Outsmarting the social services fraudster

IBM InfoSphere Identity Insight helps agencies predict, detect and investigate fraud effectively and quickly

Massive case overload, growing populations and expansion of day-to-day programs are challenging organizations that deliver social services and benefits. In addition, ongoing cuts in funding and personnel and attacks on the integrity of social programs because of rising attempts to abuse or defraud the system clearly call for a new approach to managing services. Today's agencies need ways to improve social services case-load management, reduce fraudulent claims and efficiently deliver services to citizens—all in a cost-effective manner.

As overwhelming as these obstacles may seem, organizations can make great headway toward overcoming them by adopting and deploying an Entity Analytics (EA) solution. IBM® InfoSphere® Identity Insight software helps social services agencies attack fraud head-on, so they can deliver sustainable outcomes while enabling programs to do more with less.

Fraudsters today use many techniques to mask who they are and whom they know. They also take many measures to hide what they are doing with the very specific intent of taking advantage of systems, garnering services that were intended for someone else and joining with others to collectively work the system. These factors compel social services leaders to consider several questions:

- What would it mean to your organization if you could prevent fraud from occurring in real time?
- What if you discovered 15 percent duplication hidden among your client and citizen identifiers? What would that mean to your organization, and what could you accomplish if you could understand more clearly who is who?
- What if you were able to also understand who the fraudsters had relationships with in multiple degrees and with whom they had things in common—for example, whether two suspects had lived at the same address or at one time had the same phone number?
- What if you were able to automatically warn your colleagues and sister agencies of potential threat or fraud?
- What if you knew who was most likely to take advantage of the system and could watch for them—identifying them before they were provided services and funding?

To get an advantage, organizations need a comprehensive view of citizens across the services spectrum. Not only do the requirements for creating an integrated, horizontal and longitudinal view of citizens help reduce fraud, waste and abuse, they also inherently drive operational cost-efficiencies and deliver an enhanced citizen experience (see Table 1).

Table 1: A comprehensive view of the citizen

Requirement	Action
Locate unique identities	Provide a true horizontal view and, with the insight of a rich citizen index, help improve operational efficiencies.
Find non-obvious identities	Identify and integrate the identities that are not easy to spot and the possible connections involved, especially for fraud, waste and abuse.
Discover relationships and handle declared relationships	Recognize relationships that are unspecified and handle declared relationships to help with fraud and abuse investigations and enhance citizen experiences.
Integrate event processing	Determine which transactions have occurred across programs to enhance operational efficiency and the ability to prevent fraud.
Detect patterns and raise alerts	Automate analytics that identify patterns for study to help improve operations and address fraud, waste and abuse.
Handle massive amounts of sparse data	Manage numerous stovepipe systems with varying degrees of accuracy.

By deploying EA as a core technology, organizations can gain an edge in fraud detection and make significant gains toward operational efficiencies—which are key to accommodating these requirements.

Applying Entity Analytics to enhance investigations

EA is the methodical process of detecting like and related entities across large, sparse and disparate collections of both new and old data using advanced techniques to establish connections that are not obvious. Analytics are then applied to enable organizations to make well-informed, rapid decisions.

As a foundational component of the IBM approach to help improve social services, EA is delivered through InfoSphere Identity Insight software. InfoSphere Identity Insight deploys advanced EA specifically optimized to recognize nefarious individuals and organizations in spite of their sophisticated attempts to mask who they are, their unscrupulous relationships and what they are doing.

This core functionality helps social services organizations reduce time and labor for caseload management, comply with new regulations fast and cost-efficiently and identify fraudulent behavior rapidly to stop it before it occurs.

Comparing data in real time

Using a process called incremental context accumulation, EA detects like and related entities across large, sparse and disparate collections of old and new data. Context accumulation is an ongoing process that occurs simultaneously with analytics.

Context accumulation does much more than match new and old data. New information is compared to what was known in the past—providing context—and handled accordingly in an assertion. An assertion, for example, deems that an individual is the same as another individual or is related to another individual. A key part of this process is a method called self-correcting assertion false positives. This method means a new piece of information may reverse a previous assertion and the system corrects the assertion accordingly.

For example, if two male individuals have the same name, address and phone number, a system using EA makes the assertion that these individuals are the same person and links them together. On the other hand, if the records are updated with dates of birth that are very different, the system automatically unlinks the two records as being the same person, creates two entities and relates them as a father and son relationship.

The EA process can be broken down into the following analysis components:

- **Detecting like entities:** Using context accumulation, this ongoing process connects entities and identifies them as the same across data records.
- **Detecting related entities:** Similar to detecting like entities, this process uses data in context to determine relationships between entities.
- **Utilizing large, sparse and disparate information:** EA typically excels at analyzing these types of data. Large data applies to data sets populated with many records—even up to billions of records. Sparse and disparate data represents records that may not contain a lot of information, but can be used to make an assertion. These three data types make up a valuable resource—and demonstrate why accumulating records through context is so important.
- **Comparing old and new information:** EA is designed to operate in real time, meaning information that is new is literally just arriving to an organization. Old information is data from legacy or stovepipe systems. Together, new and old data form the context by which new records are compared and handled accordingly.

Along with detecting like and related entities through context accumulation, EA performs analytics on them. Analytics can take many forms ranging from collusion detection, conflict detection, space-and-time detection and hangout detection.

The purpose of these analytics is to help organizations make sense of their data for enhanced decision making. If fraud detection is the goal, then the analytics are configured to alert an organization to patterns in the data that could indicate an occurrence of fraud. If an enhanced citizen experience is the goal, then making sense out of all services rendered and having a more informed view of who is who, who knows who and associated activities helps dramatically improve the ability to serve the citizen quickly and cost-effectively.

Targeting fraud investigations with Entity Analytics

InfoSphere Identity Insight uses EA to help social services organizations identify and detect where and when fraudulent practices may be occurring. Based on incoming source data, InfoSphere Identity Insight detects like and related entities and performs analytics to help target their investigation to an area where fraud may be occurring.

InfoSphere Identity Insight offers the capability to integrate event information into the context of like and related entities. Event information may be transactions or activities performed between entities, and this complex event processing offers a high level of pattern detection. When a condition—for example, a pattern—involving transactions that may indicate fraud is known to occur within the data, InfoSphere Identity Insight can be configured to alert the organization any time that pattern occurs again.

In typical social services environments, an inordinate amount of time and resources is spent investigating, verifying, researching and re-researching information. Across multiple systems, activities such as making multiple phone calls, locating files and collating and compiling the information are carried out to detect and determine if fraud is occurring. The goal: answer critical queries such as: Is this person a valid new citizen in the system? Is the service requested valid? Do they actually qualify?

InfoSphere Identity Insight in action: Protecting child welfare

A social services organization can use InfoSphere Identity Insight to conduct a background check of a foster parent applicant to determine if that individual is related to someone that may put a child at risk. For example, suppose that Johnson Smith is applying to be a foster parent. The social services organization receiving the application needs to know if Mr. Smith meets the eligibility requirements. In a typical scenario, a caseworker manually searches for Johnson Smith in known registries, and conducts background checks through local police departments. However, these manual processes take considerable time to complete and may require help from already constrained and overloaded resources.

When deployed, InfoSphere Identity Insight enables a caseworker to locate and review Johnson Smith's holistic dossier in a matter of seconds. Alerts and associations are presented for a quick and accurate assessment. As reflected in Figure 1, simply viewing only one report reveals immediately that Mr. Smith has a relationship through a shared address with Frank Smith. At one time, Johnson Smith also shared a phone number with Frank Smith. However, Frank Smith has a red alert associated with his identity: with one click, the caseworker can see that Frank Smith is identified as a known felon. Based on this investigation, approving Johnson Smith as a foster parent is not recommended.

IDENTITY INSIGHT PERSON RECORD

Closest Match

MOST COMMON NAME	MOST COMMON ADDRESS	ALERT	PROG A	PROG B
SMITH, Johnson	2567 James Street, NW	N	N	Y

Known Relationships

MOST COMMON NAME	MOST COMMON ADDRESS	ALERT	ROLE	
SMITH, Jeanette	2567 James Street, NW	N	Spouse	
SMITH, Rick			Minor	

Top Five by Frequency

NAMES		DOBS		ADDRESSES	
SMITH, John	5	1961-01-31	5	1287 NW 18th Ave	5
SMYTH, Jon	1			23 Front Road, #1	2
JOHNSON, Smith	1			2567 James Street, NW	1

Record with Similar Name

NAME	ADDRESS	ALERT	PROG A	PROG B
SMITH, Johnson	23 Front Road, #1	N	N	Y
SMYTH, Jon	1287 NW 18th Ave	N	N	N
JOHNSON, Smith	2567 James Street, NW	N	Y	Y

Related by Address

NAME	ADDRESS	ALERT	PROG A	PROG B
SMITH, Frank	23 Front Road, #1	Y	N	Y
SMITH, Jeanette	2567 James Street, NW	N	N	N
SMITH, Robert	23 Front Road, #1	N	N	Y
SMITH, Jean	23 Front Road, #1	N	N	N

Related by Phone

NAME	PHONE	ALERT	PROG A	PROG B
SMITH, Jeanette	703-927-1876	N	N	Y
SMITH, Frank	703-556-9835	Y	N	Y

Figure 1: Instantaneous presentation of a dossier for a background check

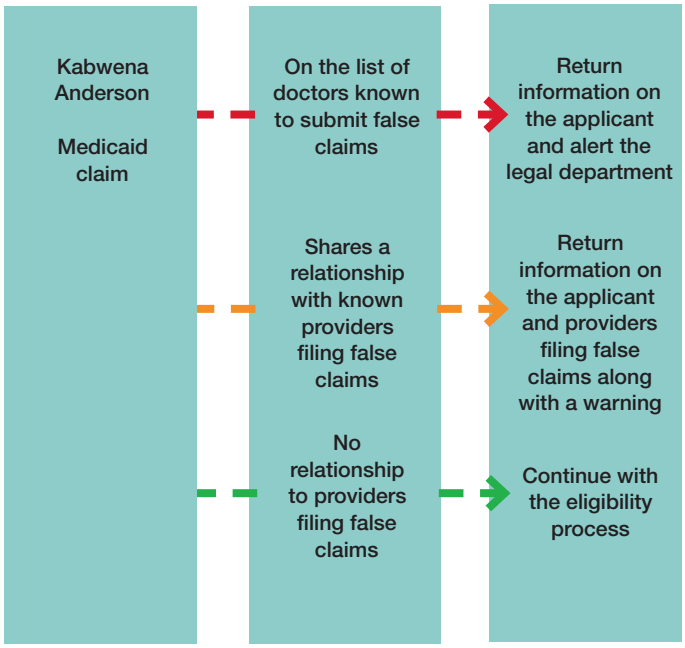

Figure 2: Decision logic for preempting provider fraud

InfoSphere Identity Insight in action: Preempting provider fraud

InfoSphere Identity Insight can help social services organizations to stop fraudulent practices before they occur. For example, the Department of Health and Human Services is pursuing a group of providers who have been caught filing false claims. The department wants to know when anyone associated with the false claim ring—such as doctors, claimants and witnesses—is filing for new services from state and county agencies.

An individual named Kabwena Anderson files a claim for health services. How can the department determine if she is associated with the false claim ring?

Spotlight on success: North Carolina Department of Health and Human Services

The North Carolina Department of Health and Human Services tracked down fraud to help reduce improper Medicaid payments to providers.

- **Business challenge:** The department needed a way to detect and investigate questionable billing practices by providers of Medicaid outpatient behavioral health care.
- **Solution:** The department deployed InfoSphere Identity Insight combined with IBM data analytics software.
- **Results:** Identified USD191 million in potentially false Medicaid claims by 206 outpatient behavioral health providers in the state.

Without an EA approach, this determination would generally be accomplished by flagging individuals manually. Often, claims agents would conduct a paper search to locate anyone within the ring who had already applied for services, which requires agents to spend extra time searching across multiple systems. They may also have to make multiple phone calls to try to detect and confirm this type of activity from any of the individuals in the false claim ring.

Using InfoSphere Identity Insight, the department can easily establish a watch list of individuals who need to be tracked as possible false claimants. A user interface supplies the department with the capability to define alerts and determine who and what systems need to be notified. As the service is requested, a lookup is automatically executed against the watch list, and notifications are sent to the appropriate people and systems to prevent additional fraud from occurring (see Figure 2).

Spotlight on success: Alameda County Social Services Agency

The Alameda County Social Services Agency created an integrated reporting system to achieve visibility and avoid overpayments.

- **Business challenge:** Lack of visibility into cases and their progress hampered outcomes and led to increased costs.
- **Solution:** The agency utilized InfoSphere Identity Insight to deploy an information system combining identity and relationship resolution with business analytics for enhanced visibility.
- **Results:** The agency achieved an average annual benefit of USD24 million, primarily through enhanced outcomes and reduced overpayments because of improvements in case information, documentation for discontinued benefits and caseworker productivity through automation of services-related workflows.

Maintaining social program integrity

InfoSphere Identity Insight enables organizations to enhance benefits delivery while helping ensure the proper use of resources. By linking clients and relationships within and among programs, it facilitates collaboration among partner organizations and allows social services programs to reduce overpayments through appropriate matching of eligibility information. Boosting the efficiency of the intake and eligibility determination processes helps agencies speed service delivery to citizens.

High-quality entity linking also results in accurate data for measuring critical success factors, such as migrating clients to self-sufficiency. Additionally, InfoSphere Identity Insight helps protect against legal and regulatory risks by enabling organizations to reduce errors, strengthen reporting and document client and provider compliance with the terms of participation.

Enabling an integrated approach to information management

InfoSphere Identity Insight integrates with other IBM Information Management software to deliver an optimized, citizen-centric process that is designed to enhance the use of available resources. The solution can be integrated with other enterprise systems through a wide variety of protocols and technologies, providing a solid foundation for data management, content management, integration, data warehousing and governance.

Agencies can manage, analyze and integrate data in real time from a variety of sources, such as client databases, vendor lists, employee databases, regulatory compliance lists and streaming data feeds. InfoSphere Identity Insight helps protect sensitive data that originates from these sources, enabling agencies to gain needed cross-organizational insights while maintaining information security and privacy.

Supporting program integrity with Entity Analytics

Social services organizations can verify the identity of citizens upon initial interaction for more accurate determination of eligibility for one or more social programs.

- **Payment and tax fraud control:** Helps reduce improper payments to citizens who are applying for mutually exclusive benefits, and identify individuals who are evading tax liabilities
- **Eligibility verification:** Checks the background of program applicants using watch lists and other external data
- **Benefit fraud:** Uncovers hidden relationships between citizens and other benefit recipients that would negate and/or reduce benefits

Helping social programs improve services and reduce costs

Social services agencies and organizations have their work cut out for them in current economic conditions, facing growing caseloads and a shrinking force of caseworkers. Deploying EA can be a first step to helping improve all aspects of services delivery including process understanding and analysis, services creation and deployment and infrastructure coordination and integration across various services.

The heightened efficiency enabled by InfoSphere Identity Insight also helps generate substantial cost-saving benefits. Enhanced management and coordination with partners such as nonprofits and community-based organizations (CBOs) can lead to increased cost sharing among organizations. And helping eliminate gaps in initial services can decrease the need for repeat services, which helps reduce overall agency costs.

In addition, InfoSphere Identity Insight helps drive strategic initiatives for smart social services, enabling programs to deliver measurable outcomes, control costs, safeguard program integrity and meet government mandates.

Gaining the upper hand on social services fraudsters

Implementing EA has an enormous advantage for social services agencies. How can organizations assess whether this approach is the right one for them? How do they determine the best place to start their journey?

IBM recommends beginning with five steps:

1. Contact an IBM marketing representative or IBM Business Partner.
2. Arrange a live social services demonstration of the IBM InfoSphere Identity Insight software.
3. Complete a proof of concept by analyzing data.
4. Develop a business case.
5. Visit **ibm.com**/us-en/marketplace/infosphere-identity-insight to check out solution briefs, customer case studies and thought-leadership papers.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States
October 2017

IMW14654-USEN-00