White Paper
July 2010

Threat and Fraud Prevention

IBM InfoSphere Identity Insight

Information Management

Contents

Introduction

Organizations are increasingly turning their attention to more effectively deal with threat and fraud. In regard to threat, intelligence and public safety organizations continue to be faced with massive amounts of data which must be analyzed to determine if there is a need to respond, prevent, and apprehend. In a downward moving economy, enterprises and social services agencies are under increasing pressure to control the costs associated with fraud (and its cousins "waste and abuse").

At first glance "threat" and "fraud" don't seem to go hand-in-hand. While the standard textbook definitions will not link these two words, at the core, they do share several distinguishing features:

1. They are both perpetrated by an individual with motives for gain—either financial or other personal agenda

2. Often, they require the involvement of other individuals, sometimes "insiders", to help them take advantage of a particular vulnerability

3. Both focus on a particular target, and depending on the type of target, a certain set of methods for exploitation are circulated within a guarded community.

Understanding these features is the basis for being able to select and deploy technologies that can move an organization from a focus on "research and reaction" to one that is able to "preempt and prevent". Both of these models require the same information — recognizing a person, their social network, and their actions for what they truly represent. The major difference between these two extremes is basically time. Can we discover this information before these individuals inflict harm? Time is an enemy to the organization in "research and react" mode and a friend to the criminal. Reducing this time, in some cases to fractions of a second, is one of two main ingredients in shifting the organization norm to prevention.

The second part of the recipe is expert analytics. Systems must function in the same way an analyst with a suspicious piece of information does — assemble all related data that has been observed previously ("context accumulation") to help

assess whether this is in fact damaging activity. Organizations must apply that same approach and make their data processing activities operate as intelligently. This can only be achieved through built-for-purpose expert systems that has been designed to make sense out of the data about people and their activities.

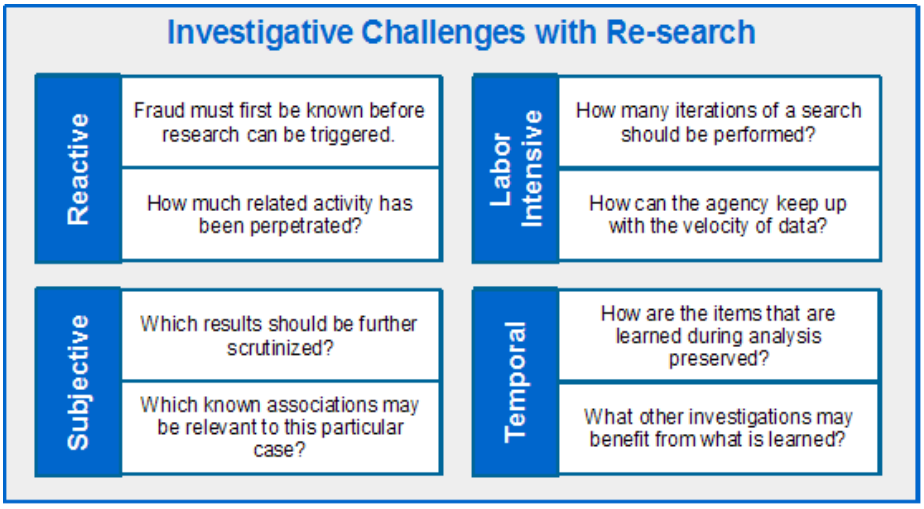
In this paper, we will examine the challenges that organizations face related to making sense of information in order to revolutionize their ability to mitigate threat and fraud. We'll then explore how IBM InfoSphere Identity Insight is helping organizations achieve this goal. Identity Insight is a market-leading entity resolution and complex event processing platform answers the three fundamental questions most pertinent to preventing negative activities – who is who, who knows who, and who does what. Finally, we will review some examples of public and private organizations that are successfully achieving their missions using this commercial-off-the-shelf software.

Overcoming the Re-search Burden

As we noted above, many organizations are mired in "research and react" mode. While research is key to detecting the relevance of an event, it is not simple or straightforward. By speaking with many organizations about how they undertake investigations, we've identified a pattern that is common within both public and private sectors. We refer to this pattern as the "re-search cycle"- a play on words which stresses the iterative nature of the process. We'll spend some time focusing on this cycle since the challenges it illustrates are the same ones that must be solved by the system used to "preempt and prevent."

In the typical investigative scenario, a report comes in with some personal identifying attributes — perhaps a name and/or phone number. For the most part, analysts have refined processes around what should be done with these breadcrumbs. These data points are used to query a primary system (the first "search"). This returns a set of new information that an analyst then reviews to determine what should be further scrutinized. At this point, the investigator must once again query (a second "search") the primary system or a set of secondary systems. This in turn surfaces new data that must once again go through this cycle.

It doesn't take long to realize that the investigator is faced with a number of obstacles to complete his investigation in a timely and accurate manner. How many iterations of a search should be performed? Which results should be further scrutinized? Which known associations may be relevant to this particular case? When querying a secondary system, which attributes should be used? Should a secondary system be searched at all? Mastery at making these decisions is some of the "art" of good investigative work. However, since the effort can be so great, there is a real risk of investigators abandoning items early, before exhausting every avenue and consequently missing what should be knowable. The picture below summarizes the key challenges.



What investigators (and expert systems) need is the ability to ask a question one time and be presented with the full range of what is knowable as the response. For example, when searching for a particular name and address, the system should respond with a ranked list of the most likely subjects of interest. A single click on one of these individuals should present a comprehensive view of all data points about that person, even if they have been observed at different addresses, or with different names! Add to this response a fully weighted list of this person's associations, and the activities they have been involved in. This information should be delivered in a moment's response and in real-time. We refer to this breadth of information as "full context" and the process that

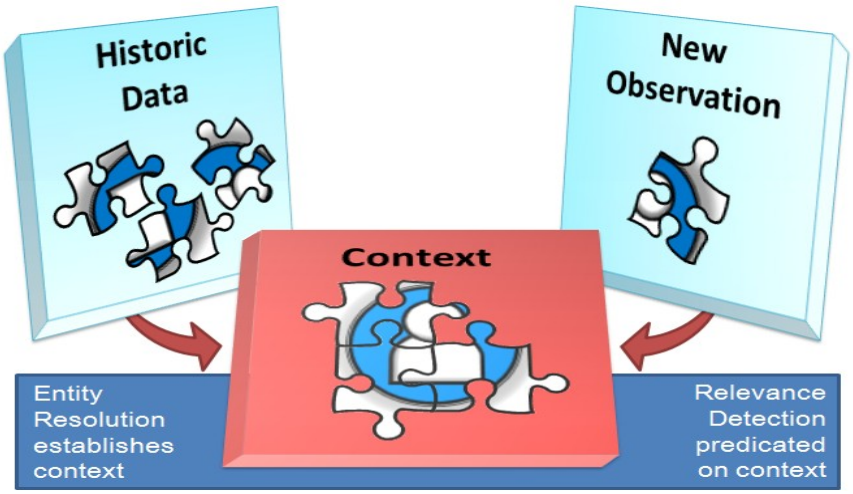
assembles this as "context accumulation". We will examine context accumulation in the following section, and then later in this paper illustrate how this requirement for an analyst is the same requirement for expert systems to then detect the relevance of an event in regard to threat or fraud.

Context Accumulation

Context accumulation is the linchpin for shifting an organization into a "preempt and prevent" approach for threat or fraud. Context accumulation is the ability to determine how a new piece of data relates to what one already knows, and then remember what is discovered so that the next piece of data the organization receives can benefit. To better understand this concept we refer people to our favorite analogy - solving a puzzle.

In this scenario, each puzzle piece is an "observation" - any data that your organization typically deals with (e.g. a loan application, a flight purchase, an address change from the internet portal, etc.). The first puzzle piece can be placed anywhere in the working space with little analysis (is it a corner or an edge). The next piece needs much more diligence. What is the color? What is the pattern? How many "innies" or "outies" does the piece have? Is it a figural? These questions must all be considered with regard to the other pieces we've already placed. As more pieces are analyzed and then connected (context accumulation), patterns and color groups form and eventually a picture emerges (full context).

In the same way that one piece of the puzzle helps us connect others, so too does data. "Data finds data." In other words, new data must be evaluated to find the data it should be connected with. This analysis must take into account the net sum of all prior information the enterprise holds. If we do not consider all past observations, the new data may be connected to only a subset of what may be possible, or may not be connected at all. An organization in this state suffers from what we call "enterprise amnesia" since they've essentially forgotten what they should know.



When all data is assembled correctly, we've then established the primary unit of context – the "entity". Therefore, (for our purposes) context accumulation can be considered synonymous with "entity resolution". The entity, having all prior pieces of information correctly assembled, enables "relevance detection" which allows an investigator to answer his most pressing questions:

- Who is this person?
- Do I already have a relationship with him?
- Is this person misrepresenting her identity?
- Has this person's interactions with our organization been negative?
- Do they have relationships with people who we have stopped in the past?
- Does their profile of activity look suspicious?
- Have we approved this activity before for this individual?
- Should a new piece of information about this person influence a previous decision we made?

Each of these questions must be answered in relationship to the full picture of the entity. In the following section we will provide a broader definition for entity

and then in the following section describe why establishing the entity is not a simple proposition.

Entities The Basic Unit of Context

In its most basic form, context is understood by resolving multiple data points into a single entity and recognizing how entities are related. Although entities are most often thought of as people, they may also be things such as businesses, vehicles, credit cards, guns, locations, or computers. Each entity is composed of a set of data attributes. Any attribute that is used to identify or describe a person or organization can be referred to as Personally Identifiable Information (PII). This would include items such as name and address but may include many other data elements as well:

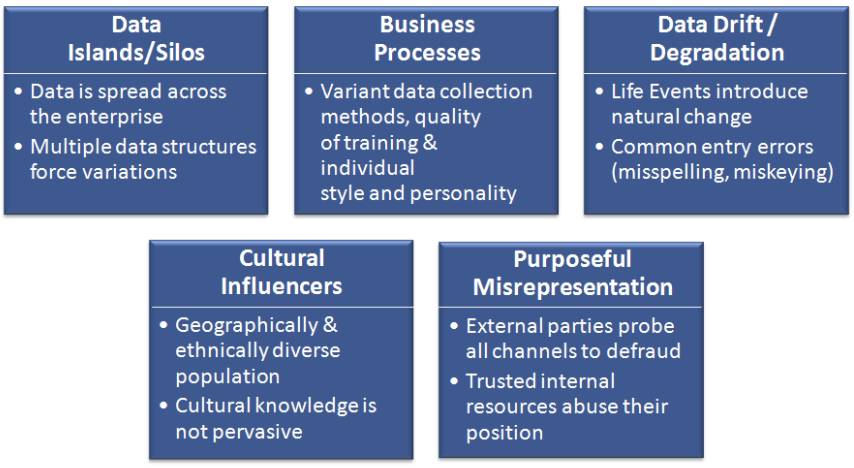
Name	Last name/Surname, First name/Given name, Middle name, Title, Prefixes/Suffixes, Generation, Organization name, Aliases, Nick Name
Location	Address 1, Address 2, Address 3, City, State/Province, Postal Code, Country, Latitude/Longitude, Corporate Region
Identifier	SSN, Driver's license, Bank Account Number, Tax ID, Passport, Loyalty Club, Phone, Credit Card
Attribute	Date of Birth, Nationality, Citizenship, Place of Birth, Height, Weight, Eye Color, Hair Color, Email Address, Cookie, IP Address, Machine ID
Associations	Spouse, roommate, vehicle, meeting

While some of these attributes are stable over a person's life, like a Social Security Number and Place of Birth, most other attributes change over time. Furthermore, individuals may have multiple values for any attribute type that must be correlated to present a complete view of the entity.

Each data type requires a unique set of capabilities to find other data values it may match with. If we were only looking for data that matched exactly, this would be an easy problem. However, the nature of how an organization gathers and manages data makes this ineffective. Additionally, since fraudsters manipulate information in unique ways, we must deploy sophisticated methods to detect weak signals. We review these challenges in the following section.

Personal Identifiable Information Data Challenges

In order to achieve context awareness, organizations must resolve and relate all relevant sources of data, and then present that information to the decision maker at the moment of highest utility. This effort is complicated by five issues common to all organizations:



Data Islands/ Silos

IT systems are very complex with different systems offering specialized processing of one type or another, often resulting in duplicate copies of the same or similar information. Over time, this information becomes out of synch, and in many cases, irreconcilable. In this environment, no single system is the

universally agreed to system of record for specific elements of information. To get a comprehensive view, all systems must be analyzed.

The data structures supporting these systems lend to this complexity. For example, address fields of only 30 characters or last name fields of only 15 are not rare. Systems may also impose different format and reference values when data is stored. The most common reference item is the gender field. Systems typically use "M" or "1" to indicate that the gender is "male". In order to reconcile entities, these references values must be translatable.

Business Processes and Workflows

Data quality continues to erode at the point of entry. Duplicate and erroneous information is constantly entering systems. However, the problem cannot be fixed by trying to standardize data entry. There are too many ports of entry to control, and it is too hard to change people's behaviors. The same data may be input differently from each source based on the quantity and quality of training, as well as individual style and personality.

Data Drift and Degradation

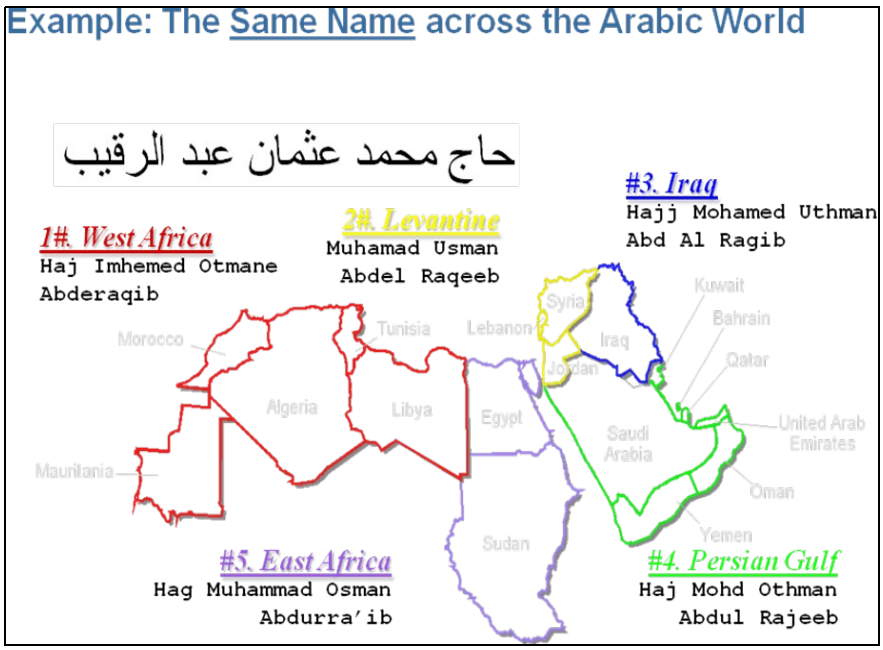
Information about people and organizations, by its very nature, is dynamic. People move, get new phone numbers, get married, take new jobs, open up new bank accounts, and so on. Recognizing how current activity (new data) relates to historical activity (historical data) is necessary to understand the whole picture of who a person is, who they know, and what they do.

Cultural Influencers

Servicing an increasingly geographically and ethnically diverse population introduces other data challenges. For example:

- Where countries include neighborhood, village, or suburb in an address, how should that information be used to determine whether two locations are actually the same?
- How should we parse "Maria del Carmen Bustamante de la Fuente" into first and last name fields?

- When validating a first name, can the analyst confirm whether "Homood" is a valid nickname for "Mohammed," "Ahmad," or "Mahmood"? (It is actually a nickname for all three).



Purposeful misrepresentation

Individuals and organized crime seek to take advantage of "the system" at every turn. This is true in both commercial and public enterprises. These threats may come from insiders who are trusted with data input and access, as well as from third-parties, who purposefully distort their identity and intent.

IBM InfoSphere Identity Insight

We've reviewed a lot of material to get to this point. In summary, many organizations take a reactive approach to threat and fraud. This is burdened by the "re-search cycle" - where investigative resources iterate through a subjective, labor intensive process for discovering information. We've outlined how context accumulation (or entity resolution) is the means by which we can avoid this expensive process. Establishing the entity is not a simple process, as there are data challenges that emanate from both internal and external sources. However, organizations must solve these problems in order to have the complete view with which to analyze incoming data and then enter into more timely relevance detection.

Real-time relevance detection predicated on full context is the goal of the organization that wishes to "preempt and prevent" fraud or threat. IBM InfoSphere Identity Insight software includes three segments of functionality that make this a possibility. These functions come together to form the analytical power of Identity Insight and are most easily remembered as "the three W's":

- Who is Who?
- Who knows Who?
- Who does What?

Who is Who – Identity Resolution

The Identity Resolution process determines whether multiple records that appear to describe different individuals or organizations are actually records for a single identity. This analysis is undergirded by our distinctive "full entity based resolution" which uses all permutations of attribute combinations to find other related records across the information universe. This feature is necessary to find individuals who seek to hide their identity.

Once the process has determined that two or more identities are the same, it integrates multiple records into a single entity and assigns a unique identifier. The resolved identity data is presented in a comprehensive, unified view that maintains all of its original attributes, such as information about the individual or organization from prior records— even identifying the source system records that provided the original data.

This rich tapestry of entity data forms the basis of information discovery, allowing Identity Insight to determine which entities and relationships should be brought to the attention of analysts for further investigation. The attributes that will be of interest to an organization will vary widely based on the industry:

Banking	An individual applying for an online account who had a credit account default for non-payment.
Social Services	The citizen applying for a new program is already the beneficiary of several others.
Retail	A corporate employee filed a slip-and-fall claim at a company outlet.
Law Enforcement	Someone stopped for a traffic citation has an outstanding warrant.
Border Security	Should the passenger be permitted to board the plane?

Who knows who – Relationship Resolution

Identifying a potential threat is often not possible without observing relationships within a network of individuals. Once accurate identity is established, Identity Insight uses the entity data to establish the nature of relationships between different individuals. Identity Insight learns whether people are, or ever have been, related in any way. Admittedly, not every relationship matters, therefore, Identity Insight only raises alerts on discoveries of relevance.

The software understands both expressed and unexpressed relationships. Expressed relationships, such as two individuals sharing a bank account, are fairly simple to identify. Unexpressed relationships are often hidden in the data, and as such, require more diligence to recognize. These unexpressed

relationships may indicate simply that people interact on a regular basis or may designate networks of persons engaging in suspicious or illegal activities through intermediaries.

InfoSphere Identity Insight goes far beyond basic "link analysis" by providing non-obvious relationship awareness (NORA™). As a distinguishing component of the analytical platform, NORA provides real-time assessment of how new data may impact the nature of a threat when viewed across multiple degrees of relationships. This functionality is like spinning a web around a social network with the person of interest at the center. If an individual on the outermost edge of the web shows up anywhere in the data space, NORA will alert the appropriate investigative group — even though there were no common data shared between these two individuals. Organizations that require weak-signal detection will find this feature compelling.

Understanding context in the form of who is related to who provides critical insight to maximize opportunities with customers, improve customer acquisition and retention, and mitigate risk.

Who does what – Complex Event Processing

Having the knowledge of "who is who" and "who knows who" well established, Identity Insight then applies complex event processing to evaluate all transactions of the entity, and optionally, of associated entities. The capability to determine all occurrences of the same person across the information landscape is required to have a clear picture of how an individual is interacting with the organization. This sophistication allows the IBM solution to discover well-concealed fraudulent activities.

The Identity Insight complex event processor is based on the observation that in many cases an alert cannot be triggered by a single event, but by a complex composition of events happening at different times and under different conditions. Events represent information about something that happened in the enterprise, such as "a prospect opens an account", "a customer transferred $300", "a citizen applied for benefits" or "a passport was just scanned". An event alert occurs when a collection of events meets specified criteria over a specified life span. Event alerts are based on business rules that are defined in the complex event processor and indicate situations of interest.

Using this technology, an enterprise can create and deploy a series of user-defined rules, unique to its business, enabling it to proactively address situations that exceed allowable thresholds. A very straightforward example would be monitoring people trying to hide transactions greater than $10k by spreading the transfers across multiple accounts to prevent being flagged for suspicious activity reporting. The following categories and tests would be used to describe this example:

Composition	Two or More payments
Correlation	Received by same person (could be various identities)
Chronology	24 hours or less
Conditions	Total amounts between $9,000 and $10,000 Monies from another institution Applies to US payees
Strategies	Raise alert for investigation by compliance team

Since Identity Insight offers transaction/event processing capabilities in near real-time, an analyst can receive an event alert the instant that threshold is met, rather than waiting for nightly batch cycles to perform this analysis.

Customer Perspectives

Both public and private enterprises have used IBM InfoSphere Identity Insight to revolutionize their ability to address threat and fraud. The following pages describe some of the business challenges within each of these enterprises and then discuss how Identity Insight is making a difference for a variety of our customers.

Financial Services

Financial institutions are continually challenged by individuals who seek to defraud their business. These challenges stem from a variety of channels, both internal and external. The crimes take a variety of shapes — Common Point of Purchase, Bust-out Fraud, Identity Theft, Impossible Geography, Card Not Present, and many others. Governments have placed the burden on the banks to identify and disrupt these schemes in order to protect their customers. Anti-Money Laundering, OFAC, PEP, Enhanced Due Diligence, NACHA — each of these requires diligence on the part of the enterprise to scrutinize the identity of the individuals with whom they do business and validate that the business is legitimate.

Red Flags legislation is also representative of this legislative pattern. As part of an Identity Theft Prevention program, these requirements specify five categories where the bank must focus:

- Information from Consumer Reporting Agencies
- Suspicious Documents
- Suspicious Personal Identifying Information
- Unusual Use of an Account
- Notice Regarding Possible Identity Theft

Traditionally, organizations have applied technologies within a particular channel (Credit, Wires, etc...) to deal with a very specific subset of these challenges. This strategy has proved to be costly to manage, incomplete in execution, and invariably overrun with false positives. Financial institutions should establish a rich analytical platform that can be leveraged within and across each channel. This platform should discover attempts at misrepresentation of identity, find networks of suspicious individuals who are collaborating, and dissect complex event scenarios that may indicate nefarious activity. The platform should allow the organization to customize the rules and thresholds to provide maximum flexibility to the business.

IBM clients are adopting InfoSphere Identity Insight to provide this key analysis. Combining both entity resolution and complex event processing within a single product, organizations are able to establish an identity, proactively discover suspicious relationships, and test for violations of business thresholds.

Here are a few examples of how customers are deriving value by using InfoSphere Identity Insight:

- An international payment provider chose to build their integrated fraud and compliance environment with Identity Insight as the analytics engine. The customer believed it was critical that data be analyzed in context rather than simply analyzing each transaction in isolation. Identity Insight first confirms the identity of each individual entered in the system, resolving against watchlist data (both internal and WorldCheck). Identity Insight then validates whether the transaction made by the individual passes business and regulatory rules, taking into account all other transactions this individual has been involved in. This has allowed the company to focus both business and IT operations around a single solution that provides robust capabilities in finding fraud.

- A US regional bank made Identity Insight a cornerstone of their Anti-money Laundering/Know Your Customer solution. The solution analyzed all customer data to uniquely resolve each individual across channels and identify relationships of interest. As data was being analyzed, Identity Insight performed validations against internal and external watchlists to determine whether there were conflicts (i.e. "alerts") that should be reported. The organization chose to send these alerts into their standard case management system. The solution provided additional benefits as the resolved identities and relationships were made available to their data warehouse to support their business intelligence reporting.

- A global money transfer organization chose to integrate Identity Insight into their existing analytical platform. While satisfied with their business rules engine, they realized they lacked a comprehensive view of the customer whom they were applying the rules against. The organization valued Identity Insight for its patented technology to

uniquely resolve identities, and thus know their customer. Identity Insight has been deployed to operate in near real-time within their transaction streams to supply the unique customer identifier on each transaction, which is then the center of all their analysis.

Social Services

State and local governments are seeking to optimize their programs to better meet the needs of their population. Information pertaining to a citizen and his/her family is currently spread across many systems – welfare, adult and aging, child programs, etc. These information silos prevent social workers from understanding the extent to which citizens qualify for benefits and raise significant hurdles in finding that information. To streamline their efforts, agencies must build a complete picture of a citizen made possible by bringing together information from across the organization into a single integrated view.

At the same time government agencies are coming under increased pressure to drive out costs related to waste, fraud, and abuse in the system. To address these issues, social service organizations cannot depend solely on new policy. What is required is the ability to harness the information they have in order to recognize unusual and suspicious activity. Only in this way can deserving citizens receive the social services they need while the agency realizes significant cost savings by preempting the abuse schemes of scam-artists.

Identity Insight has helped social service programs around the globe to better serve their citizens:

- A county in the State of California was seeking to reduce costs while improving the performance of state social programs in alignment with the state's Deficit Reduction Act. The legislation required that the Work Participation Rate (WPR) for welfare recipients reach 50 percent, and put the burden on county social service agencies to find a way to enforce this policy. The county teamed with IBM to deploy an information management system that combines Identity Insight with business intelligence to give workers an agency-wide, comprehensive view of individual cases. The system provides managers and

caseworkers with a complete, real-time understanding of case and program status, reveals relationships between benefit recipients and programs, and generates reports in minutes instead of weeks or months. To prevent abuse, the system initiates alerts when clients are out of compliance, and more importantly, when clients are eligible for additional services that could benefit them.

- A U.S. state needed to improve the integrity of its Medicaid program and managed care operations. The organization coordinated payments for 15,000 healthcare providers across millions of recipients with total fiscal responsibility in the billions of dollars. The agency recognized that significant costs could be avoided by taking action on ambiguous beneficiary enrollment, deceased recipients, and providers on an excluded list for prosecution. Additionally, the agency needed to comply with Federal Payment Error Rate Measurement (PERM) guidelines to ensure continued funding. The agency selected Identity Insight to strengthen the prepayment identification and verification process to maximize third-party recoveries. The new solution enhanced the state's ability to investigate fraud and ensure compliance with provider Medicaid standards. Beyond their own walls, the agency now coordinates anti-fraud activities with other state agencies to improve the procedures and protocols for the detection and prevention of Medicaid fraud.

- A European unemployment agency needed help with their mission to prevent wrongful payment, detect committed fraud, and expedite related investigations. While the agency already prevented millions of dollars in improper payments each year, the estimated total cost of fraud to the government across their entire social sector was in the billions. These statistics represented a great opportunity to the agency. They engaged the IBM team to conduct a pilot program, which quickly identified 50 individuals who should be removed from receiving unemployment benefits. The program is being rolled out to all sites across the country and will qualify nearly 750,000 applications each month. The solution will be used to find several types of fraud, including contribution avoidance, company collusion in falsifying entitlement, and identity-related fraud.

Tax Agencies

Tax agencies typically lose about 15% of total revenues to tax evasion and other types of noncompliance. With increasing budgetary and staffing restrictions, closing this 'tax gap' has never been more important. Such initiatives, however, are complicated by the agency's need to also respond to increasingly sophisticated tax evasion techniques.

These intensifying challenges mandate a fresh approach to managing tax compliance and fraud investigations. Yet, many agencies continue to rely on traditional random audit selection, tax collection, and enforcement methods they know to be outdated. These methods rely upon data and data relationships that are invalid and insufficient to promote maximum compliance. Instead, these methods often put the burden of an onerous examination on honest taxpayers. Auditors require tools to determine how noncompliance occurs, while also protecting the privacy of taxpayers.

Tax agencies must better leverage information—much of which they have already collected—to find the most egregious offenders. The first step is to centralize information about taxpayers, tax service providers, tax processing organizations, employers, financial institutions. Once this data is brought together, agencies can then deploy built-for-purpose analytical tooling in order to:

- Provide tax compliance collectors with a solution that support and empower them to make better real-time decisions
- Proactively detect and mitigate fraud to manage risk and follow-up on tax avoiders
- Segment taxpayers to detect who may be a higher risk, to better focus the agencies limited resources
- Detect and determine if taxpayers are properly registered and eliminate duplicate registrations

- Automate manual steps to verify taxpayer names, identities and relationships

Identity Insight is being used by national and state tax agencies to provide both the centralized registry and analytical capabilities required for preventing fraud and achieving compliance.

- A state tax agency was unable to effectively use a broad set of disparate sources to identify "non-filers". The investigative time and resource cost required to find alternative locations and contacts for the compliance department to pursue collectible revenue was a significant barrier. The situation was further complicated by the multiple taxpayer profiles for a single individual. The agency selected Identity Insight to improve tax compliance and reporting through proactive detection of taxpayer identities and relationships. The agency can now identify all parties that participated in a tax event, and therefore can more accurately determine which taxpayers are underreporting, underpaying or are non-filers. Identity Insight is also operating in real-time to notify enforcement officials when there are updates to data about taxpayers, as well as to trigger downstream events in other IT systems.

- A national tax agency needed to improve enforcement of the criminal provisions of the tax code and other related statutes related to anti-money laundering. This required deep analysis of data submitted from financial institutions related to suspicious activity. The agency selected Identity Insight to streamline access to a wider selection of data sources in support of both on-going investigations, as well as the development of new investigations. This has allowed the agency to add automation to what were manual, time-consuming information collection activities. The expanded analytic, visualization, and reporting capabilities available to agents and analysts provides the ability to leverage information that assists them in identifying and prioritizing cases for possible prosecution.

Law Enforcement

Law enforcement agencies have found that the data they have already collected is an invaluable tool for use in solving new investigations. However, like many other organizations, the number of data silos has led to significant challenges in using this information effectively. Warrants, arrests, street checks, gang data, intelligence reports, and ballistics are among many sources that may supply the key to solving an investigation. Finding the relevant information, however, is fraught with challenges. In most cases, these sources of data do not share common identifiers for any one individual, precluding the department from accessing a complete view of the suspect.

Police agencies are often surprised to find that even their record management systems lack the capabilities to solve data issues. While these systems may "suggest" existing records that are a match, they do not enforce the choice and they do little to manage the data conditions that arise when duplicates are created. In a recent study with a law enforcement customer, IBM identified a 35% duplication of identities in their system. This simple fact means that officers often lack access to all related records—missing opportunities to apprehend a person of interest, or worse, missing the data to correctly characterize risk in a given situation.

Law enforcement agencies are in desperate need of context accumulating analytics to integrate the disparate data sources that are critical to their investigative efforts. Such analytics provide the ability to locate an individual, present a complete history of their interactions, and support link analysis to uncover potential leads on active and inactive cases. Since each new piece of data to enter the system is analyzed in the context of all known data, investigators no longer miss opportunities to share information. Rather, the analytical environment maximizes the information's usefulness across every related investigation.

Moreover, these advanced analytics do not operate only on a passive basis. The technology will notify an investigator the moment the enterprise receives new data that relates to one of their cases (such as a witness to a traffic incident). This capability should not be underestimated, since it moves what is currently

"searched for" – a latent, manual process - into something that is "automatically discovered" in real-time. Exciting new forms of predictive policing come within reach.

Identity Insight is being leveraged by police agencies in the following scenarios:

- A European police agency selected Identity Insight to accurately recognize individuals (despite different variants of the data), and then detect relationships – fully automated and in real-time. The agency found that Identity Insight expedites an investigator's access to the relevant data, especially in extensive, complex cases with massive amounts of data (which is typical of their most high priority investigations). New data that has connections to existing information automatically raises alerts (data finds data), thus streamlining investigations.

- A police agency in Canada needed a way to automatically reconcile identities (duplicates within and across systems) and uncover relationships to uncover networks of suspicious individuals on active and inactive cases. While evaluating Identity Insight and proving its value for Master Name Indexing, they discovered that individuals previously known to the system were in fact multiple repeat offenders who had attempted to obscure their identity. The solution also provided other advantages within the agency, including previously unknown relationship linkages for their intelligence division.

- In the U.S., a large metropolitan police agency, like all police agencies, was maintaining dozens of systems containing crime data. The department recognized it needed an integrated, accurate, and consistent central data repository to reduce the human capital required to perform federated search and analysis. Using Identity Insight alongside their crime information warehouse, the agency now provides an "enterprise single view of the citizen" to investigators in pursuit of major crime. Analysts are now able to spend time on proactive crime investigations rather then data manipulation

Intelligence

National security challenges have never been greater. Near-misses like the Christmas Day bombing of Northwest flight 253 remind the world that higher levels of vigilance are necessary. Coping with the ever-growing volumes of data make the nature of the problem all that more complicated. Harnessing the information at hand to detect not only the obvious and non-obvious, but the adversary's efforts to conceal their identities and activities is no trivial task. Detecting the presence and actions of these individuals is virtually impossible without context accumulation.

It is worth noting that the Identity Insight technology was originally developed by Systems Research and Development (later acquired by IBM). By 2001, the venture capital arm of the CIA (In-Q-Tel) recognized the applicability to various intelligence programs, and twice granted funding to the company to further advance the technology. As a result, Identity Insight plays a unique role in national security and intelligence missions.

Find out more

For more information about how IBM InfoSphere Identity Insight can be applied to help your organization combat threat and fraud, contact your IBM representative, or visit:

ibm.com/identity