship between Mark and his physician Dr. O'Connell. The newly acquired information has informed Medicaid that the two shared the same residence. This information has just created a solid lead for the Medicaid program to pursue and potentially build a case that may have otherwise remained undetected.

Anonymous Resolution

The third component of RIS is Anonymous Resolution. In the technology age where personal information is readily collected and shared, governments and private sector organizations have encountered increasing pressure to protect citizen privacy. For instance, following the events of 9/11, individuals and groups have became more vocal regarding how their rights have been infringed upon due to new, more invasive surveillance methods. As a result, data sharing has become a challenging and sensitive subject. Other current challenges of note include the fact that relatively few data owners in their silos really want to share their data and public sector organizations do not want to expose their "subjects of interest."

In an effort to address these concerns, Anonymous Resolution was developed. Anonymous Resolution allows multiple data holders to share anonymized identity-based data whereby all identities are managed and correlated while in their cryptographic form. This allows for a more secure method of resolving identities and detecting clients, providers and other subjects of interest while still preserving the privacy of the data.

Social service scenario #4 revisited:

Daniel is an unemployed resident from Florida. He is applying for income assistance in Pennsylvania. During the application process, Daniel does not disclose that he owns a Florida vacation home, a 2005 Honda Accord, and a Ski-Doo watercraft.

Anonymous Resolution would provide the capability to the income assistance case worker in Pennsylvania to resolve true identities and discover hidden relationships. Without Anonymous Resolution, Daniel's income assistance application would be eligible for Pennsylvania income assistance benefits. When deployed, Anonymous Resolution would create a hashed value correlated to Daniel's personal information. This would allow his data to be compared safely and securely with other jurisdictions and third party data bases (in this case land registry offices, motor vehicle registration data bases and marine data bases) thereby revealing Daniel's hidden assets, thus prompting further scrutiny.

Social service scenario #5 revisited:

Susan Gance has been receiving unemployment benefits for three months. On her way to a job interview, she is involved in an automobile accident and sustains multiple injuries to her head and neck. According to her doctor, Susan's injuries will leave her unable to work for 12 months. Susan moves in with her mother and applies for disability benefits using her mother's address. Although Susan's temporarily disability would normally qualify her for disability benefits, she is already receiving unemployment assistance and this will affect the amount of assistance she can receive.

Similar to the previous scenario, this situation may be difficult to detect and handle correctly, in particular due to the different addresses used. Again, Anonymous Resolution can facilitate sharing between two organizations without revealing identity information. Without Anonymous Resolution, Susan's disability benefits application would be received and she would be determined eligible based on her doctor's evaluation. When Anonymous

Resolution is deployed, the application for disability benefits will be compared to any benefits received from other programs and jurisdictions. When the system encounters Susan's unemployment benefits, an intelligence alert is activated. This alert will initiate further investigation and the proper evaluation of Susan's eligibility.

Social service scenario #6 revisited:
Matt Berry, a Medicaid recipient in Arizona, has submitted an application for Medicaid to Florida. He applies for these benefits using the address of his recently acquired winter vacation home in Ft. Lauderdale (Florida). Due to privacy legislation, data sharing between the 2 jurisdictions is not permitted. Without Anonymous Resolution, Matt's application would be eligible for Medicaid in Florida. With Anonymous Resolution, Matt's application would be entered into the Florida database, which would then be compared to other states. Matt's Arizona Medicaid record would be found and an alert would be generated signaling Medicaid staff of a potential issue.

The following scenario illustrates how a combination of RIS modules (Identity Resolution and Anonymous Resolution) can solve further, more complex problems.

Social service scenario #7 revisited:
Jonathan Miller, also known by his nickname, Jack, has recently passed away. His wife, Helen, has notified the regional government of the date of his death. The regional government sends a notice to the national government. However the national government fails to update Jonathan's status because he is in the identity repository under the nick name, Jack. As a result, the national government continues to pay full pension benefits, which Helen continues to receive into the joint account shared with her late husband.

The implementation of RIS in this scenario would result in a different outcome. For example, when the regional government database is enabled by Anonymous Resolution, the update to Jonathan's record would include data sharing with other databases using a cryptographic format. RIS components act perpetually, and this comparison would occur as the data is entered into the local system. Given that Jonathan is registered for pension benefits using his nickname Jack, Identity Resolution will discover that Jonathan Miller and Jack Miller share the same address, social security number and driver's license. In addition, Identity Resolution will recognize that Jack is a nickname for Jonathan. As a result of these similarities, Identity Resolution would consider the two records to be the same person. Consequently, the national government database would update Jonathan's record and terminate his pension benefits.

Conclusions

IBM RIS provides a powerful solution for making constituent application data clearer and more comprehensible for eligibility decisions. It does this before benefits and services are extended. This disambiguated provider and constituent identity data is available on demand for use by case and risk management applications and employees. RIS is the central technology solution to address fraud, waste and abuse in the social services and social security environment. Optionally, IBM WebSphere Customer Center and IBM Information Server can be added to RIS to provide other complementary role and capability to build upon existing technology investments.

Identity and prioritize initiatives

Successfully addressing the challenges facing social sector organizations requires more than new technology; it requires a comprehensive approach, based on a clear understanding of the issues, a deep understanding of the business, advanced technology thinking, and talented professionals who are passionate about what they do. As the largest provider of solutions for the social sector worldwide, IBM is able to bring together this powerful combination.

The IBM Global Social Segment is a dedicated team of subject matter experts, solution developers and industry consultants focused on social services and social security organizations. IBM has invested in a portfolio of industry solutions and thought leadership to help organizations take advantage of global best practices in the social sector. For an on line self-assessment of capabilities in this space, please visit: **ibm.com**/government/socialsegment

As the organization pursues various initiatives to help achieve its vision, an important element may be teaming with a partner to assist in its efforts to develop a strategy and a business value assessment (BVA) and business case that aligns with its objectives.

IBM consultants plan and execute the BVA from a social services business perspective employing a proven assessment method to help gain the maximum benefits and insight into the organization. The BVA offering provides a set of tools to prioritize and analyze the impact of making an RIS investment, or adding more function to an existing case and risk management system. Because the BVA is modular, an organization has the flexibility to choose the modules that address its business needs. The BVA method can help:

- *Align the social services organization and IT management with a common and prioritized set of identity disambiguation capabilities for case management and risk management system (s).*
- *Provide a visualization of the solution when it is complete.*
- *Give a high-level cost and benefit analysis to define the value of Risk Intelligence Solutions in financial terms.*

For more information

To learn more about IBM's Risk Intelligence Solutions and the IBM Business Value Assessment, contact your IBM Software sales representative or visit: **ibm.com**/software/data/ips/solutions/risk-compliance/government.html

1 Jonas, Jeff. *Threat and Fraud Intelligence, Las Vegas Style*. IBM. IEEE Security & Privacy, 2006. 28-34.

2 "Overview of the Social Security Administration." *Social Security Administration*. 2006. 20 Mar. 2006 http://www.ssa.gov/finance/2006/PerfGoals.pdf

3 "Overview of the Social Security Administration." *Social Security Administration*. 2006. 20 Mar. 2006 http://www.ssa.gov/finance/2006/PerfGoals.pdf

4 Based on conversation with T. Friedman at Gartner Group Research

IBM Corporation
Software Group
Route 100
Somers, NY
10589
U.S.A.

Produced in the United States of America
08-07

G507-1492-00