IBM: Analytics and Big Data
White Paper

April 2017

Strike back against identity fraud

IBM Counter Fraud Management gives insurers a powerful weapon to deter fraud

Contents

Executive summary

Fraud has no boundaries. It hits every industry in a variety of ways, across multiple channels within an organization, and is particularly damaging to insurance companies. It wreaks havoc for the individuals who are impacted and for businesses in which fraud occurs. For insurers, it can lead to financial loss and affect legal fees and brand reputation, but above all, it influences consumer confidence in a lasting way.

Masked identities and relationships are at the core of most fraud and financially motivated crimes. To fight back against fraud criminals, insurance organizations should employ a three-pronged approach to better protect and mitigate against fraud — before transactions are completed and money is disbursed (because once money is disbursed it's very difficult to get back).

The first step is to confirm that the person you are dealing with is who they say they are. This requires Entity Analytics to accurately resolve identities in real time. The next step is to verify that what the person wants to do is authorized and is the right thing to do. This requires being able to quickly see data, identities and relationships in context to uncover odd, unusual and atypical patterns or actions so that additional investigation can be performed before transactions are completed. The third and final step is to make sure that the money is being disbursed legally and responsibly. This requires making sure that the receiving parties are authorized and the transactions are legal before funds are released.

This paper presents identity fraud trends affecting the insurance industry and focuses on how IBM Counter Fraud Management's multilayered approach and diverse analytical techniques help customers take a proactive approach to preventing fraud. How? By delivering the insights needed to resolve identities earlier and enabling better business decisions to be made before fraud occurs.

Identity fraud is bad for business

Identity fraud is a complex and growing problem with significant financial and legal implications. Identity theft and synthetic identity fraud create ambiguous, misrepresented and blurry identities, making it extremely difficult for insurance companies to accurately determine if a customer is in fact who they claim to be. In addition, technology-savvy, international and highly organized crime rings are driving the vast majority of identity fraud schemes by attacking the online and mobile technology tools that insurance companies use to improve customer experience and drive loyalty. Further complicating things, insurers today must balance reducing losses due to the payment of fraudulent claims with delaying payment for those customers who are submitting legitimate claims.

Multiple types of identity fraud provide many attack vectors

Identity fraud takes many forms and there are many ways for ethically challenged people to exploit this. Four of the most common, high-level forms include:

Changed or manipulated names: occurs when multiple variations of the same name are used. For example, Kate Mills, Kate Mills-Green, Katie Green and Katherine Green are all the same person. While this may or may not be intentional, it could result in duplicate entities within a data set. In the example of an insurance policy, this person may change the name she uses to get a reduced price in a policy, or she may have a pre-existing injury or claim under one name and is using the same injury or claim to request duplicate funds under another variation of her name.

Stolen identity: happens when someone steals your identity for personal or monetary gain. There are many reasons a person or a group of people would do this. Unfortunately,

identity theft has recently become the fastest growing crime in our increasingly digital world. Potential thieves are becoming extremely adept at leveraging stolen data to commit insurance fraud, access bank accounts, get credit cards and in some cases even obtain a mortgage.

Made-up or fake identity: involves using the worldwide web and basic technology to create fake names and IDs with a few clicks of the mouse. Websites exist like http://www.fakenamegenerator.com that give a complete fake identity including a social security number, date of birth, employment history, etc.

Synthetic identity: is similar to the items above but is slightly different because thieves use a combination of legitimate and fabricated information from several different people to create a new fictitious identity, which is then used to commit many types of fraud. In this type of scheme, a fraudster will use a valid and issued Social Security Number (SSN) and combine it with a new name at a different address. (Many organized fraud rings target SSNs that are not actively being used, such as those of children, the elderly and other vulnerable populations.) These fake identities are then used to apply for credit, open accounts, purchase insurance policies, enroll in medical benefits and submit false insurance claims. They can even be used to raise capital, launder money, obtain driver's licenses and passports, travel under fake names, avoid association with known negative lists and files and undermine legislation designed to protect citizens. Synthetic identities can also undermine economies by extracting funds from a country and ultimately using these funds against that country.

Identity fraud is complex, costly and growing

Identity fraud is much more prevalent than most people are aware. Per the 2015 Identity Fraud Study by Javelin Strategy & Research, fraudsters stole $16 billion from 12.7 million U.S. consumers in 2014 resulting in a new identity fraud victim every two seconds[1] And it's getting worse. Approximately 15 million United States residents had their identities used fraudulently in 2016 — that's over 1,700 new identity fraud cases every hour of every day.[2]

Online and mobile technology open the door for fraudsters

Increased pressure to deliver a positive customer experience contributes to the rising exposure to fraud. Insurers use online and mobile technology to provide better service and entice clients to stay with them. However, this same technology also enables fraudsters and organized crime syndicates to create and use fake identities to conduct fraud. Claims can now be called in, sent through a mobile device or submitted online as part of a swift first notice of loss. As the insurer collecting the qualifying data, how do you know your customers are in fact your customers, if they actually had an accident or if they were really injured in the alleged accident?

Organized crime is in the driver's seat

Fraud is no longer just the activity of an occasional hacker. Experts estimate that 80% of fraud schemes are committed by organized crime syndicates.[3] These crime rings view identity fraud as an easy, white-collar, more lucrative and less dangerous way of obtaining millions of dollars in cash.

Sophisticated crime rings come in many forms including staged accidents, crash for cash schemes with multiple actors (e.g. drivers, passengers, repair shops, medical facilities and/or doctors, etc.) and multiple IDs. Many organized crime groups use the proceeds raised from synthetic identities to further their other criminal activities. Some of those activities can include: illegal drugs, human trafficking, violent crime and potential terrorist financing operations. Per financial crime expert Dr. Kalyani Munshani, "Using synthetic identities, safe houses can be established, cars can be rented, heavy vehicles can be bought, international travel can be facilitated and restricted goods can be bought without any flags being raised.[4]

Insurance companies face reduced profitability and increasing premiums due to fraud

Insurance fraud is estimated to be the second largest economic crime in America, exceeded only by tax evasion. [5] According to the Coalition Against Insurance Fraud (CAIF), fraud conservatively costs insurance companies $80 billion a year across all lines of insurance. [6] Per the FBI, non-health related insurance fraud costs over $40 billion per year. [7] This forces insurers to constantly be on alert: especially executives who are under enormous pressure to implement effective countermeasures.

Given that the insurance industry consists of more than 7,000 companies that collect over $1 trillion in premiums each year, it's no surprise that the massive size of the industry contributes significantly to the cost of insurance fraud by providing more opportunities and bigger incentives for committing illegal activities. [8] In fact, fraudulent claims are the single largest expense to property and casualty insurers, eroding up to 10% of the insurers revenue. And these losses are traditionally rolled into higher premiums that are passed on to the policyholders. That means insurance fraud costs the average U.S. family between $400 and $700 per year in the form of increased premiums. [9]

Insurance fraud examples

A key first step in claims submission is to validate that you are dealing with a legitimate client and a legitimate activity. In this digital world, it is far easier for both opportunistic individuals and professionally run crime groups to use altered names, stolen IDs or made up, false IDs to perpetuate a scheme. Consider some of the following real-word fraud examples:

Additional indicators of how fraud is impacting insurance institutions include:

- Anti-fraud technology likely will continue growing through next year. Nearly a third of insurers say they are budgeting to expand their technology.[10]
- 55% of U.S. consumers say poor service from an insurance company is more likely to cause a person to defraud that insurer. [11]
- 10% of property-casualty claims are fraudulent. [12]

Fraudulent claims

Fraudsters use stolen or false identities to submit fraudulent applications and stage false claims. Typically, they use stolen identities to obtain credit cards, debit cards and checks which are then used to purchase insurance policies. They then submit fake claims against these insurance policies to obtain payment. For example, a Miami, Florida crime ring purchased numerous insurance policies online using stolen, unauthorized credit card information and electronic bank checks to facilitate their crimes. Investigators identified the ring through their use of common email addresses used to purchase multiple policies. The investigators linked the policies to staged automobile accidents and false claims that the crime ring made with the help of suspect clinics. Insurers need fraud management solutions to help determine which claims are legitimate and which are fraudulent.

Workers' compensation

Workers' compensation insurance provides employees with medical and income benefits if they have been injured on the job. And while most employers and workers are very honest, some workers commit compensation fraud for personal profit and it costs the U.S. insurance industry tens of billions of dollars every year.[13]

Let's consider one suspicious worker's compensation claim

recently presented to a U.S. carrier. Employee Joe reported that on Monday morning he slipped and fell on the way into the office. Employee Joe claimed injuries even though he had only been with the company for a month and the soft tissue injuries he was claiming seemed exaggerated. Simultaneously, passenger George was the passenger in a low speed accident that resulted in soft tissue injuries reported to the same insurance company as the worker's compensation claim above. Both Joe and George were represented by the same law firm, who was known for unethical business practices with suspicious medical claims. Both Joe and George also went to the same medical provider who treated them for the soft tissue injuries being claimed.

Because these claims used two different claimant names and were submitted to two different lines of business for the same insurance carrier, the insurance company did not link them together until after the auto claim was paid in full. The worker's compensation adjuster referred the claim to the Special Investigation Unit for further investigation. Using entity analytics and link analysis, the carrier learned these two people lived at the same address and had the same phone number and a very similar date of birth.

During the investigation, employee Joe was interviewed, surveillance was conducted to obtain pictures and many other investigative steps were done. The investigation was able to prove that Joe and George were the same person and that this person also went under a third name to collect Social Security Disability benefits. The case resulted in a successful prosecution of Joe (and his alter egos), the attorney representing him under multiple names and the doctor who treated him for the same injury under multiple names. Insurers need entity analytics, link analysis and basic investigation skills to prosecute these criminals and to ensure that restitution and jail times are awarded.

Fake companies

Many criminals use synthetic identity fraud techniques to create false identities which are then used to create fraudulent businesses to extract money from insurance companies. For example, a Bulgarian organized crime group, with ties to the Russian mafia, Serbian mafia and the Italian Cosa Nostra, created security and insurance front companies to mask their criminal activities. Likewise, an Armenian-organized crime group with connections to the Russian mafia perpetrated healthcare fraud using their ownership and operation of Family Chiropractic Center, Inc. Insurers need solutions that help them determine if the companies they do business with are legitimate.

Global crime rings

Organized crime families such as the Cosa Nostra, Italian crime families in the US and Sicily, along with Russian, Mexican and Albanian mafia families across the globe have been diversifying into sophisticated forms of crime with a focus on insurance fraud. [14] One costly case involved a global crime ring that defrauded 70 U.S. insurers and made more than $11 million in false workers' compensation claims. The ring members used a network of 19 fictitious medical clinics, stole the identities of thousands of victims to submit false claims and used stolen doctors' identities to create false medical reports. The crime proceeds were laundered through Dubai, Armenia and the Philippines with ring members coming from Iran, Germany, the Philippines, Mexico and Armenia. Insurance fraud is a worldwide epidemic costing billions of dollars each year. Companies need better fraud management solutions to protect against well organized, global crime rings.

Identity resolution is top priority

Insurers need to validate customer identity and behavior patterns in real time to offset fraud as early in the process as possible and before money is moved or claims are paid. This means they need to confirm that the customer they are dealing with is who they say they are, relationships are verified and that the customer is engaging in normal behavior. They also need to ensure that the money is being sent legally to a verifiable recipient.

Combatting identity fraud involves a range of challenges, including:

- Correctly identifying a "customer," whether it be an individual or an organization, in person or through virtual representation. This means verifying someone is who they say they are when they open a claim, serve as witnesses, provide repairs, deliver medical care etc.

- Understanding hidden patterns and relationships among customers. This could mean having the same person be a witness on one claim but a third party on another claim.
- Reducing false positives to prevent unnecessary investigation of legitimate transactions.
- Increasing detection speed to limit losses and customer exposure.

Insurers of all sizes need to reduce the financial impact of identity fraud — while driving operational efficiency and investigative productivity — to improve profitability. They also need to establish best practices that can adapt to changing threats (which means being able to ingest more data from more sources [especially on the web and other external sources] to find the facts), all while maintaining compliance with state and federal regulations.

Many identities and diverse data sources increase complexity

Cyber criminals and threat vectors are rampant and constantly evolving. Fraud protection solutions must do the same to keep pace and protect against fraud. This requires access to vast amounts of open source data, including structured and unstructured data.

Insurance organizations conduct business with many people in many different roles such as employee, agent/broker, policyholder, beneficiary, named driver, excluded driver, claimant, passenger, third-party claimant/driver/passenger, witness, lawyer, medical professional or repair shop employee, among others. Managing and resolving all these identities is challenging. In addition, there are also entities on various notification lists such as internal watch lists, industry watch lists, industry alerts, official sanction list, etc. that must be considered.

Further complicating identity resolution, the data on all of these people comes in from disparate systems, in different data formats, with varying levels of completeness and accuracy of information. For example, you might only know a witness to a claim's name and telephone number, but for a policyholder you'll have more information. One data record may have the correct social security number while another record may have two digits accidently or intentionally transposed. One data record may spell a name one way and include a middle name while a related record for the same person spells the name differently and does not include a middle name or initial.

Name resolution is an important — albeit often problematic — part of these processes. There are no consistent standards for names. Some countries mandate standards, but they vary from country to country. Nicknames, transliterations between languages, multiple family names (common in many countries), different orders of names and many other factors make the variations appear very different. In addition, personal and corporate names are often represented differently in diverse onboarding systems, or the people involved may provide conflicting information. Often, this is unintentional and the result of human error (for example, names are mistyped or misspelled) or the same person may have different roles within the same company (beneficiary in one instance, account holder in another). Intentional misrepresentation of identities, however, is typically a sign of fraud.

Existing tools and processes are not effective

Conventional solutions are not fully effective at spotting stolen or synthetic identities or abnormal transactions. For example, Master Data Management (MDM) tools are frequently used to remove duplicates, standardize data formats and eliminate incorrect data to create an authoritative source of master data or a single point of reference that is then used across personnel and departments. While helpful, MDM solutions struggle with fraud because these programs typically do not include the wide range of entities that are relevant for fraud detection and investigation. MDM solutions analyze only the entities that an insurer has a formal relation with (e.g. policyholders, employees and contractors), but do not address all the occasional third parties, witnesses and other entities that insurers interact with when processing claims or completing transactions.

In addition, the usual strategy is a gradual buildup of fraud-detection defenses over time, resulting in silos of separate tools for detection and prevention. While each of these countermeasures may be effective against specific attack vectors, they don't exchange intelligence and alerts with each other and therefore can't fully cover the threat space.

Further complicating matters, very few of these point solutions share data. Each uses varying analytical techniques across channels and transaction systems, which result in organizations simply not having a complete view of risk exposures across the institution. This prevents many insurance companies from seeing patterns or behaviors that would spark a concern that fraudulent activity is crossing multi-business lines because the observation space is simply too narrow.

False positives waste investigative resources and increase risk

Early detection of potential fraud is critical to minimize financial loss and reduce risk exposure. Relying on just one analytic methodology is not enough. Insurers must focus on the most critical and harmful attack vectors first to minimize loss and risk. In addition, it is important to minimize false positives and false negatives as they negatively impact customer experience and waste limited fraud investigation and mitigation resources. For example, incorrect results might delay a policy approval or claim processing service which frustrates customers. People are impatient and no one likes to be told to wait for approval, or worse, being treated suspiciously based on facts that wind up being erroneous. Likewise, investigators might spend valuable time tracking a false positive only to find that a true fraud has occurred while they were focused on the false positive.

A different approach is needed

To keep pace with ever changing and growing threats, insurers are moving away from retrospective fraud detection methods to real-time fraud detection using multiple data streams. This enables more preventative, analytics-reliant fraud management that improves operations and delivers more effective detection and investigative techniques to prevent fraud.

An effective strategy requires both new processes and advanced tools. On the process side, collaboration among the departments that are responsible for fraud, cyber security and even operations is an essential first step. C-level visibility is equally important to ensure both a high level of priority and the budget and other resources needed to improve the organization's counter fraud posture.

On the technology side, it's not a matter of replacing existing systems or building better tools; for the most part, today's security products are effective within their (often narrow) domains. But what if you could combine the power of multiple tools and augment this with systems that continuously learn? The resulting solution would broaden the sphere of action to deliver a far higher level of protection and adapt faster than the criminals. And that's exactly the IBM approach.

Cognitive computing is required for continuous learning

As part of this new approach, cognitive systems are needed – systems than can understand, reason, learn and interact. In a counter fraud context that means:

- Understanding information in context and having a broad set of expertise relevant to counter fraud.
- Reasoning with a purpose to generate hypotheses, generate alerts, suggest avenues of investigation and provide supporting proof for these items.
- Learning at scale to capture feedback about the accuracy of its hypotheses, alerts and suggestions and to use this information to continuously improve.
- Interact in an intuitive and natural way (for example, interacting with an investigator as if they were interacting with a colleague).

Given the velocity of identity fraud, what was safe yesterday may not be safe today. Data from multiple types of sources and systems must be continuously analyzed and updated in an intelligent manner with ongoing learning to maintain a confidence level that entity identities and actions are accurate and legitimate.

IBM Counter Fraud Management (CFM) helps prevent fraud

IBM Counter Fraud Management is a proven next generation offering, delivered as a single, integrated solution that addresses all phases of enterprise counter fraud measures. This multilayered ecosystem of tightly woven analytical techniques, is designed to continuously learn and deliver stronger insights to augment the fraud unit in its decision-making. It helps prevent fraud by enabling insurers to verify if customers are who they say, understand who knows who and determine if a

particular action should be taken — all before a transaction is completed or a claim is paid. How? By eliminating information silos, expanding the observation space and enabling unified enterprise business intelligence to balance historical data with behavior patterns and business rules for early entity and relationship resolution.

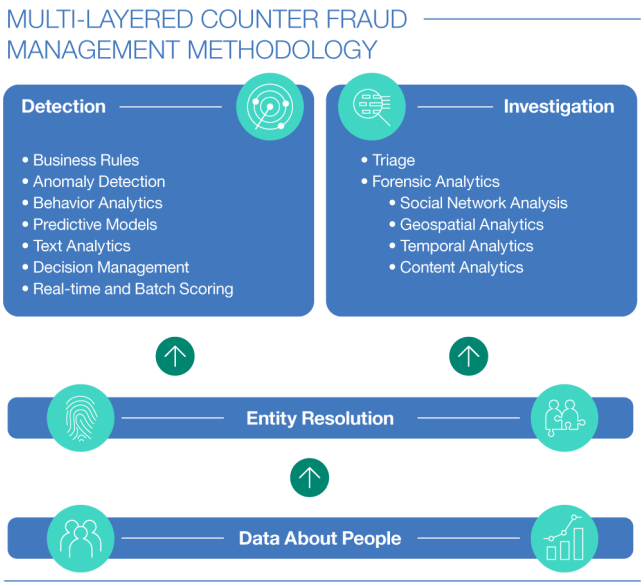
The IBM Counter Fraud Management solution allows you to reduce fraud loss exposure by being able to extract more insight from all data sources (structured and unstructured) — and share that intelligence across the institution — in order to validate identities, clarify obscure relationships and uncover suspicious behavior so the best course of action can be taken. In addition, robust dashboards provide a view of the overall fraud management process across the enterprise. Visualizations depict contextual correlations designed to help team members gain deeper fraud insights. System reports enable analysis of current and potential exposures and the effectiveness of current procedures to proactively calculate the impact of changes to operations and productivity.

CFM uses multilayered methodology to fight identity fraud

One analytic approach is not enough for a robust fraud operation. Fraudsters will try to hide their identities to avoid detection, yet there are often still clues in other data elements, which insurers need to extract, that can enable more effective decision-making. Each fraud type is unique and requires a different blend of detection and investigation analytical techniques. This is why IBM Counter Fraud Management employs multilayered analytical techniques throughout the observation space to deliver actionable intelligence and fast fraud response.

Multiple, diverse data sources combined into a centralized, dynamic entity database

In many organizations, the raw data that represents identities and relationships already exists. The problem with most systems is that there is no simple way to manage, analyze and resolve the volume of data that you need to gain the maximum insight from it. With the IBM Counter Fraud Management solution, organizations can manage, analyze and integrate data in real time from any source, such as customer databases, vendor lists, employee databases, regulatory compliance lists

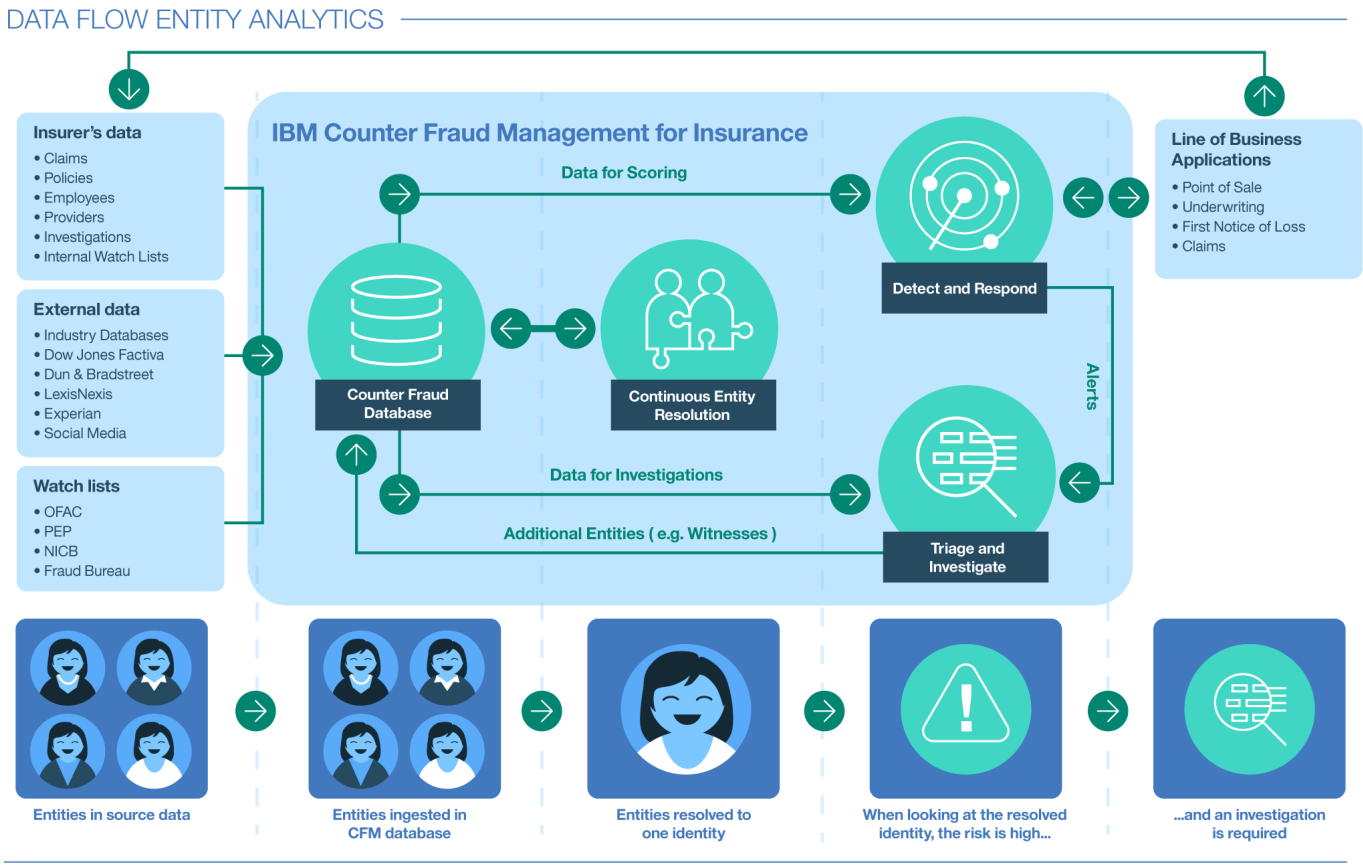


and streaming data feeds. All data about people is transported into a central repository for evaluation to create a record of truth for a given person, place, object, event, etc. This dynamic entity database integrates with other enterprise systems through a wide variety of protocols and technologies and is then used as a platform for all other knowledge-based applications.

Entity resolution determines which identities are true or fraudulent

Many insurance institutions today struggle to understand the relationships that they have with their customers. IBM Counter Fraud Management Entity Analytics helps organizations solve business problems related to recognizing the true identity of someone or something ("who is who") and determining the potential value or danger of relationships ("who knows whom") among customers, employees, vendors and other external forces.

The IBM Counter Fraud Management Entity Analytics Engine leverages advanced algorithms specifically optimized to recognize nefarious individuals and organizations despite their sophisticated attempts to mask their identity, their



unscrupulous relationships and their activities. By examining relevant individuals, their relationships and their actions, the Entity Analytics Engine uses the three-pronged approach to provide a comprehensive picture of who a person is, who the person knows and what the person does:

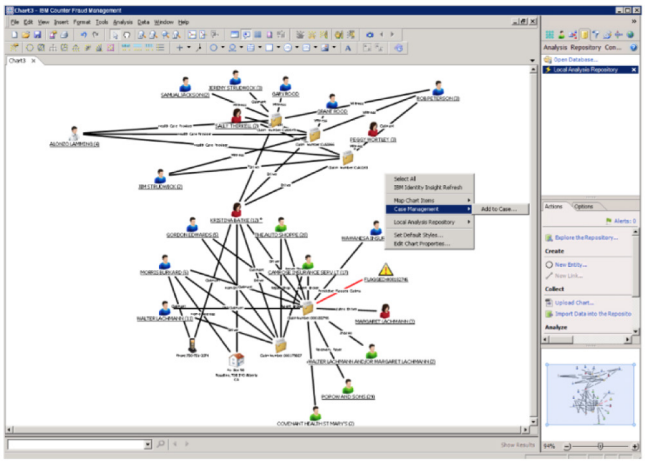
1. **Identity resolution to verify who is who.** By accumulating identity context over time, the Entity Analytics Engine uses various enterprise sources of information to determine whether individuals really are who they say they are. IBM's proprietary Global Name Recognition and Entity Resolution™ technologies look at these attributes across time to help ensure the most accurate identity and determine if a previous assumption should be corrected based on new facts.

2. **Relationship resolution to uncover who knows whom.** Once accurate identity is established, complex relationships can be uncovered. The Entity Analytics Engine processes resolve identity data to determine whether people are, or ever have been, related in any way.

3. **Complex event processing to understand who does what.** Having the knowledge of "who is who" and "who knows whom" well established, the Entity Analytics Engine 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 criminal activities.

Entity Analytics Engine
The IBM Counter Fraud Management Entity Analytics Engine can map internal and external data sets and can also consume unstructured data to provide an enhanced understanding of the customer and their business relationships while providing it in a network link graph for further human review.

IBM COUNTER FRAUD MANAGEMENT ENTITY ANALYTICS ENGINE SCREENSHOT

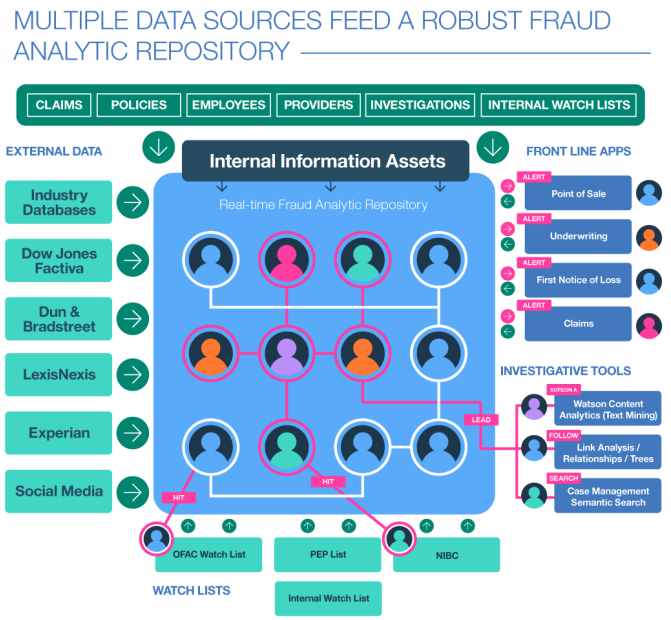


Using a combination of deterministic and fuzzy methods, the IBM Counter Fraud Management Entity Analytics Engine detects the real entities behind all people that insurers deal with — policy owners, claimants, drivers, third parties, witnesses, agents, employees, etc. It also recognizes when multiple references to what appears to be different individuals are actually about the same entity (within the same and across data sources). For example, it is essential to understand the difference between three claims filed by three people versus one person who is behind all three claims.

For each resolved entity, the system integrates the disparate identity records into a composite view of the entity, while maintaining full attribution for each record. (Full attribution ensures that data is never lost and is always traceable back to its original source.) As new data is loaded into the system, the Entity Analytics Engine updates and manages the information in context for the entities in the entity database. It can completely comprehend the meaning of new or changed data as it is loaded, making the most of each transaction and enhancing the comprehensive view of each entity in the entity database.

Building on the entity resolution process, the IBM Entity Analytics Engine then detects relationships between entities in the entity database, as records from multiple data sources are loaded and processed. The system links entities by identity attributes, such as telephone numbers and addresses, to uncover relevant, yet non-obvious relationships. It then assembles networks of associations and entities using individual data attributes (such as identification numbers and names), locations (such as IP addresses), facilities (such as warehouses, schools, airports or hotels), organizations (such as cells, clubs, associations or gangs), money (such as cash or wire transfers) and accounts (such as loyalty clubs, banks, checking, credit or savings). Finally, it identifies suspect or interesting relationships, even those that are hidden or disguised, and sends real-time alerts based on a set of user-defined rules. IBM Counter Fraud Management solution also enables analysts and investigators to perform sophisticated searches against the entity database to further explore each related entity and every entity or attribute that those entities are linked to.

This process is designed to mine the overall information landscape in real time, bringing to light all of the associations and occurrences involving the same person or group. If a questionable situation or pattern is detected, the system proactively generates alerts.



Entity analytics in action

In a recent IBM project, a P&C insurer was trying to get a firmer grasp on the composite of suspicious claims to better control and reduce financial losses. The focus was first on identifying who they were dealing with, and then understanding the interconnections within recent claims.

Using IBM Counter Fraud Management's (CFM) Entity Analytics and scoring, this insurer uncovered an alarming number of sanctioned individuals tied to auto policy data. More concerning, of these sanctioned individuals tied to policy data, 16% had been previously convicted of financial and/ or organized crimes. While having a past criminal as a customer is not an indication of fraud, it does provide insight into the risk of the portfolio.

IBM CFM also uncovered over two hundred policies which were issued to previously repudiated policyholders, with 10% having claims that had already been paid (real money out the door). By changing names or other attributes, these known fraudsters were able to bypass internal watch lists and get policies again.

This one project reaffirms the creative web of potential auto fraud. Each entity, no matter how small, has a network of some size that must be thoroughly examined so that risk exposure can be understood prior to the money being dispersed.

Global Name Recognition technology

Furthermore, IBM Counter Fraud Management can use Global Name Recognition technology, a powerful tool recognized and approved by the US Department of Defense. This expertise helps organizations to understand, recognize and match multicultural names by leveraging a unique knowledge-based approach consisting of nearly 1 billion names from more than 20 years of linguistic research.

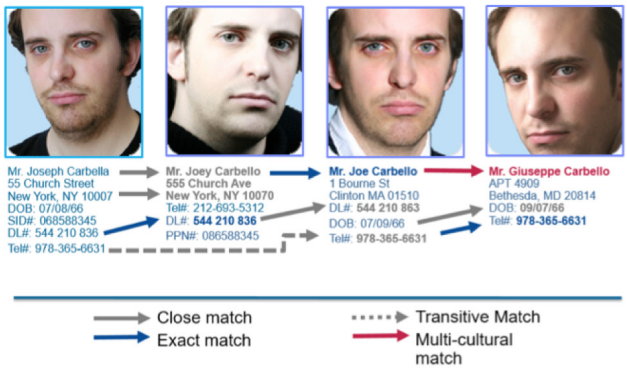


Figure: Sample identity data from multiple cross-cultural data sources

Strengthen investigations with actionable intelligence using IBM Watson Content Analytics.

Once Entity Analytics have been applied and the identities are resolved, carriers can then turn their attention to using additional advanced tools, including IBM Watson Content Analytics within IBM Counter Fraud Management, to do deep dive investigations.

IBM's powerful Watson cognitive computing technology to helps organizations aggregate, analyze and visualize massive amounts of information to expose unique insights. Watson Content Analytics helps organizations interpret and understand their enterprise information to validate what is known and reveal what is unknown.

Watson Content Analytics:

- Transforms information into insights by uncovering trends, patterns and relationships from enterprise content through intuitive analytics visualizations.
- Provides advanced content discovery and exploration by guiding users to relevant content through business understanding.

IBM Counter Fraud Management benefits

IBM Counter Fraud Management solutions help customers take a proactive approach to preventing fraud and financial crimes. Increasing organizational efficiency and effectiveness through a common, collaborative environment, IBM CFM improves situational awareness across operational communities through on-demand intuitive analysis and visualization tools. Our early detection capabilities paired with our predictive, cognitive techniques utilized across the solution suite enable companies to be more effective and make smarter, more informed decisions across a centralized, aggregated view of information from disparate sources.

IBM Counter Fraud Management helped one Canadian organization reduce 257,000 separate entities into just 187,000 — successfully resolving over 70,000 incorrect or obfuscated records. This enabled the organization to identify $41 million worth of claims with anomalous behavior.

IBM can help insurance organizations resolve identities and relationships earlier to address their enterprise fraud challenges and drive tangible business value while realizing these immediate benefits:

- Detect fraud before unnecessary payments occur (reducing losses and lowering operating costs).
- Reduce the volume of false positive fraudulent claims (so that legitimate transactions or claims are paid swiftly to a legitimate person to strengthen brand loyalty and customer retention rates).
- Prioritize true positives by identifying suspicious risk and placing transactions/claims on hold until further investigation is done.
- Quickly distinguish fraudsters from your valued customers.
- Deter suspicious transactions with confidence.
- Improve the effectiveness and efficiency of investigators.
- Focus investigations on high-risk cases.
- Manage the claims investigation process from prevention through litigation.
- Meet regulatory compliance obligations.
- Protect the institution's clients from identity theft and loss.
- Employ enterprise intelligence to continuously adjust operations and stay ahead of trends.

With IBM CFM, non-obvious connections are no longer overlooked and the rules and models applied to fragmented data and fraud rings no longer go unnoticed. Insurers can find more fraud and increase fraud savings by accurately resolving identities and finding suspicious cases that would have otherwise gone unnoticed.

IBM Counter Fraud Management is industry-agnostic

The functionality listed within CFM above is useful to any vertical industry and especially financial organizations who wrestle with similar entity fraud and identity resolution challenges. In the case of banks, CFM can help with identity theft schemes including account takeover, account opening, check fraud, ATM fraud as well as anti-money laundering schemes. Likewise, the CFM for Safer Payments offering helps prevent fraud in all cashless payment channels. Used by some of the largest portfolios in the world, this cognitive solution offers superior fraud detection accuracy and greatly reduces false alarms. It can be used for issuers, acquirers, payment switches, multi-channel or online banking and alternative payments.

For more information

To learn more about how IBM Counter Fraud Management allows organizations to reduce fraud loss exposure, please contact your IBM marketing representative or IBM Business Partner, or visit the following website: **www.ibm.com/counterfraudinsurance**

Endnotes

[1]Javelin Strategy, "$16 Billion Stolen from 12.7 Million Identity Fraud Victims in 2014, According to Javelin Strategy & Research," March 23, 2015, https://www.javelinstrategy.com/press-release/16-billion-stolen-127-million-identity-fraud-victims-2014-according-javelin-strategy.

[2]Identitytheft.info, "Identity Theft Victim Statistics," seen online February 13, 2017, http://www.identitytheft.info/victims.aspx.

[3]United Nations Office on Drug and Crime, Comprehensive Study on Cybercrime, February 2013.

[4]CBC News | Canada, "Suspected terrorist links to synthetic ID fraud are being 'ignored,' Rick MacInnes-Rae, and Mark Gollom, March 4, 2014, http://www.cbc.ca/news/canada/suspected-terrorist-links-to-synthetic-id-fraud-are-being-ignored-1.2557677.

[5]National Insurance Crime Bureau (NICB), "Insurance Fraud: Understanding The Basics," April 21, 2011, https://www.nicb.org/search/site_search?kw=Insurance Fraud: Understanding The Basics.

[6]Coalition against Insurance Fraud, seen online February 13, 2017, http://www.insurancefraud.org/statistics.htm.

[7]FBI, "Insurance Fraud," seen online February 13, 2017, https://www.fbi.gov/stats-services/publications/insurance-fraud.

[8]FBI, "Insurance Fraud," seen online February 13, 2017, https://www.fbi.gov/stats-services/publications/insurance-fraud.

[9]FBI, "Insurance Fraud," seen online February 13, 2017, https://www.fbi.gov/stats-services/publications/insurance-fraud.

[10]Coalition against Insurance Fraud, The State of Insurance Fraud Technology," November 2016, https://www.sas.com/content/dam/SAS/en_us/doc/whitepaper2/coalition-against-insurance-fraud-the-state-of-insurance-fraud-technology-105976.pdf.

[11]Coalition against Insurance Fraud, seen online February 13, 2017, http://www.insurancefraud.org/statistics.htm.

[12]Coalition against Insurance Fraud, seen online February 13, 2017, http://www.insurancefraud.org/statistics.htm.

[13]Coalition against Insurance Fraud, seen online February 13, 2017, http://www.insurancefraud.org/scam-alerts-workers-compensation.htm

[14]Thomson Reuters, Detecting And Investigating The Growing Presence Of Organized Crime In Insurance Fraud, 2013.

IBM Corporation

Route 100

Somers, NY 10589

Produced in the United States of America, April, 2017