IBM Counter-Fraud Management
Version 1.0.0

Solution Guide

Note
Before using this information and the product it supports, read the information in "Notices" on page 47.

Product Information

This document applies to IBM Counter-Fraud Management Version 1.0.0 and may also apply to subsequent releases.

Contents

Introduction v

Chapter 1. A day in the life of IBM Counter-Fraud Management 1

Chapter 2. Discovery 3
Data sources 3
Predictive models. 4
Anomaly detection models 5
Training predictive models. 6
Business rules 6
Decision trees 7
Deployment 8
IBM products used in the discovery phase 9

Chapter 3. Investigation 11
Conducting and managing an investigation. 11
Conducting a link analysis 12
Conducting a social network analysis. 14
Analyzing alerts 15
Analyzing key performance indicators 17
IBM products used in the investigation phase 18

Chapter 4. Detection 21
Entity resolution. 22
Recognize phase. 22
Resolve phase 23
Relate phase 23
Scoring a model 26
Statistical analysis 27
Combining, prioritizing, and optimizing decisions 28
IBM products used in the detection phase 28

Chapter 5. Prevention 31
Enhancing the model and business rules. 31
Reviewing alerts for quality, accuracy, and timeliness 31
Re-scoring customers 32
IBM products used in the prevention phase 32

Chapter 6. Case study: Property and casualty claim fraud 35
Staged accidents fraud scheme 35
Who is involved in the scheme? 35
What is the scheme? 35
What the insurance company does 36
Special Investigations Unit 37
Discovery 37
Investigation 38
Detection 41
Prevention. 42

Appendix. Troubleshooting a problem 43
Troubleshooting resources 43

Notices **47**

Index **51**

Introduction

IBM® Counter-Fraud Management provides actionable insights to identify fraud, to take the most appropriate action to deal with it, and to improve business results by reducing loss while maintaining a positive customer experience for genuine customers.

Accessibility features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products. Accessibility features are documented in each product's documentation.

IBM® HTML documentation has accessibility features. Because PDF documents are supplemental, they include no added accessibility features.

Forward-looking statements

This documentation describes the current functionality of the product. References to items that are not currently available may be included. No implication of any future availability should be inferred. Any such references are not a commitment, promise, or legal obligation to deliver any material, code, or functionality. The development, release, and timing of features or functionality remain at the sole discretion of IBM.

Chapter 1. A day in the life of IBM Counter-Fraud Management

IBM® Counter-Fraud Management provides actionable insights to identify fraud, to take the most appropriate action to deal with it, and to improve business results by reducing loss while maintaining a positive customer experience for genuine customers.

IBM Counter-Fraud Management helps you determine issues such as:

- How do you distinguish fraudsters from valued customers without impacting your mainstream business?
- Is a new insurance claim legitimate?
- Which bills are for legitimate services?
- Is the party entitled to the benefit that has been applied for?
- Which accounts should never have been opened in the first place?

For example, when a new insurance claim is made, all the information in the claim is analyzed by the detection engine for relationships and watch list identification. The detection engine includes business rules, entity analytics, anomaly detection matches, predictive models, and decision trees. If you are a manager, you are sent the claim and all supporting information. You review it and assign the claim to an investigator. If you are an investigator, you use a variety of tools: visual intelligence, link analysis, relationships analysis, identity insights, and alerts. During the investigation, as you discover new information through your use of these tools and through the interviews that you conduct, you feed the new information into the models, alerts, reports, and dashboards.

Here are the typical phases of working with IBM Counter-Fraud Management:

Discover
By continuously comparing customer, account, or transaction data to the data of cases that are known to be fraudulent, you can discover suspicious transactions prior to payment while continuing to pay valid transactions quickly and with greater certainty.

Investigate
In the investigation phase, you gather data about potential fraud schemes that have been discovered or detected. You investigate each one, building cases for prosecution, recovery, or denial of payment. The models, rules, and watch lists are updated with this data and are then applied in the detection and discovery phases.

Detect As fraudulent activity patterns occur in a business process, they are recognized and highlighted for further investigation. Detecting fraudulent activity patterns can occur in real time, such as during an interaction with a customer. Detection can also occur from batch processing by collecting data from other sources. For example, professionals who act on behalf of a business, such as claims adjudicators, provide data after a visit to a claim site.

Prevent
In the prevention phase, apply the results of the detection phase to stop newly-detected fraud, or to encourage fraudsters to abandon their planned schemes by showing that you know more about the scheme than they think.

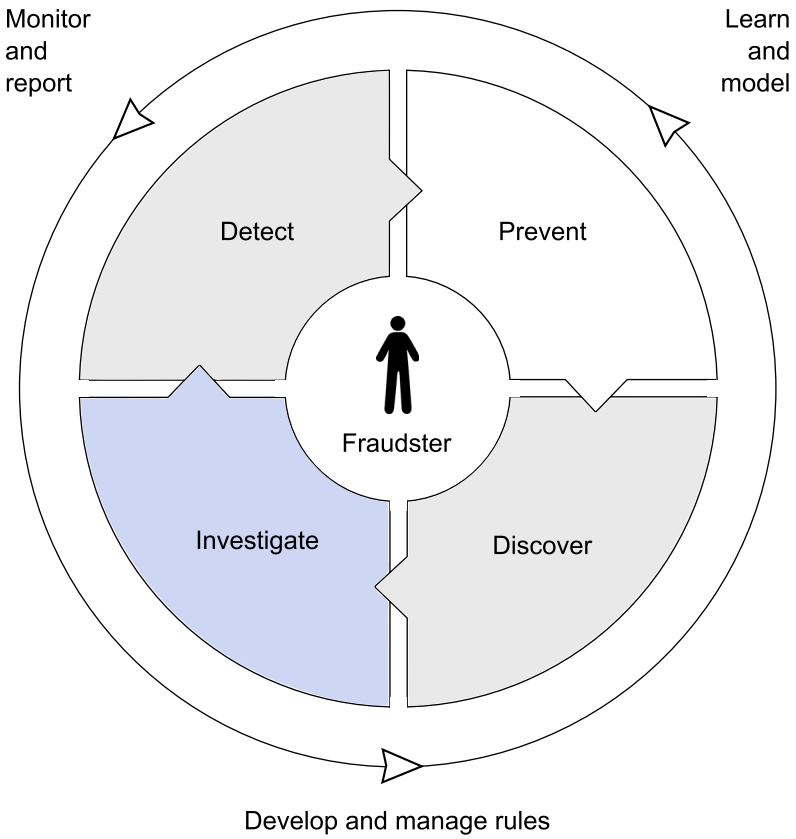

Figure 1. Workflow

Related concepts:

Chapter 2, “Discovery,” on page 3
By continuously comparing customer, account, or transaction data to the data of cases that are known to be fraudulent, you can discover suspicious transactions prior to payment while continuing to pay valid transactions quickly and with greater certainty.

Chapter 4, “Detection,” on page 21
As fraudulent activity patterns occur in a business process, they are recognized and highlighted for further investigation. Detecting fraudulent activity patterns can occur in real time, such as during an interaction with a customer. Detection can also occur from batch processing by collecting data from other sources. For example, professionals who act on behalf of a business, such as claims adjudicators, provide data after a visit to a claim site.

Chapter 5, “Prevention,” on page 31
In the prevention phase, apply the results of the detection phase to stop newly-detected fraud, or to encourage fraudsters to abandon their planned schemes by showing that you know more about the scheme than they think.

Chapter 3, “Investigation,” on page 11
In the investigation phase, you gather data about potential fraud schemes that have been discovered or detected. You investigate each one, building cases for prosecution, recovery, or denial of payment. The models, rules, and watch lists are updated with this data and are then applied in the detection and discovery phases.

Chapter 2. Discovery

By continuously comparing customer, account, or transaction data to the data of cases that are known to be fraudulent, you can discover suspicious transactions prior to payment while continuing to pay valid transactions quickly and with greater certainty.

In the discovery phase, you build models, decision trees, business rules, and alerts by drawing on information from off-line analysis. This enhanced information is used during investigations to uncover potential fraud.

Data sources

You or the administrator need to specify the data sources to use in the IBM® Counter-Fraud Management solution for modeling, analysis, simulation and testing, and scoring.

Use IBM SPSS® Statistics and IBM Analytical Decision Management to plan the model and to decide which data sources to use. You need the following types of data in the modeling process:

Historical or analytical data
To build the model, you need information about what to predict. For example, if you want to predict mortgage fraud, you need information about customers who have defaulted on their mortgages in the past. This is often referred to as historical data or analytical data, and it must contain some or all of the fields in the project data model, plus an additional field that records the outcome or result that you want to predict. This extra field is used as the target for modeling.

Operational or scoring data
To use the model to predict future results, you need data about the group or population that you are interested in, such as incoming claims. This is often referred to as operational data or scoring data. The project data model is typically based on this data.

You can use the following types of data sources:

- a database that supports ODBC, such as IBM DB2®
- an Enterprise View that is defined in IBM SPSS Collaboration and Deployment Services
- a file that is used by IBM SPSS Statistics, such as a txt or csv file

When you add a new data source, map all of its fields to ensure compatibility with the project data model. For example, if the project data model requires a field named purchase with values Yes and No for the measurement level flag, then any data source that you use must have a compatible field. If the field names are not identical, they can be mapped accordingly. Note that the input and associated mapped field must have the same data type.

You can characterize the information that each data field represents. Define a measurement level to determine how a given field is used in business rules, models, or other applications.

You can derive additional fields or attributes for the application by using the expression manager. For example, if you use banking data, you may want to create an expression that shows the ratio between a customer's income and the number of loan accounts they have. Expressions are always numeric with a measurement of Continuous; this cannot be changed.

To enforce corporate-wide policies, use global selections to choose the records to include or exclude from processing by the application. For example, you may have a corporate-wide policy to exclude customers with poor credit or payment histories from future mortgage campaigns. Global selections can be particularly effective when used in combination with shared rules. Shared rules are saved as separate objects that can be used by multiple applications. If the shared rule changes, all applications that use the rule can then be updated.

Data mining that uses IBM SPSS Modeler focuses on the process of running data through a series of nodes. This is referred to as a stream. This series of nodes represents operations to be performed on the data, while links between the nodes indicate the direction of data flow. Typically, you use a data stream to read data into IBM SPSS Modeler, run it through a series of manipulations, and then send it to a destination, such as a table or a viewer.

For example, to open a data source, you add a new field, select records based on values in the new field, and then display the results in a table. In this example, your data stream would consist of the following nodes:

- Variable File node, which reads the data from the data source
- Derive node, which adds the new calculated field to the data set
- Select node, which uses the selection criteria to exclude records from the data stream
- Table node, which displays the results of your manipulations onscreen

For more information

See the following product documentation:

- IBM Analytical Decision Management documentation (http://www.ibm.com/support/docview.wss?uid=swg27024118)
- IBM Content Analytics with Enterprise Search Information Center (http://pic.dhe.ibm.com/infocenter/analytic/v3r0m0/index.jsp)
- IBM SPSS Modeler Information Center (http://pic.dhe.ibm.com/infocenter/spssmodl/v15r0m0/index.jsp)
- IBM SPSS Statistics Information Center (http://pic.dhe.ibm.com/infocenter/spssstat/v21r0m0/index.jsp)

Predictive models

Use models to predict what is likely to happen in the future based on patterns in past data.

Models and business rules are complementary. Models lend insight and predictive power that is built on actual observations of past results. They can discover patterns that may not otherwise be apparent. Business rules may be based on corporate policies, business logic, or other assumptions. They bring common business logic to applications. The ability to combine models and rules is a powerful feature.

When building a predictive model, you need a data source and a target field. You can also choose options for preparing and partitioning data and for selecting the fields and records to use. The model is generated by applying a range of methods as appropriate to the target type, and automatically identifying the specific technique or combination that performs best on the selected data.

Use predictive models, to identify groups that show a higher or lower likelihood relative to a specific outcome. For example, you might look for customers who are most likely to default on a mortgage payment.

IBM SPSS Modeler Premium and IBM Content Analytics with Enterprise Search may be used together to construct a 360-degree view of suspects and relationships. Structured and unstructured data can be combined and resolved to improve the accuracy of the model. You can correlate unstructured information, such as reports and notes, to structural systems. You can derive and identify new trends, patterns, and anomalies in unstructured information. Semantic searching and risk alerts help turn volumes of data into a wealth of insights.

When scored, the model returns one or more fields that contain predictions, as well as the confidence interval values that are associated with those predictions. The predictions or scores that are returned by the model can then be used as input to business rules, prioritization, and other points in the application as appropriate.

For more information

See the following product documentation:

- IBM Analytical Decision Management documentation (http://www.ibm.com/support/docview.wss?uid=swg27024118)
- IBM Content Analytics with Enterprise Search Information Center (http://pic.dhe.ibm.com/infocenter/analytic/v3r0m0/index.jsp)
- IBM SPSS Modeler Information Center (http://pic.dhe.ibm.com/infocenter/spssmodl/v15r0m0/index.jsp)

Anomaly detection models

Use a clustering model to detect anomalies, which are unusual cases, or outliers, that do not conform to the natural groups in your data.

Clustering models identify groups of similar records and label the records according to the group to which they belong. This is done without the benefit of prior knowledge about the groups and their characteristics. In fact, you may not even know exactly how many groups to look for. There is no predefined output or target field for the model to predict. These models are often referred to as unsupervised learning models because there is no external standard by which to judge the model's classification performance. The value of clustering models is determined by their ability to capture interesting groupings in the data and provide useful descriptions of those groupings.

Clustering models are often used to create clusters or segments that are then used as inputs in subsequent analyses. For example, you can use a claim clustering model to organize high-risk claims into groups based on the types of applicable risk factors. The cluster result is defined as the target field and a decision tree is created to help understand the generated clusters.

For more information

See the following product documentation:

- IBM Analytical Decision Management documentation (http://www.ibm.com/support/docview.wss?uid=swg27024118)
- IBM Content Analytics with Enterprise Search Information Center (http://pic.dhe.ibm.com/infocenter/analytic/v3r0m0/index.jsp)
- IBM SPSS Modeler Information Center (http://pic.dhe.ibm.com/infocenter/spssmodl/v15r0m0/index.jsp)

Training predictive models

Predictive models must be trained to determine which data is useful and which data is not needed. When a model gives you accurate predictions, it can be used to score real-time data.

Historical measurement data is pre-aggregated, run through predictive models in IBM SPSS Modeler, and trained to determine which data is useful and which data is not needed. After you test and verify the model, you can generate a runtime predictive model. This process generates the scores that are used in scorecards and helps you to discover fraudulent claims or services.

Models must be retrained periodically to adjust for changing fraud patterns.

For more information

See the following product documentation:

- IBM SPSS Modeler Information Center (http://pic.dhe.ibm.com/infocenter/spssmodl/v15r0m0/index.jsp)

Business rules

Business rules are used to automate decisions based on business logic or on the output from predictive models.

Business rules in IBM SPSS Modeler

Depending on the application, you might use rules to exclude customers based on payment history, to refer risky claims to a special investigations unit, or to target those with the highest propensity to commit fraud as identified by a predictive model.

Models and business rules are complementary. Models lend insight and predictive power that is built on actual observations of past results, and can discover patterns that might not otherwise be apparent. Business rules might be based on corporate policies, business logic, or other assumptions. They bring common business logic to applications. The ability to combine models and rules is a powerful feature.

You can create, apply, and save rules at different points within each application. Alternatively, you can create and apply shared rules by using IBM SPSS Rules Management. Shared rules are separate objects that are used throughout applications to select and process records and to automate decisions accordingly.

You can create expressions with Control Language for Expression Manipulation (CLEM), a language for analyzing and manipulating the data that flows along IBM

SPSS Modeler streams. Data miners use CLEM extensively in stream operations to perform tasks that are as simple as deriving profit from cost and revenue data or as complex as transforming web log data into a set of fields and records with usable information. Frequently, CLEM expressions consist of a combination of functions.

For example, CLEM can be used within IBM SPSS Modeler to complete the following actions:

- Compare and evaluate conditions on record fields.
- Derive values for new fields.
- Derive new values for existing fields.
- Analyze the sequence of records.
- Insert data from records into reports.

Business rules in IBM Operational Decision Manager

Business rules and real-time events can help your enterprise achieve business process agility. The combination of business rules and events can offer intelligent decision making that enables you to take insightful, timely action in response to changes in your business network.

Business rules provide a snapshot view of static data. The rules are executed in a defined order or in an order that is determined by the inference-based algorithm of the rule engine. Business rules respond to each call as a unique transaction. One or more values are then calculated.

Event rules analyze data over variable time frames. Multiple unrelated events are processed from varied sources to identify a pattern. Event rules receive individual events from the network and, if the event completes a pattern of interest, actions are initiated on other systems.

For example, consider how business rules and event rules can be used in credit card services. The business rules detect whether transactions are over a given threshold, allow or reject the transaction, and notify customers based on the customer profile and behavior. The event rules detect events on credit cards, aggregate data on credit cards, and call business rules when a decision needs to be computed for allowing or rejecting the transaction.

For more information

See the following product documentation:

- IBM Analytical Decision Management documentation (http://www.ibm.com/support/docview.wss?uid=swg27024118)
- IBM Operational Decision Manager Information Center (http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp)
- IBM SPSS Modeler Information Center (http://pic.dhe.ibm.com/infocenter/spssmodl/v15r0m0/index.jsp)

Decision trees

When a claim or transaction is scored and identified as having a high probability of being fraudulent, recommendations can be generated to identify the best action according to your business goals.

You can use IBM Analytical Decision Management to combine the logic of business rules with the insight gained through predictive models. You can then determine what happens based on the scores received. For example, if a score breaches a threshold, what is the resulting action? Should the intake agent ask additional questions or refer the case to a special investigation team?

Specify the range of possible decisions or recommendations that can be returned by the application as well as the models and rules that determine how they are allocated. Depending on how the application is configured, the result may be a single decision for each record, a set of candidate decisions, or an aggregated point total or model score.

Defining allocations

Recommendations can be allocated by using one of the following methods:

- Based on segment rules or random percentage, which can use the model scores as inputs
- Dynamically allocated to items that are not in the dimension tree
- Based on aggregated point totals
- Based on model scores

For example, you could assign risk points to each claim based on the number of risk factors that apply.

You can automate alerts for recommended actions by integrating with other systems or by defining a routing rule to send email messages.

For more information

See the following product documentation:

- IBM Analytical Decision Management documentation (http://www-01.ibm.com/support/docview.wss?uid=swg27024118)
- IBM Operational Decision Manager Information Center (http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp)
- IBM SPSS Modeler Information Center (http://pic.dhe.ibm.com/infocenter/spssmodl/v15r0m0/index.jsp)

Deployment

You can deploy the application to a testing environment or to a real-time production environment, such as a call center or a web site. You can also deploy it to contribute to batch processing.

There are a number of options for deployment.

- In IBM Operational Decision Manager, the decision logic can be deployed to the production system as business rules or event rules. When the development and testing of the rule application is complete, you can package the rule application into a ruleset and deploy it to a runtime environment.
- In IBM InfoSphere® Identity Insight, pipelines can be deployed to a single server or multiple servers depending on the system requirements and the server resources.
- In IBM SPSS Modeler, a stream can be deployed in the repository. A deployed stream can be accessed by multiple users throughout the enterprise and can be

automatically scored and refreshed. For example, a model can be automatically updated at regularly-scheduled intervals as new data becomes available. Alternatively, a set of streams can be deployed for Champion Challenger analysis in IBM SPSS Collaboration and Deployment Services, in which streams are compared to determine which one contains the most effective predictive model.

For more information

See the following product documentation:

- IBM InfoSphere Identity Insight Information Center (http://pic.dhe.ibm.com/infocenter/easrr/v8r0m0/index.jsp)
- IBM Operational Decision Manager Information Center (http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp)
- IBM SPSS Collaboration and Deployment Services Information Center (http://pic.dhe.ibm.com/infocenter/spsscads/v5r0m0/index.jsp)
- IBM SPSS Modeler Information Center (http://pic.dhe.ibm.com/infocenter/spssmodl/v15r0m0/index.jsp)

IBM products used in the discovery phase

Several IBM products are used in the discovery phase.

IBM Analytical Decision Management

Use IBM Analytical Decision Management version 7.0 in combination with predictive analytics, local rules, and scoring to deliver recommended actions in real time, which helps you to make the right business decisions about fraudulent activity. This component automates and optimizes transactional decisions based on known characteristics and this enables known high-risk activity patterns to be detected as they occur.

For more information, see the IBM Analytical Decision Management documentation (http://www.ibm.com/support/docview.wss?uid=swg27024118).

IBM Content Analytics with Enterprise Search

Use IBM Content Analytics with Enterprise Search version 3.0 to search unstructured data, such as documents, reports, email, surveys, and applications and to find new actionable insights. The combination of content analytics and enterprise search capabilities can help you understand the meaning and context of human language to make fact-based decisions in areas such as crime intelligence, insurance claims, and patient care.

For more information, see the IBM Content Analytics with Enterprise Search Information Center (http://pic.dhe.ibm.com/infocenter/analytic/v3r0m0/index.jsp).

IBM Operational Decision Manager

Use IBM Operational Decision Manager version 8.0 to enable your business to respond to real-time data with intelligent, automated decisions. IBM Operational Decision Manager provides a business rules management system that is easy to evolve, trace, audit, and test.

For more information, see the IBM Operational Decision Manager Information Center (http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp).

IBM SPSS Collaboration and Deployment Services

Use IBM SPSS Collaboration and Deployment Services version 5.0 to manage analytical assets, automate processes, and efficiently share results widely and securely.

For more information, see the IBM SPSS Collaboration and Deployment Services Information Center (http://pic.dhe.ibm.com/infocenter/spsscads/v5r0m0/index.jsp).

IBM SPSS Modeler Premium

Use IBM SPSS Modeler Premium version 15.0 to predict the outcome of future events and interactions by discovering hidden relationships in databases, flat files, unstructured data, or your Cognos® Business Intelligence environment. Entity analysis helps you to combine and resolve the structured and unstructured data to improve model accuracy. Social network analysis helps you discover relationships among social entities and the implications of their behavior.

For more information, see the IBM SPSS Modeler Information Center (http://pic.dhe.ibm.com/infocenter/spssmodl/v15r0m0/index.jsp).

IBM SPSS Statistics

Use IBM SPSS Statistics version 21.0 to address the entire analytical process, from planning to data collection to analysis, reporting and deployment.

For more information, see the IBM SPSS Statistics Information Center (http://pic.dhe.ibm.com/infocenter/spssstat/v21r0m0/index.jsp).

Chapter 3. Investigation

In the investigation phase, you gather data about potential fraud schemes that have been discovered or detected. You investigate each one, building cases for prosecution, recovery, or denial of payment. The models, rules, and watch lists are updated with this data and are then applied in the detection and discovery phases.

Conducting and managing an investigation

To conduct and manage an investigation, an analyst designs a solution and the artifacts in the solution, a manager reviews and assigns cases, and an investigator and analyst complete the field investigation and analysis of the information that they discover.

Designing a solution

As an analyst, you use IBM Case Manager Builder to design a solution and the artifacts in the solution.

You need to understand the following concepts when designing a solution:

Solution
A solution consists of one or more related case types that provide the documents, data, business processing, and routing to the investigation teams.

Case types
Case types define the tasks, the necessary document types to support the task, the task steps, and the roles that must complete those steps to complete an investigation. The properties of the case type are displayed in views in IBM Case Manager Client.

Document types
Document types help you to organize and classify the documents that belong to a case. You can provide additional information about the documents by assigning properties to the document type.

Tasks A task has one or more steps that must be completed to complete the task. A case is not complete until all required tasks are completed or manually disabled. Each task is associated to one or more roles.

Steps Steps are the actions in a process that must be completed for a task. Use the step editor in IBM Case Manager Builder to create and edit steps, assign the steps to roles, and connect steps. Steps are called work items in IBM Case Manager Client.

Roles A role, such as Manager or Investigator, represents a specific business function for the entire solution.

You associate roles to tasks. You assign users and groups to roles in IBM Case Manager Client to specify which users can access a particular task or step. Because you define roles for the solution, you can reuse those roles across all case types when you design the solution. You can also choose to create a role that is applied only to a specific case type. When you create

tasks or steps, you can assign roles to the task or step from roles that are already defined for the solution, or you can create a new role for the solution.

Managing an investigation

As a manager, you use IBM Case Manager Client to review and analyze the work documents that are associated with each case. The work documents that are associated with the case can include an address history, link analysis chart, and prior claims synopsis.

After reviewing the cases that are referred to your team, you triage them using risk scores, deciding which to investigate first.

You then assign the cases to investigators and analysts from one of the following pages:

- Work page, which displays your in-baskets
- Cases page, which displays the list of cases
- Case Details page, which displays information about a selected case

With the IBM Case Analyzer component, you can analyze, monitor, and report information at the case level, identifying dynamic trends and monitoring case processing in real time.

Conducting an investigation

As an investigator or analyst, you use IBM Case Manager Client to process work items for an investigation.

You have access to two in-baskets: a personal in-basket of work items that are assigned to you and a role in-basket of work items that are not yet assigned to a person. For example, you can view the Investigator in-basket and assign a work item to yourself. You can view the in-basket only for your role. For example, if you are an investigator, you cannot view the Management in-basket.

While conducting the investigation and completing your assigned work items, use IBM Case Manager Client to collaborate with others, asking other knowledge workers or experts for advice in real time. You can also browse and search cases for more information to help you in your current investigation.

You can analyze, monitor, and report information at the case level, identifying dynamic trends and monitoring case processing in real time.

For more information

See the following product documentation:

- IBM Case Manager Information Center (http://pic.dhe.ibm.com/infocenter/casemgmt/v5r0m0/index.jsp)

Conducting a link analysis

During the investigation, you analyze and visualize the relationships of all the parties involved in the case.

Recognizing identities

Using the core process of entity resolution, IBM InfoSphere Identity Insight resolves inconsistent, ambiguous identity records into comprehensive entities across multiple data sets, despite deliberate attempts at misrepresentation.

An entity is a collection of one or more identities that represent the same person, organization, place, or item. Entities are stored in the entity database.

In the entity resolution process, IBM InfoSphere Identity Insight completes the following actions:

- Multiple records that seem to describe different entities are analyzed and, where applicable, are identified as a single entity.
- For each resolved entity, the disparate identity records are integrated 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 information is updated and managed in context for the entities in the entity database, resulting in an enhanced and comprehensive view of each entity in the entity database.

Detecting relationships

Building on the entity resolution process, IBM InfoSphere Identity Insight detects relationships between entities in the entity database, as records from multiple data sources are loaded and processed.

In the entity relationship process, IBM InfoSphere Identity Insight completes the following actions:

- Entities are linked by identity attributes, such as telephone numbers and addresses, to uncover relevant, yet non-obvious relationships.
- Networks of associations and entities are assembled 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).
- Suspect or interesting relationships are identified, even those that are hidden or disguised. Real-time alerts that are based on a set of user-defined rules are then sent. IBM InfoSphere Identity Insight 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.

You can view graphs or charts of entities and their relationships to other entities.

For more information

See the following product documentation:

- IBM InfoSphere Identity Insight Information Center (http://pic.dhe.ibm.com/infocenter/easrr/v8r0m0/index.jsp)

Conducting a social network analysis

You can examine group structures and communication flows within a network chart by focusing on the relationships that exist between entities.

This type of analysis is called social network analysis. It combines organizational theories with mathematical models to help you understand the dynamics of groups and organizations in which you are interested. Use Analyst's Notebook in IBM i2® Intelligence Analysis Portfolio to conduct the social network analysis.

Analysis of the structure of a network provides the following information:

- The performance of the network as a whole and its ability to achieve its key goals.
- Characteristics of the network that are not immediately obvious, such as the existence of a smaller subnetwork operating within the network
- The relationships between prominent people of interest whose position might provide the greatest influence over the rest of the network
- How directly and quickly information flows between people in different parts of the network

Centrality and centrality measures

Centrality is a key concept in social network analysis. A highly centralized network is dominated by one person who controls information flow and might become a single point of communication failure. A less centralized network has no single point of failure, so people can still pass on information even if some communication channels are blocked.

Use the centrality measures to provide different perspectives on the social relationships within the network. You can also influence the centrality measures by taking into account the direction of links and the weightings applied to them.

Betweenness centrality measure
The number of paths that pass through each entity.

Entities are gatekeeper entities if the entity has many paths running through it or if it connects different clusters in the network. Gatekeeper entities play an important communication role because they can quickly channel information to most of the others in the network.

Link betweenness centrality measure
The number of paths that pass through each link.

This can help to identify key connections of influence within the network. A link through which many paths pass might be a route for information exchange between entities.

Closeness centrality measure
The proximity of an entity to the other entities in the social network.

An entity with a high measure of closeness centrality has the shortest paths to the other entities, allowing them to pass on and receive communications more quickly than others in the organization. Information travels further to and from an entity on the edge of a network that is attached to few other entities. Entities on the edge of a network have a lower measure of closeness centrality.

Both direct and indirect closeness must be considered. Direct closeness is when two entities are connected by a link. Indirect closeness exists when information can pass between these entities via another entity.

Degree centrality measure
How connected an entity is by counting the number of direct links each entity has to others in the network.

This centrality measure can reveal how much activity is going on and who are the network's most active members.

Eigenvector centrality measure
How connected an entity is and how much direct influence it might have over other connected entities in the network.

Link direction

A link with arrows added to it represents the directed flow of information between entities; either in a single direction or in both directions. This might have an important bearing on how quickly information is passed from one part of the network to another. For example, a person might receive information from many others in the network but send information only to a select few.

Link weightings

Not all relationships in a network are equal, for example, the link between two people connected through a family relationship might be stronger than a link between two business associates. These links can be weighted so that they represent real-world strengths when carrying out social network analysis.

Charts and maps

Visualize the data by displaying it in charts and maps. You can filter chart items to display only items that meet specific criteria. For example, filtering can help you identify peak times of activity. You can also map entities and links to Google Earth where they are displayed with the icons and link colors from Analyst's Notebook.

For more information

See the following product documentation:

- IBM i2 Intelligence Analysis Portfolio Information Center (http://pic.dhe.ibm.com/infocenter/i2iap/v8r9m1/index.jsp)

Analyzing alerts

Use the Visualizer component in IBM InfoSphere Identity Insight to evaluate alerts to decide which alerts to review and which alerts to transfer to other groups.

Alerts display in the **Alert Summary** window of the Visualizer. This window is the starting point for evaluating, assigning or transferring, and reviewing alerts.

Alerts are grouped into alert summaries. Alert summaries contain all alerts of the same alert type with the same description, alert severity, status, resolution rule, relationship score, and resolution (likeness) score. One alert summary typically contains multiple individual alerts, each of which need to be reviewed and

analyzed. Part of the review includes assigning a disposition to the alert, so that you and other Visualizer users know the status of the analysis and can see comments indicating your findings.

Remember, your **Alert Summary** window only displays the following:

- Alert summaries for your group's unassigned alerts
- Alerts that you have already assigned to yourself

You do not see the alerts that other analysts in your group have assigned to themselves. Nor do you see alerts that are assigned to other groups.

Types of alerts

You can see the following types of alerts:

Attribute alerts
: Attribute alerts are alerts that are produced by attribute alert generators, which create a persistent system query looking for specific attributes or identities in the entity database. Whenever attributes for entities match the criteria of the attribute alert generator, the system creates an attribute alert.

Event alerts
: An event alert occurs when a collection of complex events meets specified criteria over a specified life span. Event alerts are based on business rules that are defined in a complex event processor. These alerts can indicate situations of interest, such as two or more purchase transactions of more than 10,000 U.S. dollars that occurred in the last hour at locations 240 kilometers from each other.

Role alerts
: A role alert identifies when one or two entities linked through a relationship that meets or exceeds a configured role alert rule. Role alerts are based on configured roles and role alert rules. They can indicate a warning or a problem (such as a customer knows a fraudster) or simply indicate relationships of interest (such as a customer knows an employee).

Evaluating alert summaries

How do you decide which alerts to assign to yourself for analysis? Start by reviewing the alert summaries in the **Alert Summary** window. As you look at the alert summaries, compare the importance of the information that makes up that alert summary with your analysis goals. You might need to evaluate one or more pieces of alert information before you can decide.

To get you started, here are some tips to help you prioritize alert summaries:

Alert severity
: Start by sorting the alert summaries by severity. This information might be enough to help you decide which alerts are most critical or important to begin analyzing.

  For example, if your organization uses "C" for alerts with a critical severity, you can immediately see which alerts are critical by simply looking at their severity.

Alert description
: Severity might not be enough information alone. The alert description

might help you decide which alerts are higher on the priority list if there are multiple alert summaries with the same alert severity.

For example, it might be more important to analyze alerts that are grouped by the "Passenger Knows Someone on the No Fly List" description than the "Passenger Knows Employee" description.

Likeness Score and Relationship Score

The higher the scores, the more likely it is that there is a relationship of interest or that the identity is the entity.

In the "Passenger Knows Someone on the No Fly List" example, if both the Likeness and the Relationship scores are 100, then the person on the No Fly list is the Passenger, and you need to take immediate action. If the likeness score is less than 70 and the relationship score is less than 85, this alert might still be important, but not critical. You might still want to analyze the entities involved in the alert, but you might not need to take immediate action.

Assigning alerts

After you know which alerts you want to work on, based on priority, you can assign those alerts to yourself. When an alert is assigned to you, that alert displays only on your **Alert Summary** window, preventing duplicate work by another user on the same alert. You can immediately see the alerts that you alone are currently researching.

If you see one or more alerts in your **Alert Summary** window that you think might belong to another group, you can transfer those alerts.

Reviewing and processing alerts

When you assign yourself one or more alerts, then you can start researching and analyzing those alerts. The Visualizer simplifies the task in the **Research** window, which displays all the relevant, associated information about the alert into one window. From the **Research** window, you can do the following tasks as part of your analysis:

- Review the alert details
- Look at the entity resumes of the related entities
- View the associated entity or alert graphs to visualize and explore the commonalities of the entities or attributes that are part of the alert
- Add comments indicating the findings of your analysis
- Change the status of the alert as your analysis progresses

For more information

See the following product documentation:

- IBM InfoSphere Identity Insight Information Center (http://pic.dhe.ibm.com/infocenter/easrr/v8r0m0/index.jsp)

Analyzing key performance indicators

To improve efficiencies, analyze key performance indicators such as money saved, money recovered, average time for investigations, and the number of analysts and investigators involved in investigations. You can analyze key performance indicators during an investigation or at the end of an investigation.

Dashboards

A dashboard is a group of objects, such as charts or indicators, that allows you to see related pieces of business information in a central location.

Dashboard charts are visual presentations of a series of related data values. They help you to quickly see comparisons, patterns, and trends in data. Dashboard charts retrieve the metrics from an underlying business view, where the chart data is in one or more columns in the view, and each row is an element of the chart series.

A dashboard indicator is a visual representation of a number's position on a scale. Indicators are useful for identifying progress towards a target and quantity levels within a range.

Business rules monitor data streams looking for exceptional business conditions and produce alert messages that describe the conditions when they exist. Further, rules can monitor a found condition and identify when it no longer exists. In IBM Cognos Real-time Monitoring Dashboard, you can create business rules from templates that predefine conditional logic. You pick the rule condition and identify the values to test. The system notifies you whenever the condition is met.

Alert messages are notifications of exceptional events in your business activities. They can be a simple message indicating that an event has occurred, or they can be detailed messages that provide contextual information that describes why the event happened or options for responding to the exception.

Reports

IBM Case Manager supports powerful reporting based on IBM Cognos BI reports and Cognos Real-time Monitoring dashboards. Users can customize reports for viewing historical and work-in-progress data generated from OLAP cubes.

For more information

See the following product documentation:

- IBM Cognos Business Intelligence Information Center (http://pic.dhe.ibm.com/infocenter/cbi/v10r2m0/index.jsp)

IBM products used in the investigation phase

Several IBM products are used in the investigation phase.

IBM Case Manager

Use IBM Case Manager version 5.1.1 to simplify the delivery of case management solutions. IBM Case Manager unites content, process, and people to deliver optimized case outcomes through analytics, rules, collaboration, and social computing.

For more information, see the IBM Case Manager Information Center (http://pic.dhe.ibm.com/infocenter/casemgmt/v5r0m0/index.jsp).

IBM Cognos Business Intelligence

Use IBM Cognos Business Intelligence version 10.2.0 to analyze key indicators in dashboards and reports.

For more information, see the IBM Cognos Business Intelligence Information Center (http://pic.dhe.ibm.com/infocenter/cbi/v10r2m0/index.jsp).

IBM i2 Intelligence Analysis Portfolio

Use IBM i2 Intelligence Analysis Portfolio version 1.0.5 to identify patterns, links, and relationships from vast, disparate data sets enabling you to rapidly identify and disrupt fraud.

For more information, see the IBM i2 Intelligence Analysis Portfolio Information Center (http://pic.dhe.ibm.com/infocenter/i2iap/v8r9m1/index.jsp).

IBM InfoSphere Identity Insight

Use IBM InfoSphere Identity Insight version 8.1 to investigate and visualize relationships and to resolve identities.

For more information, see the IBM InfoSphere Identity Insight Information Center (http://pic.dhe.ibm.com/infocenter/easrr/v8r0m0/index.jsp).

Chapter 4. Detection

As fraudulent activity patterns occur in a business process, they are recognized and highlighted for further investigation. Detecting fraudulent activity patterns can occur in real time, such as during an interaction with a customer. Detection can also occur from batch processing by collecting data from other sources. For example, professionals who act on behalf of a business, such as claims adjudicators, provide data after a visit to a claim site.

As soon as data is collected, it is submitted automatically to IBM® Counter-Fraud Management to detect possible fraud. To accommodate a wide range of business process workload profiles including processing large numbers of transactions, a hybrid of batch and real-time analytics and decision processing is supported.

The analytics and decision processing services include the following functions:

- Entity resolution of incoming identities and relationships
- Profiling and scoring of structured and unstructured data
- Statistical analysis
- Combining, prioritizing, and optimizing decisions by using models and business rules

The analytic and decision processing services automate complex detection tasks to deliver actionable referrals, often to a case management system.

Cases that warrant further investigation are routed to IBM Case Manager for a special investigations unit to pursue. IBM Case Manager helps assemble the related information for the case and unites content, process, and people to deliver optimized case outcomes through analytics, rules, collaboration, and social computing. During the investigation, updates that are entered in IBM Case Manager are automatically pushed to IBM i2 Intelligence Analysis.

Business rules are used to automate decisions based on business logic or on the output from predictive models. For example, you might use rules to exclude customers based on payment history, to refer risky claims to a special investigations unit, or to target customers with the highest propensity to commit fraud as identified by a predictive model. You can create, edit, and share rules that can be used throughout applications to select and process records and to automate decisions accordingly.

While business rules bring common business logic to applications, models lend insight and predictive power. The ability to combine models and rules is a powerful feature. For each rule and model, you can specify the range of possible decisions or recommendations that can be returned. The result can be a single decision for each record, a set of candidate decisions, or an aggregated score. You can also combine the output from multiple rules and models by using a matrix.

Additionally, the analytic and decision services can invoke an external process to push to or pull from decision data that is recorded in the data store.

An analytic process can be simple or complex.

Here is an example of a simple analytic process:

1. Feed a single transaction from an external system via IBM Integration Bus to IBM SPSS Collaboration and Deployment Service.
2. Return a single score back to the external system.

Here is an example of a complex analytic process:

1. Feed a single transaction along with some transaction history to IBM Integration Bus.
2. Resolve entity data using IBM InfoSphere Identity Insight.
3. Read profile data using IBM Integration Bus.
4. Aggregate the transaction history using IBM Integration Bus.
5. Merge data using IBM Integration Bus.
6. Perform calculations using IBM Integration Bus.
7. Apply IBM Operational Decision Manager business rules.
8. Conditionally calculate scores using IBM SPSS Collaboration and Deployment Service.
9. Feed scores along with other input data to IBM SPSS Collaboration and Deployment Service to execute a module in IBM Analytical Decision Management.
10. Apply IBM Operational Decision Manager business rules to make a final decision about a recommended action.
11. Send the final decision to an external system or to IBM Case Manager.
12. Store the calculations, scores, and results of decision processing.

Entity resolution

Pipelines perform entity resolution as they process incoming identity records in these phases: recognize, resolve, and relate.

Pipelines are the component that perform name and address hygiene standardization, data quality management, and entity resolution. The pipelines also perform relationship resolution and generate alerts, based on the system configuration.

Recognize phase

During entity resolution, pipelines must recognize the data by validating, optimizing, and enhancing the incoming identity data. During the recognize phase of the pipeline process, the pipelines cleanse and standardize the data values, as well as perform data quality checks on the data to protect the integrity of the entity database.

Data quality management (DQM) is the pipeline process that checks the data for required values, valid data types, and valid codes. You can also configure DQM to correct the data by providing default values, formatting numbers and dates, and adding new codes.

For more information

See the following product documentation:

- IBM InfoSphere Identity Insight Information Center (http://pic.dhe.ibm.com/infocenter/easrr/v8r0m0/index.jsp)

Resolve phase

During entity resolution, the pipelines resolve identities into entities. After the data values in the identity records have been cleansed, standardized, or enhanced, the pipeline uses sophisticated search algorithms to compare the data values in the incoming identity record against existing entities in the entity database to determine if they are the same entity.

Resolving entities involves the following steps:

Generating candidate lists
The system uses the information on the incoming identity record to match against entities already in the entity database to create a list of potential entity resolution candidates. Each candidate shares enough attribute values to continue evaluating the candidate for entity resolution. You can configure the criteria that the system uses to generate the candidate lists.

Applying the resolution rules
After the system generates candidate lists, it applies the resolution rules to each entity on the candidate list. It uses a scoring method that calculates a resolution score to determine if the incoming identity and the existing entity should be resolved.

Resolution rules are a set of criteria that the system uses to define how compared entities resolve (if they are or are not the same entity) and relate (if entities are not resolved to the same entity, how many attributes they share).

You can configure resolution rules and set the thresholds for the resolution scores to determine how closely the attribute values must be for the incoming identity and the candidate entity to be resolved into one entity.

Re-resolving and unresolving
The re-resolve process occurs during the entity resolution process. Two entities are resolved as the same entity and a composite entity record is created. Entity resolution uses the new composite entity record to start the process all over again, to see if the new composite entity can be resolved to any of the other entities in the entity database.

The unresolve process occurs as part of the entity resolution process when the attribute values on the incoming identity provide new information that indicates that a composite entity is actually made up of two entities and the composite entity record is split into the two entities. The system knows which records belong to which entity because of the data source associated with each record. When the unresolve process completes, the system then begins the re-resolve process.

For more information

See the following product documentation:

- IBM InfoSphere Identity Insight Information Center (http://pic.dhe.ibm.com/infocenter/easrr/v8r0m0/index.jsp)

Relate phase

During entity resolution, pipelines also complete the relationship detection process, which detects relationships between identities and entities and then generates alerts for relationships of interest.

Roles classify identities by defining the focus or purpose for each identity. In this way, relationships are detected and established. You define and assign roles to identities by data source or as part of transforming the original data source data into Universal Message Format (UMF).

When the pipeline processes incoming identities for entity resolution and resolves the identity to an existing entity, the two records have a 0-degree relationship; that is, the incoming identity and the entity are the same. But the entity resolution process can go beyond 0-degree relationships, depending upon how the system is configured.

After the pipeline exhausts all possibilities in the entity resolution resolve phase, the relationship detection process evaluates the entities that remain on the candidate list, or those entities that did not resolve to the incoming identity, to see if a relationship exists between them. Typically, entities that are on the candidate list are linked to the incoming identity at 1-degree of separation for at least one attribute. Both entities share the same attribute data values for at least one attribute, which is why the entity is on the candidate list.

After the process detects a relationship, the system compares the assigned roles between the identity and the entities to the configured role alert rules. If the system finds that the roles that are assigned to the identity and an entity meet the criteria for that rule, the system generates an alert. It has detected a relationship of interest. The relationship can be at 0-degrees, 1-degree, or multiple degrees, depending upon how the system and the role alert rules are configured.

Relationships

Relationships are links between two or more entities. Relationships are detected at the end of the entity resolution process, when two entities share several data attribute values.

Relationships can be based on links discovered by the system, disclosed by an analyst, or both. However, not every relationship is interesting enough to warrant an alert for further analysis or investigation. Define relationships of interest by configuring role alert rules that specify which combination of roles assigned to entities need to generate alerts. For example, you might want to be alerted if an insurance claimant knows one of your employees.

For more information

See the following product documentation:

- IBM InfoSphere Identity Insight Information Center (http://pic.dhe.ibm.com/infocenter/easrr/v8r0m0/index.jsp)

Roles

A role is a classification of an identity that defines the focus or purpose of that identity. You can associate one or more roles with an identity. As identities are resolved into entities, entities inherit all associated roles.

Use roles to configure role alert rules, which define relationships of interest and generate alerts. Examples of useful roles might include employees, vendors, customers, or watch list.

Every identity is assigned a role in one of the following ways:

Incoming data source
When you configure a new data source, you associate a role with that data source, which will assign that role to all identities containing that data source code.

Universal Message Format
When you transform the data source into Universal Message Format (UMF), you can directly assign roles as part of the UMF record using the <SEP_ROLES> UMF segment with the <ROLE_CODE> UMF tag. If you configure by UMF, you must add data quality management rules and a lookup table.

For more information

See the following product documentation:

- IBM InfoSphere Identity Insight Information Center (http://pic.dhe.ibm.com/infocenter/easrr/v8r0m0/index.jsp)

Alerts

Alerts are messages or other indicators that signal that an event has occurred. Attribute alerts are generated whenever entities match a specified collection of attributes. Role alerts are generated whenever linked entities share roles that you define as being interesting or conflicting.

It is important to define what alerts meet your organization's goals. A good place to begin is to ask which relationships between entities are of interest to your organization. Relationships are based on user-configured roles, which are assigned to incoming data records by the source system. When two entities share enough attribute data values without resolving to the same entity, those entities form a relationship.

For example, you might want to generate an alert if the address for a person who is listed on a government watch list is similar to the address of one of your employees. Another relationship of interest might be that two separate slip-and-fall reports are for people with similar names and addresses.

Attribute alerts

Attribute alerts are alerts that are produced by attribute alert generators, which create a persistent system query looking for specific attributes or identities in the entity database. Whenever attributes for entities match the criteria of the attribute alert generator, the system creates an attribute alert.

You can create your own personal attribute alert generators. If you are looking for a specific identity or any identities or entities that match a specific set of attributes, you can create your own personal attribute alert generator that searches for matches until the specified expiration date. The attribute alert generators that you create are only available to you.

Examples of possible entity attributes you might want to be notified about include:

- Name and unique number, such as a credit card number
- Name and phone number
- Address
- Name and non-unique number

Role alerts

A role alert identifies when one or two entities are linked through a relationship that meets or exceeds a configured role alert rule. Role alerts are based on configured roles and role alert rules. They can indicate a warning or a problem (such as a customer knows a fraudster) or simply indicate relationships of interest (such as a customer knows an employee).

Make sure that the role alert rules configured for your organization clearly define which entity roles create a relationship that your analysts want to investigate further. To define relationships as being interesting or conflicting, configure the role alert rules that identify which roles should not exist in a single entity or cannot be linked between entities.

During entity resolution, the pipeline evaluates relationships between the incoming identity and entities on the candidate list. After it determines that a relationship exists between the incoming identity and a candidate entity, the system evaluates whether the roles assigned meet a configured role alert rule. If so, the system generates a role alert.

For more information

See the following product documentation:

- IBM Cognos Business Intelligence Information Center (http://pic.dhe.ibm.com/infocenter/cbi/v10r2m0/index.jsp)
- IBM InfoSphere Identity Insight Information Center (http://pic.dhe.ibm.com/infocenter/easrr/v8r0m0/index.jsp)

Scoring a model

To score a model means to apply it to some data or a population in order to obtain a result or prediction that can be used as input to decisions.

Depending on the application, the scoring results can be written to a database table or flat file or used as inputs to the segment, selection, and allocation rules that drive decisions in an application.

During entity resolution, the system computes how closely the attributes for an incoming identity match the attributes of an existing entity. The results of this computational analysis are the scores that the system uses to resolve identities into entities and to detect relationships between entities.

Resolution scores

After the entity resolution process uses a confirmation and denial process to prevent false positives, the system creates a baseline resolution score for both the incoming identity and the entity on the candidate list. The resolution score defines the likelihood that the compared identities represent the same entity. This score is user-defined and is used to resolve a new identity to an existing entity.

As the pipeline processes incoming identities for entity resolution, it compares the shared attribute values for the attributes of the incoming identity and of each entity on the candidate list. Part of the comparison includes computing scores that represent how closely the attribute values match. These scores are then compared against the configured thresholds and resolution score for each resolution rule.

When you configure an attribute to be used for confirmation or denial, you specify the number of points up or down to adjust the baseline resolution scores of the incoming identity and the candidate entity. If the attribute values match, the resolution score can be positively affected by adding the configured number of points. If the attribute values do not match, the relationship score can be negatively affected by subtracting the configured number of points.

The system compares the resulting resolution score of the incoming identity and the candidate entity to each resolution rule. If the resolution score meets or exceeds the configured resolution confidence score for the resolution rule, the system resolves the incoming identity into the candidate entity, creating one composite entity in the entity database.

Relationship scores

The relationship score is assigned during entity resolution as a result of applying the resolution rules. The relationship score defines how closely the two compared identities are related to each other. This score is user-defined and is used to relate entities.

During entity resolution, the pipeline compares the incoming identity against the remaining entities on the candidate list. While these candidate entities may not resolve to the incoming identity, they are still evaluated for relationships.

If the relationship score satisfies the criteria configured for relationships by degrees of separation, the system determines that the two entities are related. The relationship is written to both composite entity records. The system then checks the configured role alert rules to determine if the relationship is considered a relationship of interest. If so, the system generates an alert.

If the relationship score does not satisfy the criteria configured for relationships, the process moves to the next entity on the candidate list, until all entities have been evaluated for relationships.

For more information

See the following product documentation:

- IBM SPSS Modeler Information Center (http://pic.dhe.ibm.com/infocenter/spssmodl/v15r0m0/index.jsp)

Statistical analysis

You can use IBM SPSS Statistics to view data, formulate hypotheses for additional testing, clarify relationships between variables, create clusters, identify trends, and make predictions.

When analyzing statistics, you can use linear models or nonlinear models. Linear models offer a variety of regression and advanced statistical procedures designed to fit the inherent characteristics of data that describes complex relationships. Nonlinear models provide the ability to apply more sophisticated models to data.

To improve risk analysis and decision making, you can also use simulation capabilities in IBM SPSS Statistics to automatically model many possible outcomes when inputs are uncertain.

Customized tables help you to easily understand the data and quickly summarize results in different styles for different audiences.

For more information

See the following product documentation:

- IBM SPSS Statistics Information Center (http://pic.dhe.ibm.com/infocenter/spssstat/v21r0m0/index.jsp)

Combining, prioritizing, and optimizing decisions

While selections and allocations may return multiple possible decisions or recommendations for each record, you can specify how the final decision is made. This can be done by using a prioritization or optimization equation, or by combining the output from multiple rules and models using a matrix.

Use prioritization to identify the best or most profitable offer for each customer, and to experiment with different parameters to see how each affects your bottom line.

Use optimization to identify the best or most profitable dimension for each entity within certain constraints. In other words, optimization defines the best way that entities, such as customers or claims, can be allocated to dimensions, such as offers or channels. The goal of optimization is to identify the solution that best meets a specific goal, such as minimizing the risk of fraud.

For applications that use a matrix, the best decision is determined by combining the aggregated results from multiple rules or models or both. Business rules and models may return a different result. For example, the rule may say to fast track a claim while the model says to refer it to a special investigation unit. By combining the two methods, any biases inherent in one may be balanced by the other so that you can make the best decision for each claim. You can use the matrix to specify how each combination is handled.

For more information

See the following product documentation:

- IBM Analytical Decision Management documentation (http://www-01.ibm.com/support/docview.wss?uid=swg27024118)
- IBM Operational Decision Manager Information Center (http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp)
- IBM SPSS Modeler Information Center (http://pic.dhe.ibm.com/infocenter/spssmodl/v15r0m0/index.jsp)

IBM products used in the detection phase

Several IBM products are used in the detection phase.

IBM Analytical Decision Management
Use IBM Analytical Decision Management version 7.0 in combination with predictive analytics, local rules, and scoring to deliver recommended actions in real time, which helps you to make the right business decisions about fraudulent activity. This component automates and optimizes transactional decisions based on known characteristics and this enables known high-risk activity patterns to be detected as they occur.

For more information, see the IBM Analytical Decision Management documentation (http://www.ibm.com/support/docview.wss?uid=swg27024118).

IBM Case Manager

Use IBM Case Manager version 5.1.1 to simplify the delivery of case management solutions. IBM Case Manager unites content, process, and people to deliver optimized case outcomes through analytics, rules, collaboration, and social computing.

For more information, see the IBM Case Manager Information Center (http://pic.dhe.ibm.com/infocenter/casemgmt/v5r0m0/index.jsp).

IBM Cognos Business Intelligence

Use IBM Cognos Business Intelligence version 10.2.0 to analyze key indicators in dashboards and reports.

For more information, see the IBM Cognos Business Intelligence Information Center (http://pic.dhe.ibm.com/infocenter/cbi/v10r2m0/index.jsp).

IBM i2 Intelligence Analysis Portfolio

Use IBM i2 Intelligence Analysis Portfolio version 1.0.5 to identify patterns, links, and relationships from vast, disparate data sets enabling you to rapidly identify and disrupt fraud.

For more information, see the IBM i2 Intelligence Analysis Portfolio Information Center (http://pic.dhe.ibm.com/infocenter/i2iap/v8r9m1/index.jsp).

IBM InfoSphere Identity Insight

Use IBM InfoSphere Identity Insight version 8.1 to investigate and visualize relationships and to resolve identities.

For more information, see the IBM InfoSphere Identity Insight Information Center (http://pic.dhe.ibm.com/infocenter/easrr/v8r0m0/index.jsp).

IBM Integration Bus

IBM Integration Bus version 9.0 ties activities together through orchestration, reliably exchanging related fraud information and mediating information content to capture pertinent information content.

For more information, see the IBM Integration Bus Information Center (http://pic.dhe.ibm.com/infocenter/wmbhelp/v9r0m0/index.jsp).

IBM Operational Decision Manager

Use IBM Operational Decision Manager version 8.0 to enable your business to respond to real-time data with intelligent, automated decisions. IBM Operational Decision Manager provides a business rules management system that is easy to evolve, trace, audit, and test.

For more information, see the IBM Operational Decision Manager Information Center (http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp).

IBM SPSS Collaboration and Deployment Services

Use IBM SPSS Collaboration and Deployment Services version 5.0 to manage analytical assets, automate processes, and efficiently share results widely and securely.

For more information, see the IBM SPSS Collaboration and Deployment Services Information Center (http://pic.dhe.ibm.com/infocenter/spsscads/v5r0m0/index.jsp).

IBM SPSS Modeler Premium

Use IBM SPSS Modeler Premium version 15.0 to predict the outcome of future events and interactions by discovering hidden relationships in databases, flat files, unstructured data, or your Cognos Business Intelligence environment. Entity analysis helps you to combine and resolve the structured and unstructured data to improve model accuracy. Social network analysis helps you discover relationships among social entities and the implications of their behavior.

For more information, see the IBM SPSS Modeler Information Center (http://pic.dhe.ibm.com/infocenter/spssmodl/v15r0m0/index.jsp).

IBM SPSS Statistics

Use IBM SPSS Statistics version 21.0 to address the entire analytical process, from planning to data collection to analysis, reporting and deployment.

For more information, see the IBM SPSS Statistics Information Center (http://pic.dhe.ibm.com/infocenter/spsstat/v21r0m0/index.jsp).

IBM WebSphere® Message Queue

IBM WebSphere Message Queue version 7.5 acts as the information transport between the components of the IBM® Counter-Fraud Management solution. It provides a rapid, reliable, and secure transport of messages and data between applications, systems, and services.

For more information, see the IBM WebSphere Message Queue Information Center (http://pic.dhe.ibm.com/infocenter/wmqv7/v7r5/index.jsp).

Chapter 5. Prevention

In the prevention phase, apply the results of the detection phase to stop newly-detected fraud, or to encourage fraudsters to abandon their planned schemes by showing that you know more about the scheme than they think.

At the end of each investigation, identify how the fraud alert workflow model can be enhanced to detect and prevent future fraudulent activities. Add new business rules and scoring directives or enhance the existing ones.

Enhancing the model and business rules

At the end of each investigation, it is typical for a Special Investigations Unit (SIU) to conduct a post-mortem review of the investigation. The team identifies additional business rules and scoring directives to be placed on the fraud alert workflow model to detect and prevent future activities.

Each investigation provides more information that might need to be captured in new business rules or in changes to the rules and models.

For example, you add additional questions to be presented to intake agents so that new work is routed to the correct business process.

For more information

See the following product documentation:

- IBM Content Analytics with Enterprise Search Information Center (http://pic.dhe.ibm.com/infocenter/analytic/v3r0m0/index.jsp)
- IBM Operational Decision Manager Information Center (http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp)
- IBM SPSS Modeler Information Center (http://pic.dhe.ibm.com/infocenter/spssmodl/v15r0m0/index.jsp)

Related concepts:

Chapter 2, “Discovery,” on page 3
By continuously comparing customer, account, or transaction data to the data of cases that are known to be fraudulent, you can discover suspicious transactions prior to payment while continuing to pay valid transactions quickly and with greater certainty.

Reviewing alerts for quality, accuracy, and timeliness

Periodically, alerts need to be reviewed for quality, accuracy, and timeliness.

A sample of recently completed alerts is selected for review. For example, a weighted sampling method can be used to ensure that 75% of the sample consists of alerts that were closed by new employees.

A quality control auditor uses IBM InfoSphere Identity Insight to review and analyze the work that was done by anyone who worked on and closed the alert. The alert details, related entities, comments added by investigators and analysts, and associated entities or alert graphs are all reviewed.

If the alert remains valid and accurate, this information is included in a comment and the review is closed. If issues are discovered, the alert is referred back to an analyst or manager for correction.

For more information

See the following product documentation:

- IBM InfoSphere Identity Insight Information Center (http://pic.dhe.ibm.com/infocenter/easrr/v8r0m0/index.jsp)

Related concepts:

"Alerts" on page 25
Alerts are messages or other indicators that signal that an event has occurred. Attribute alerts are generated whenever entities match a specified collection of attributes. Role alerts are generated whenever linked entities share roles that you define as being interesting or conflicting.

Re-scoring customers

When an approved change is made to a scoring model, the system determines which customers must be re-scored.

Changes are not immediately put into use in the live, or production, scoring processes. Rather, you work with a copy of the current live model in IBM SPSS Modeler. When you have made all necessary changes, analyses are performed on the changes to confirm that the changes do not cause any logic conflicts which would corrupt or break the model and to estimate the impact of the changes. You review and confirm the changes. The model can then be moved into production and customers are re-scored.

For more information

See the following product documentation:

- IBM SPSS Modeler Information Center (http://pic.dhe.ibm.com/infocenter/spssmodl/v15r0m0/index.jsp)

Related concepts:

"Scoring a model" on page 26
To score a model means to apply it to some data or a population in order to obtain a result or prediction that can be used as input to decisions.

IBM products used in the prevention phase

Several IBM products are used in the prevention phase.

IBM Cognos Business Intelligence
Use IBM Cognos Business Intelligence version 10.2.0 to analyze key indicators in dashboards and reports.

For more information, see the IBM Cognos Business Intelligence Information Center (http://pic.dhe.ibm.com/infocenter/cbi/v10r2m0/index.jsp).

IBM Content Analytics with Enterprise Search
Use IBM Content Analytics with Enterprise Search version 3.0 to search unstructured data, such as documents, reports, email, surveys, and applications and to find new actionable insights. The combination of content analytics and enterprise search capabilities can help you

understand the meaning and context of human language to make fact-based decisions in areas such as crime intelligence, insurance claims, and patient care.

For more information, see the IBM Content Analytics with Enterprise Search Information Center (http://pic.dhe.ibm.com/infocenter/analytic/v3r0m0/index.jsp).

IBM InfoSphere Identity Insight

Use IBM InfoSphere Identity Insight version 8.1 to investigate and visualize relationships and to resolve identities.

For more information, see the IBM InfoSphere Identity Insight Information Center (http://pic.dhe.ibm.com/infocenter/easrr/v8r0m0/index.jsp).

IBM Operational Decision Manager

Use IBM Operational Decision Manager version 8.0 to enable your business to respond to real-time data with intelligent, automated decisions. IBM Operational Decision Manager provides a business rules management system that is easy to evolve, trace, audit, and test.

For more information, see the IBM Operational Decision Manager Information Center (http://pic.dhe.ibm.com/infocenter/dmanager/v8r0m1/index.jsp).

IBM SPSS Modeler Premium

Use IBM SPSS Modeler Premium version 15.0 to predict the outcome of future events and interactions by discovering hidden relationships in databases, flat files, unstructured data, or your Cognos Business Intelligence environment. Entity analysis helps you to combine and resolve the structured and unstructured data to improve model accuracy. Social network analysis helps you discover relationships among social entities and the implications of their behavior.

For more information, see the IBM SPSS Modeler Information Center (http://pic.dhe.ibm.com/infocenter/spssmodl/v15r0m0/index.jsp).

Chapter 6. Case study: Property and casualty claim fraud

This case study describes an organized scheme to defraud an insurance company and how the insurance company used IBM® Counter-Fraud Management to discover and stop the fraud scheme.

Staged accidents fraud scheme

The scheme is to stage or cause accidents and then make a claim with an insurance company.

Who is involved in the scheme?

All names in this case study are fictitious. Any similarity to actual people or companies is entirely coincidental.

The following people are involved in the scheme:

Charles Morrison
Charles Morrison is the organizer of the scheme. He is a tow truck operator and owns the company Fulltime Towing and Transport. The company consists of one tow truck and does not have a physical address. He uses carbon paper documents for receipts and billing.

He realizes that he could defraud auto insurance carriers by staging or causing accidents and making claims. By carrying out these false claims, he learns which questions are asked, which documents are needed, how to use fake or altered names and addresses, and what types of accidents are best for subtle claims with little to no detection from his point of view.

He enlists his girlfriend and other friends to help.

Jessica Smythe
Jessica Smythe is Charles Morrison's girlfriend. She actively assists in staging accidents and uses her name for a variety of roles such as driver or witness. She also handles various financial aspects of the schemes, including the group's bank accounts.

Li Li is a friend of Charles Morrison. He resides in an apartment behind Charles's residence. He actively assists in staging accidents and uses his name for a variety of roles.

Juan Juan is an associate of Charles Morrison. In a number of the schemes, he locates damaged vehicles through his employment at an auto body repair facility. He actively assists in the schemes and uses his name for a variety of roles.

What is the scheme?

Charles Morrison purchased two insurance policies from the Number One Insurance Company as well as other policies from a variety of insurers. He purchased all of the policies either over the phone or the internet. He used several names, such as Charles Morris, Charlie Morrison, and Chuck Morrison. Initially he used one debit card to pay for the policies but later he used different pre-paid and restock credit cards or cash delivery services.

The group initially used their own vehicles to stage or cause accidents. However, the scheme's success has resulted in the group upgrading their own vehicles and they did not want to damage these new vehicles. The group decided to purchase vehicles exclusively for using in the scheme. They purchased damaged or salvaged vehicles, which were very cheap to acquire.

The common elements of the scheme are:

- The accidents all occur within a localized regional area.
- The accidents occur between midnight and three in the morning.
- All of the accidents have a police report.
- Most accidents involve only one person in the vehicle and no injuries. Later the group realized that they will get larger settlements if they make injury claims.
- All of the accidents are considered "Not at Fault" claims.
- All of the accidents involve a phantom vehicle or hit and run.
- Theft claims are perpetuated with vehicles that have mechanical defects and cannot run.
- All of the theft recoveries are total burns.

The most recent claim

Juan calls Charles to tell him that there is a damaged vehicle for sale for $3000 at his body shop. The vehicle has a value of $13,000. The vehicle is very damaged, including a broken axle.

Charles researches the history of the vehicle before he buys it and discovers that it was a rental vehicle with a clean title. He gives Jessica a pre-paid credit card and she purchases a policy from Number One Insurance Company as Jessie Smith.

Charles, Jessica, and Li use the tow truck to haul the vehicle to a secluded area where they cause additional damage. They collect the loose pieces that fall off. At night, they tow the vehicle to a dark street with light traffic where they leave the vehicle and throw the loose pieces of the vehicle on the ground. Jessica, using the alias Jessie Smith, calls the police from the scene.

The police arrive and interview her about the accident. The accident report states that Jessie was driving when another vehicle crossed the middle line and struck her vehicle. The other vehicle then drove away and the only identification from Jessie is that it was a black pickup. Jessie phones Li to pick her up and he arrives before the police leave. The police officer notes Li's name in the accident report. The vehicle is then towed away by the police.

Jessie phones Number One Insurance Company the next day with a very general description about the accident.

What the insurance company does

The Number One Insurance Company recently implemented IBM® Counter-Fraud Management to enable a consistent perspective of fraudulent activity throughout the different departments of the business. The company chooses the Discovery entry point for their fraud analysis because some custom analysis is already available. Improvements in this existing analysis will drive efficiency improvements in the Special Investigations Unit (SIU), whose work has been growing due to an increasing number of referred cases.

Special Investigations Unit

All names in this case study are fictitious. Any similarity to actual people or companies is entirely coincidental.

The Number One Insurance Company is an automobile insurance carrier in New Jersey, United States, and has insured Charles Morrison and some of his friends with two policies.

The following people are in the team that discovers and stops the fraud scheme:

Toshiro, the Special Investigations Unit Manager
Toshiro manages the multi-state special investigation function for the claims department, trains adjusters in fraud awareness, and coordinates with claims and legal personnel on litigated cases.

Giancarlo, the Special Investigations Unit Investigator
Giancarlo organizes, performs, and tracks the investigation of claim activity that involves policy coverage issues and suspected fraud. Giancarlo spends 50% of his time in a car driving to various locations to collect evidence and perform field investigations and inspections. He reports the status and results of his investigations to adjusters and pertinent third parties on a regular basis according to established deadlines.

Tatiana, the Special Investigations Unit Analyst
Tatiana supports the department's research, analysis, and presentation of information. She defines and executes an analytical strategy for providing reactive investigative data support in all assigned conventional and complex fraudulent claims fraud through the use of specialized analytical tools, data mining, analysis, and electronic claims file review.

Discovery

The analysts in the Number One Insurance Company build and update models, business rules, and alerts in IBM® Counter-Fraud Management. The models, rules, and alerts draw on information from custom batch analysis that runs overnight. When they are investigating claims, investigators and managers throughout the company use this enhanced information set.

Last week Tatiana closed an investigation of a small staged-accident ring that involved recently-purchased used vehicles. She will update the model with this information, build a data stream that includes a new business rule and a decision table, and build alerts to notify Special Investigations Unit (SIU) managers and analysts of potential fraudulent activity.

Updating an existing model

Tatiana wants to update the company's model with information from an investigation that was recently concluded.

She logs on to IBM SPSS Modeler Premium with her assigned username and password. She searches for and selects the data source that contains her relevant historical claims data. Tatiana selects the appropriate data items. She normalizes several pieces of data by applying transformations so that they have similar means and standard deviations. She adjusts some settings on the data, such as specifying how to handle missing values, and then merges the new data into the model.

She updates the existing predictive model and verifies that the results are accurate. She notices a discrepancy in the data: red, maroon, dark red, and rouge are listed as separate colors. She normalizes these colors to use the same code and builds the model again.

She saves the revised model to the repository in IBM SPSS Modeler Premium. The model is now available for other analysts to use.

Building a new data stream

Tatiana creates a new data stream that results in actionable data. She creates a new business rule and its outcomes.

She uses the Decision Center Business console of IBM Operational Decision Manager to create a new stream. She selects the data source that contains the appropriate claims data. She creates a new business rule to highlight recently-purchased used vehicles.

She creates a decision table for the new business rule and specifies several criteria from the system. She assigns risk point values to the new rule, and allocates an action to each potential risk sum. She sets any sum of six or more points to be immediately sent to a manager.

Tatiana looks at the resulting decision table and verifies that the claims are being routed correctly. She sees that the forecast is for a 20% increase in claims routed to a manager that include recently-purchased used vehicles. Finally, she deploys the new stream to the production environment so that other analysts in her team may now use it.

Building alerts

Tatiana wants to create a new automated email alert for the SIU team.

She uses IBM Cognos Business Intelligence to create a new report. She selects a claims data source and then chooses the appropriate data items: date that the vehicle was purchased, year of the vehicle, date of the accident. She also adds a map to the bottom of the report that shows the general area of the claim.

She sets the report delivery requirements to generate an email alert as soon as a new or updated claim is entered in the database. She specifies the subject of the email to be “Questionable Used Vehicle Claim Alert”. Tatiana designates the recipient of the alert to be based on geography (zip code). She adds a map that highlights the location of the claim. She previews the report's final layout and publishes the new alert.

Investigation

The Special Investigations Unit (SIU) is ready to investigate Jessie Smith's claim further. The manager processes the alert, reviews the referral, and assigns it to an investigator and analyst. Team members analyze and investigate the claim and then work with their manager to prepare a case for adjudication or prosecution.

Processing the alert

Toshiro is a manager with the Special Investigations Unit (SIU) at the Number One Insurance Company.

He receives an email alert that details a new claim with a high risk score. The alert includes a geographic map of where the participants of the claim reside. Toshiro has been monitoring the area because a recent claim was proven to be orchestrated by an organized group filing false claims with several carriers.

He opens the email and reviews the attached report that contains the appropriate criteria. He logs in to IBM Case Manager and verifies that the data is accurate. After reviewing the file, he discovers that the driver and passenger are residing in an area that is close to the participants in another proven fraud ring. He forwards the email to Giancarlo, an SIU investigator.

Management review and assignment

After Tatiana completes an initial review and investigation, she refers the claim to Toshiro so that he can review the claim's new data.

Toshiro logs on to IBM Case Manager. He sees a new message attached to the referral, opens it, and reviews the content. He clicks a hyperlink that opens the case. Toshiro reviews several of the work products that were created by Tatiana: address history, link analysis chart, and prior claims synopsis. He decides that it is time to assign an investigator to this case.

He creates some notes regarding his actions and assigns the case back to the original SIU analyst and also to Giancarlo, the SIU investigator (based on geography). Upon exiting IBM Case Manager, he is prompted to update the case status.

Processing the referral

Giancarlo is an investigator with the Special Investigations Unit (SIU) at the Number One Insurance Company. He has just arrived at work in the morning and has one hour to prepare before he must travel to interview his next person.

He logs on to IBM Case Manager and views a list of his current and historical cases. He sees that he has been assigned to three new cases and opens the one with the highest risk score. He begins to review the facts of the referral. The driver, Jessie Smith, reported that her vehicle was totaled in a hit-and-run accident.

Before he leaves the office, Giancarlo changes the status of the case to “Open Investigation”, saves it, and exits the system.

Additional investigation and analysis

Tatiana’s manager, Toshiro, just sent her an assignment to conduct further investigation and analysis on an open case.

She logs on to IBM Case Manager and opens the newly assigned referral. She reviews her manager's notes, and the associated work products, such as address history, link analysis chart, and prior claims synopsis.

She phones Giancarlo, the assigned SIU investigator. Tatiana tells Giancarlo that she found a previous claim for Jessie Smith where there was a witness to the accident, Elizabeth Mason. She recommends that Giancarlo contact the witness and obtain a statement. Giancarlo agrees. He then recommends that Tatiana locate any claims from other carriers that may be associated with Jessie Smith, Elizabeth Mason, or the friend who picked up Ms. Smith, Li.

Tatiana creates some notes regarding her actions. Upon exiting IBM Case Manager, she is prompted to update the case status.

Field investigation

Giancarlo's manager, Toshiro, sent him an assignment for further investigation.

Giancarlo logs on to IBM Case Manager and opens the newly assigned referral. He reviews his manager's notes and the associated work products for address history, the link analysis chart, and the prior claims synopsis.

He interviews Jessie and Li; he notes that they live in adjoining apartment buildings. During the interviews, they both indicate that they met each other about one month ago and Giancarlo discovers several inconsistencies regarding the loss facts and the sequence of events on the night of the accident. During the interview, Tatiana emails Giancarlo information indicating that Jessie and Li are listed on several prior claims under different names. Giancarlo presents the information to Jessie and Li and they both deny any prior involvement and stress that they have only recently met.

Tatiana uses IBM InfoSphere Identity Insight to gather several key pieces of evidence, such as all the insurance policies are linked to the same computer that is owned by Charles Morrison and that all of the parties in the claims either reside or work together. Giancarlo and Tatiana analyze internal data, external data, and public records, and create a link chart to establish the relationships among all the involved parties in the claims. Giancarlo interviews Jessie and Li again and they both deny that they know Charles Morrison. During this second interview, their recollection of the accident changes again and they admit knowing each other for several years.

Giancarlo is able to locate and interview Elizabeth Mason, the witness listed in a past claim that Tatiana found. In this interview, the witness states that the accident was caused by Mr. Morrison's tow truck backing into a red Cadillac. The witness also provides a statement that Mr. Morrison came to her home and offered to pay her $500 to not talk to anyone about the accident; however she did not take the money because she knows that insurance fraud is illegal.

Giancarlo attempts to schedule a third interview with Jessie and Li. However, this time, Jessie refuses to meet with him and indicates that she wants to drop the claim because she will just pay for the damage out of her own pocket. Li refuses to return any of Giancarlo's phone calls. As a follow-up, Giancarlo tries to interview Charles Morrison who agrees to talk over the phone only. Charles indicates that he only knows Jessie and Li from around the neighborhood, but he has never talked to them. He denies having any knowledge of their accident and he states that he has never been in any accidents.

Tatiana and Giancarlo prepare the work products and evidence in order to refer the claims to the appropriate authorities. This includes an executive summary, all claim documents, videos, audio recordings, and all investigative documents and visuals. Tatiana refers the case to the state's Department of Insurance and to the National Insurance Crime Bureau (NICB) for further investigation and prosecution.

Through the diligent and thorough investigation by Tatiana and Giancarlo, it is discovered that the fraud ring had submitted 50 false claims to 10 companies over the last five years for a total of $750,000 in payments. By quickly identifying the suspicious claims, the Number One Insurance Company did not make any loss

payments. As a result of the investigation, the group was subsequently convicted of insurance fraud.

Detection

Throughout the process of investigating each claim, models and business rules are applied in real time or batch mode to detect possible fraud.

Batch processing of referrals

Overnight, the analytic and decision services processed the rules that are defined for the Number One Insurance Company. The rules are used to automate decisions based on business logic or on the output from predictive models. Actionable referrals are then routed to IBM Case Manager.

In the morning, Toshiro, a manager with the Special Investigations Unit (SIU), receives a referral from the overnight processing. He reviews it in IBM Case Manager and assigns it to Giancarlo, an investigator with the SIU.

Processing a request in real time

Real-time requests are handled by IBM Integration Bus, which routes requests to the appropriate service, orchestrating multi-step analytic tasks to formulate decisions.

During the investigation, Tatiana, an analyst with the SIU, discovers that Jessie is listed on several prior claims. She feeds that information to IBM SPSS Collaboration and Deployment Service in order to get a further score from the external system. After receiving the score, she researches Jessie further and discovers that Jessie and Li are both listed on several prior claims.

Tatiana emails this information to Giancarlo, the investigator on the case.

Detecting relationships between entities

After logging on to IBM Case Manager, Tatiana sees that a new referral has been assigned to her that contains a claim with names that match other open claims.

Tatiana opens the new pending work item and begins her analysis. She reviews the known facts regarding the referral. Tatiana decides to conduct a link analysis and starts IBM i2 Fraud Intelligence Analysis. She views the generated chart and decides to focus on severity.

She conducts some additional analysis of the claimant's address history by looking at several public records. She finds an old Orlando address, and saves it in a spreadsheet. She then imports the new address, merges the data into the existing link chart, and saves it.

Back in IBM Case Manager, Tatiana types some notes about her step-by-step actions regarding the claim. She sends a message to her manager and recommends further investigation. Upon exiting IBM Case Manager, Tatiana is prompted to update the case status.

Prevention

At the end of each investigation, the Special Investigations Unit (SIU) conducts a post-mortem review of the investigation. They identify additional business rules and scoring directives to be placed on the fraud alert workflow model to detect and prevent future activities.

Enhancing the model

Tatiana updates the model with the details of the staged accident fraud, including all the names and aliases of the people involved. For example, she ensures that Charles Morrison, Charles Morris, Chuck Morrison, and Charlie Morrison all correlate to the same person.

She logs on to IBM Case Manager. She sees a new pending work item about a possible matched entity. She opens the work item and begins her analysis. Jessie Smith recently filed a claim and Jessica Smythe was the witness in another claim.

Tatiana then logs on to IBM InfoSphere Identity Insight where she is provided with the match information and other similarities. She reviews the displayed information related to the matched entity that is also similar to other entities within the system. She conducts additional research to verify information such as residencies, vehicles involved, date of birth, and so on to see if it is similar. Tatiana decides that Jessie Smith and Jessica Smythe are the same in both claims, so she reconciles both entities into one.

Back in IBM Case Manager, the system has re-scored the claim, assessed new risk points, and created a new referral.

Appendix. Troubleshooting a problem

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

Review the following table to help you or customer support resolve a problem.

Table 1. Troubleshooting actions and descriptions

Actions	Description
A product fix might be available to resolve your problem.	Apply all known fix packs, or service levels, or program temporary fixes (PTF).
Look up error messages by selecting the product from the IBM Support Portal, and then typing the error message code into the Search support box (http://www.ibm.com/support/entry/portal/).	Error messages give important information to help you identify the component that is causing the problem.
Reproduce the problem to ensure that it is not just a simple error.	If samples are available with the product, you might try to reproduce the problem by using the sample data.
Ensure that the installation successfully finished.	The installation location must contain the appropriate file structure and the file permissions. For example, if the product requires write access to log files, ensure that the directory has the correct permission.
Review all relevant documentation, including release notes, technotes, and proven practices documentation.	Search the IBM Support Portal to determine whether your problem is known, has a workaround, or if it is already resolved and documented.
Review recent changes in your computing environment.	Sometimes installing new software might cause compatibility issues.

If the items in the table did not guide you to a resolution, you might need to collect diagnostic data. This data is necessary for an IBM technical-support representative to effectively troubleshoot and assist you in resolving the problem. You can also collect diagnostic data and analyze it yourself.

Troubleshooting resources

Troubleshooting resources are sources of information that can help you resolve a problem that you are having with an IBM product.

Support Portal

The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services.

The IBM Support Portal lets you access all the IBM support resources from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself

with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos).

Find the content that you need by selecting your products from the IBM Support Portal (http://www.ibm.com/support/entry/portal).

Before contacting IBM Support, you will need to collect diagnostic data (system information, symptoms, log files, traces, and so on) that is required to resolve a problem. Gathering this information will help to familiarize you with the troubleshooting process and save you time.

Service request

Service requests are also known as Problem Management Reports (PMRs). Several methods exist to submit diagnostic information to IBM Software Technical Support.

To open a PMR or to exchange information with technical support, view the IBM Software Support Exchanging information with Technical Support page (http://www.ibm.com/software/support/exchangeinfo.html).

Fix Central

Fix Central provides fixes and updates for your system's software, hardware, and operating system.

Use the pull-down menu to navigate to your product fixes on Fix Central (http://www.ibm.com/systems/support/fixes/en/fixcentral/help/getstarted.html). You may also want to view Fix Central help.

IBM developerWorks®

IBM developerWorks provides verified technical information in specific technology environments.

As a troubleshooting resource, developerWorks provides easy access to the most popular practices, in addition to videos and other information: developerWorks (http://www.ibm.com/developerworks).

IBM Redbooks®

IBM Redbooks are developed and published by the IBM International Technical Support Organization, the ITSO.

IBM Redbooks (http://www.redbooks.ibm.com) provide in-depth guidance about such topics as installation and configuration and solution implementation.

Software support and RSS feeds

IBM Software Support RSS feeds are a quick, easy, and lightweight format for monitoring new content added to websites.

After you download an RSS reader or browser plug-in, you can subscribe to IBM product feeds at IBM Software Support RSS feeds (https://www.ibm.com/software/support/rss).

Log files

Log files can help you troubleshoot problems by recording the activities that take place when you work with a product.

Error messages

The first indication of a problem is often an error message. Error messages contain information that can be helpful in determining the cause of a problem.

Notices

This information was developed for products and services offered worldwide.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. This document may describe products, services, or features that are not included in the Program or license entitlement that you have purchased.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Software Group
Attention: Licensing
3755 Riverside Dr.
Ottawa, ON
K1V 1B7
Canada

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

Trademarks

IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at " Copyright and trademark information " at www.ibm.com/legal/copytrade.shtml.

Index

A

accessibility v
alerts 15, 25
  insurance case study 37, 38
allocations 8, 28
analysis
  insurance case study 38
  key performance indicators 18
  link 13
  social network 14
  statistical 27
anomaly models 5
applications
  deploying 8
assignments 11
  insurance case study 38
attribute alerts 25

B

business rules 6
  insurance case study 37

C

case study, property and casualty fraud
  actions of insurance company 37
  description of scheme 36
  detection phase 41
  discovery phase 37
  investigation phase 38
  involved parties 35, 37
  prevention phase 42
clustering models 5

D

dashboards
  key performance indicators 18
data sources 3
decision trees 8
decisions
  allocations 28
deploying 8
detection 21
  insurance case study 41
  products 28
discovery 3
  decision trees 8
  insurance case study 37
  products 9

E

entity resolution 22
  alerts 25
  recognize phase 22
  relate phase 24
  resolve phase 23
entity resolution *(continued)*
  roles 24
error messages 43
events 25

F

field investigations 11
fixes 43

I

IBM Analytical Decision Management
  detection phase 28
  discovery phase 9
IBM Case Manager
  detection phase 28
  investigation phase 18
IBM Cognos Business Intelligence
  detection phase 28
  investigation phase 18
  prevention phase 32
IBM Content Analytics with Enterprise Search
  discovery phase 9
  prevention phase 32
IBM developerWorks 43
IBM i2 Intelligence Analysis Portfolio
  detection phase 28
  investigation phase 18
IBM InfoSphere Identity Insight
  detection phase 28
  investigation phase 18
  prevention phase 32
IBM Integration Bus
  detection phase 28
IBM Operational Decision Manager
  detection phase 28
  discovery phase 9
  prevention phase 32
IBM Redbooks 43
IBM SPSS Collaboration and Deployment Services
  detection phase 28
  discovery phase 9
IBM SPSS Modeler
  detection phase 28
  discovery phase 9
  prevention phase 32
IBM SPSS Statistics
  detection phase 28
  discovery phase 9
IBM WebSphere Message Queue
  detection phase 28
identities 13
  alerts 15
investigations 11
  insurance case study 38
  products 18

K

key performance indicators 18

L

link analysis 13
log files 43

M

management
  assignments 11
models
  anomaly 5
  insurance case study 37
  predictive 4
  scoring 26
  training 6

P

phases
  detection 21
  discovery 3
  investigation 11
  prevention 31
predictive models 4
  deploying 8
  scoring 26
  training 6
prevention 31
  insurance case study 42
  products 32
problem management reports 43

R

referrals
  insurance case study 38
relationships 13, 24
relationships *(continued)*
  alerts 15
reports
  key performance indicators 18
role alerts 25
roles 24
rules 6
  insurance case study 37

S

scoring
  models 26
service requests 43
social network analysis 14
software support and RSS feed 43
solutions
  designing 11
statistical analysis 27
streams
  deploying 8
support portal 43

T

training
  predictive models 6
troubleshooting 43
  identifying problems 43

W

workflow 1