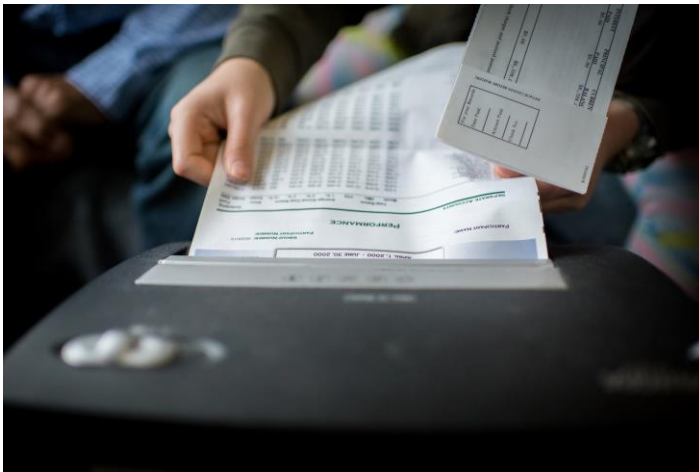


Why More Data is Not Enough

In today's digital environment, applicants and agents expect carriers to instantly provide bind-able quotes. And most of these quotes are created in virtual environments – with no in-person or a phone interview by an agent. And so there's often no 'human' interaction that might pick verbal or oral queues that suggest dissembling or misrepresentation. Instead, carriers are forced to rely on third-party data to develop and offer pricing, coverages and terms. Both in pre-fill and then again throughout the policy lifecycle. The industry has been doing this for over a decade – and the importance of third-party data in decisioning is becoming even more important in the age of Covid and remote work.

But is this always good idea? Should carriers simply accept third-party data to write risks? Are there exceptions? When should carriers buy even more data? Let's think about this for a minute.



Data Problems are Deeper Than You Might Think

At VeracityID, we've looked at millions of carrier and third-party records. What we find is that most third-party data is reliable when it's available. But depending on the region, vendor and customer type, anywhere from 10-30% of requests for data aren't filled. And in 10-15% of cases where data is returned, there are conflicts and inconsistencies between customer representations, carrier records and vendor data sets. Yet most carriers feel compelled to quote despite partial, conflicting or incomplete data.

We've found that data inconsistencies and errors can result in elevated mispricing (rate evasion costs auto carriers up to 20% of NPW; with average lost premium of around \$400 per instance) and increase the likelihood of both underwriting & claims fraud.

VeracityID Fights Underwriting Fraud

Undisclosed Drivers. Pre-Existing Damage. Rating Address Misrepresentation. Corrupted Data. Ineligible Drivers. Serial Cancellers. Unpaid Premium Applications. Commercial Vehicles. Incomplete Data. Salvage Vehicles. Ghost Brokers. Fraud Networks. Vehicles Registered to Unlisted Drivers. Known Fraudsters.

VeracityID Delivers Practical Solutions

Real-Time Quote Monitoring & Intervention. Omnichannel Solutions. API as a Service Vendor Network. Suspicious Connections Detection. Social Network Analytics & Investigations. Customer Lifecycle Event Monitoring. Dynamic Web & Mobile Interview & Data Capture. User-Configurable Boolean Rules Engine. Continuous Risk Monitoring & Scoring. Distributed Cloud Database Analytics Services. Mobile Image Capture & Recognition. GPS & Device Monitoring. Customizable Case Management & Workflow.



Why is There a Such a Big Data Quality Problem?

All data sets have errors. They often start at the beginning of the customer journey with the mis-keying of data (PWC did a famous study years ago that found manual entry of data results in 1 out of 6 records containing errors - and it's still true). These errors are compounded every time a new manual entry is created – in different systems, at different times, over many years. Think about how a claim is taken over the phone – is the right policy owner name entered? Is the address updated properly? Is the person driving the car correctly identified? Are counterparty names and descriptive details entered correctly? Is the record corrected by the adjuster after FNOL?

There are also formatting issues across data sets. Vendor supplied data is often multi-sourced and may not be consistently formatted. And carrier data is often formatted differently across different internal systems. Even carrier accounting treatment and labelling leads to errors – is it a cash, suspense or accrual account? Is it a calculated field or a source record? Who would know – and how can you tell?

Worse, data structures tend to propagate themselves within systems over time – with multiple fields containing similar data being created by different users, building up like sludge in departmental, corporate in cloud service databases. Which data set is current? How and when should I use it? Who would know?

Vendor data has the additional challenges of stale data and data provenance. Vendors generally cannot or will not disclose when data was acquired or its source. As a result, it's extremely difficult to test and evaluate whose data or which data sources are 'best.'

A plain fact of life is that data anomalies abound and data 'clean-up' efforts always fail to keep up. We're all stuck in a 'Master Data Management' Trap from which we cannot escape. No amount of entity resolution or data engineering can totally expunge it. Fraudsters know this – and they do their best to exploit weaknesses it creates in origination and claims services.

Absent an effective response, our industry is tacitly accepting data quality risk by adding 20% to quotes to pay for it.

Does anybody think that's a good idea? What would happen to the market if somebody was able to create automated processes to avoid this problem? What if some carriers are already doing it? Solving this problem is core to what VeracityID does and is addressed at length in the pages that follow.

VeracityID Detects Suspicious Claims.

Known Fraudsters. Fraud Rings. Social Network Connections to Fraudsters. Suspicious Early Claims. Pre-Existing Damage Claims. Suspicious Endorsements & Changes Around Claims. Anomalous Policy & Claims Patterns.

VeracityID Delivers Practical Solutions

Real-Time Quote Monitoring & Intervention. Omnichannel Solutions. API as a Service Vendor Network. Suspicious Connections Detection. Social Network Analytics & Investigations. Customer Lifecycle Event Monitoring. Dynamic Web & Mobile Interview & Data Capture. User-Configurable Boolean Rules Engine. Continuous Risk Monitoring & Scoring. Distributed Cloud Database Analytics Services. Mobile Image Capture & Recognition. GPS & Device Monitoring. Customizable Case Management & Workflow.

Do Data Problems Reveal Fraud or a Screw-Up – Or Nothing at All?

In a virtualized environment, it can be difficult to discern if someone is lying, lazy or just error-prone. Or if the data that created the conflict is just wrong. The customer may be in a hurry to get a quote, the purchased data may be stale or incomplete, a fraudster may be gaming the system, or an agent may be ‘testing’ options to get the best quote. Or something else.

But if you know the data isn’t 100% reliable and you don’t ‘see’ the customer prior to issuing a policy – what do you do? And does it matter in the scheme of things?

The answer is ‘of course’. Carriers use defective data to price risk every day despite knowing about leakage and claims fraud. And the problem is compounded because the magnitude of the exposure can vary widely because the customers attempting deception can have very different objectives. One customer seeking rate may never file a claim because she doesn’t want to get ‘caught’ – but may be willing to submit multiple quotes to explore rate. Another customer looking to get a pre-existing damage claim paid may only submit one ‘clean’ quote – because he wants to get coverage fast and doesn’t care (much) about price. A third customer with a history of suspicious or fraudulent claims may try to ‘hide’ in the data – changing details just enough to get a policy and file another claim. Or an agent may be inexperienced or working in a very competitive market – and feel compelled to game the system. Or some data is just wrong and a policy is misquoted.

A response to these problems needs to countenance each of these scenarios – and put into place workflow that first identifies the underlying indicators of risk and surrounding conditions, and then addresses them thoughtfully at POS and thereafter.

So what can insurance carriers do to reduce the impact of inconsistent, non-existent, misrepresented or incorrect data on financial outcomes without adversely impacting ‘good customers’ or overall sales and profit targets?

VeracityID’s view is that carriers need to fuse and deploy handful of core capabilities into a coherent, consistent approach to identify risks and anomalies, and then act upon them before issuing policies or accepting risks.

- **Identify & Organize All of Your Data**
- **Get the Right Data Toolbox(es)**
- **Operationalize Data Insights**
- **When in Doubt, Ask a Good Question**

VeracityID Fights Underwriting Fraud

Undisclosed Drivers. Pre-Existing Damage. Rating Address Misrepresentation. Corrupted Data. Ineligible Drivers. Serial Cancellers. Unpaid Premium Applications. Commercial Vehicles. Incomplete Data. Salvage Vehicles. Ghost Brokers. Fraud Networks. Vehicles Registered to Unlisted Drivers. Known Fraudsters.

VeracityID Delivers Practical Solutions

Real-Time Quote Monitoring & Intervention. Omnichannel Solutions. API as a Service Vendor Network. Suspicious Connections Detection. Social Network Analytics & Investigations. Customer Lifecycle Event Monitoring. Dynamic Web & Mobile Interview & Data Capture. User-Configurable Boolean Rules Engine. Continuous Risk Monitoring & Scoring. Distributed Cloud Database Analytics Services. Mobile Image Capture & Recognition. GPS & Device Monitoring. Customizable Case Management & Workflow.

Identify & Organize All of Your Data

Carriers have multiple sources of data that can provide insight into possible suspicious behavior. They are also essential when creating a complete picture of the customer journey. But very few carriers capture, retain and organize this data into a holistic customer view, and fewer still are able to operationalize it to make real-time risk decisions.

- **Core Systems Data:** Carrier systems are designed to capture, process and retain transaction quote, policy, claims, billing, investigative and third-party data. These systems – and this data – are organized to price and issue policies, issue bills, process claims and support investigations. But they are not designed or intended to drive ‘analytical’ systems or databases – and so they leave ‘blind spots’.
- **Synthetic/Warehouse Data:** Most carriers have developed a variety of purpose built ‘data warehouses’ that are used to support various analytical, department and audit needs. But they aren’t ‘production systems’, don’t generally have the rigorous controls found in core systems, and aren’t designed to scale in a cloud environment to fuse and manage internal and external data sets dynamically.
- **Third-Party Data:** All carriers purchase third-party data to make decisions – during applications, at point of endorsement, during the underwriting period, at FNOL and beyond. But many don’t retain it, and those that do seldom have it organized to identify risks and drive future decisions.
- **Customer Behavioral Data:** Perhaps the most important information carriers have – but seldom retain or use – is how a customer behaves during a transaction of any kind. Is the customer submitting multiple, conflicting information? Is an databases agent or aggregator ‘gaming’ the system to hide identifies or manipulate rate? Are call center, claims adjuster or SIU staff’s observations captured and leveraged when risk decisions are made? Capture and fusion of digital signals with historical and transaction data –e.g., submission multiple quotes, serial cancellations, payment problems, a prior policy history rife with problems, submission of data that appears to be manipulation (like submitting an insurance policy in my wife’s name or that omits a troubled driver) – can yield powerful insights. If you can operationalize them.

VeracityID’s experience is that all of this data – taken together – can be used to paint a picture of risk that any single component cannot capture. It’s also our finding that about 10% of new business of new business has problems that – if resolved – would reduce loss ratios anywhere from 10-40 points, depending on the channel and customer profile.

Sound interesting?

VeracityID Detects Suspicious Claims.

Known Fraudsters. Fraud Rings. Social Network Connections to Fraudsters. Suspicious Early Claims. Pre-Existing Damage Claims. Suspicious Endorsements & Changes Around Claims. Anomalous Policy & Claims Patterns.

VeracityID Delivers Practical Solutions

Real-Time Quote Monitoring & Intervention. Omnichannel Solutions. API as a Service Vendor Network. Suspicious Connections Detection. Social Network Analytics & Investigations. Customer Lifecycle Event Monitoring. Dynamic Web & Mobile Interview & Data Capture. User-Configurable Boolean Rules Engine. Continuous Risk Monitoring & Scoring. Distributed Cloud Database Analytics Services. Mobile Image Capture & Recognition. GPS & Device Monitoring. Customizable Case Management & Workflow.

It is interesting and potentially of transformational value. But there are a few things in the way:

- Data quality is uneven, at best, even when best-in-class resolution processes are in place
- Good profiles reflect probabilities – not certainties. No system can discern with 100% accuracy what customer intent might be
- The frequency of false positives – and the cost of the elevated risk – need to be balanced into an expected value of action calculation

Furthermore, data analytics aren't the only thing that matters. Other factors need to be considered, including:

- Regulatory response to using models and profiles to make underwriting decisions
- The impact on company reputation of heightened scrutiny on apps
- Agent response to actions that result in abandoned or declined app

What should carriers do?

Get the Right Database Toolbox(es)

The obvious first step is to KNOW what risks are elevated as a result of data anomalies and insights. And to do that you need to be able to answer some basic questions about risk – questions few carrier systems can readily answer today such as:

- How do different combinations of suspicious risk factors impact rate or loss ratio? How much?
- How often does a risk profile generate a false positive?
- How much business will abandon the purchase process if additional underwriting is imposed?
- *What is the expected value of action? Inaction?*

What kind of database toolboxes do carriers need to answer these questions?

Carriers need two broad types of data environments (toolboxes) to tackle these issues. The first is a rich analytical environment that allows carriers to ingest and organize data into a scalable analysis framework. Such a toolbox needs to be able to dynamically pull data from internal sources and cloud services. This rich analytical toolbox needs to be able to look at every aspect of the customer journey, create profiles of like customers, and measure the rate, loss ratio, duration and claims severity/frequency associated with each these profiles.

VeracityID Fights Underwriting Fraud

Undisclosed Drivers. Pre-Existing Damage. Rating Address Misrepresentation. Corrupted Data. Ineligible Drivers. Serial Cancellers. Unpaid Premium Applications. Commercial Vehicles. Incomplete Data. Salvage Vehicles. Ghost Brokers. Fraud Networks. Vehicles Registered to Unlisted Drivers. Known Fraudsters.

VeracityID Delivers Practical Solutions

Real-Time Quote Monitoring & Intervention. Omnichannel Solutions. API as a Service Vendor Network. Suspicious Connections Detection. Social Network Analytics & Investigations. Customer Lifecycle Event Monitoring. Dynamic Web & Mobile Interview & Data Capture. User-Configurable Boolean Rules Engine. Continuous Risk Monitoring & Scoring. Distributed Cloud Database Analytics Services. Mobile Image Capture & Recognition. GPS & Device Monitoring. Customizable Case Management & Workflow.

It should also enable analysts and data scientists to run sophisticated data experiments, develop and deploy machine learning services to discern additional risks, and ultimately to power AI tools that will eventually come to dominate automated underwriting solutions and services.

The second is a production data environment that is pre-organized to identify specific risk types and scenarios in parallel with core systems – and not to support exceptions workflow outside of normal processing.

Sound easy?

It's not. Delivering these capabilities requires organizing and resolving data from multiple sources into a time-lined data set that identifies risk in every transaction. It needs to help carriers understand which policies and quotes are really 'connected' (e.g., are they in the same household) and which are 'related' (e.g., multiple policies are at the same multi-family address). It needs to track a wide range of metrics like policy abandonment rates, unpaid premium balances, underwriting/claims statuses by step in the process, and more. So it needs feeds from multiple production systems into these environments. It's also helpful to have a cloud data augmentation tool so carriers can add more internal or external data to their analyses and during live transactions

But there are new tools to organize, manage and deliver data in a distributed cloud services environment. And there are structured and graph tools emerging than help you identify and associate risks in entirely new ways.

Operationalize Data Insights

Once you have solved your analytical and production data needs, you need an efficient way to operationalize risk insights. That means you need to be able to design, test and deploy risk workflow to address the many challenges you know about, be ready to modify your approach based on results and changing market conditions and modify your approach as risks evolve.

Practically speaking, what does 'operationalize' mean when data quality is a continuing problem and fraudsters are going to take advantage of that insight to get advantage?

- When the quality of data that feeds your decision systems is inconsistent – or worse – you need a solution set that you can update and refine at low cost. A static solution that requires intense IT investment is never going to do the trick.

VeracityID Detects Suspicious Claims.

Known Fraudsters. Fraud Rings. Social Network Connections to Fraudsters. Suspicious Early Claims. Pre-Existing Damage Claims. Suspicious Endorsements & Changes Around Claims. Anomalous Policy & Claims Patterns.

VeracityID Delivers Practical Solutions

Real-Time Quote Monitoring & Intervention. Omnichannel Solutions. API as a Service Vendor Network. Suspicious Connections Detection. Social Network Analytics & Investigations. Customer Lifecycle Event Monitoring. Dynamic Web & Mobile Interview & Data Capture. User-Configurable Boolean Rules Engine. Continuous Risk Monitoring & Scoring. Distributed Cloud Database Analytics Services. Mobile Image Capture & Recognition. GPS & Device Monitoring. Customizable Case Management & Workflow.



- Carriers have invested hundreds of billions in digital transformation in recent years – and still don't have a flexible, low-cost way to operationalize a flexible risk management solution suite or serve. But the cloud allows one to be deployed – without impacting core systems processes or investments – through API's connected to the right kind of data and workflow engine.
- The most effective response to a given risk set may be different by channel, agent, geography and customer demographic. Carriers need tools that allow them to micro-target their responses to the particular conditions of a set of risks – and update them as circumstances and changing conditions warrant.

You may be thinking – *'yeah, but you said the data is often misleading or wrong. You still want to rely on it'*. And you'd be right. All we've done so far is set up a system that allows you to dynamically target your risk identification and response program based on what your data tells you is likely true, and a way to process it. But it doesn't ensure you're doing the right thing.

The last step is to recognize that when you have reason to believe your data may be leading you to make a mistake, your customers, agents and regulators will appreciate it if you do one thing...

Ask them.

When in Doubt, Ask a Good Question

One of the most important things we've seen again and again at Veracity is that most people trying to cheat or lie are unwilling to get caught. And honest people don't mind when asked to explain something on an application or endorsement request doesn't make sense.

In industry parlance, carriers should treat data anomalies and odd behaviors as a 'tip & lead'. Instead of making a firm decision based on potentially flawed data, carriers should engage with the customer or agent, ask probing questions or request relevant data about the anomaly and get them to take action to move the process forward. For example, ask them to sign a relevant attest, update questionable data, take a photo or upload document. Or acquire more data to confirm the truth – and show the customer what you know. Do those and cheating stops – and profits rise.

It's like having a beat cop in your neighborhood, or a camera in the nursery or a set of perimeter lights and alarm on your home. Criminals and wannabe fraudsters don't know what you really know about them – but they do know that getting caught can have high costs. So signal that you see them and what they're doing – and they'll go elsewhere

VeracityID Fights Underwriting Fraud

Undisclosed Drivers. Pre-Existing Damage. Rating Address Misrepresentation. Corrupted Data. Ineligible Drivers. Serial Cancellers. Unpaid Premium Applications. Commercial Vehicles. Incomplete Data. Salvage Vehicles. Ghost Brokers. Fraud Networks. Vehicles Registered to Unlisted Drivers. Known Fraudsters.

VeracityID Delivers Practical Solutions

Real-Time Quote Monitoring & Intervention. Omnichannel Solutions. API as a Service Vendor Network. Suspicious Connections Detection. Social Network Analytics & Investigations. Customer Lifecycle Event Monitoring. Dynamic Web & Mobile Interview & Data Capture. User-Configurable Boolean Rules Engine. Continuous Risk Monitoring & Scoring. Distributed Cloud Database Analytics Services. Mobile Image Capture & Recognition. GPS & Device Monitoring. Customizable Case Management & Workflow.



Does this work? Sounds too good to be true.

Yes it works. In fact this works so well that we took an unprofitable, direct channel book's loss ratio down 40+ points and virtually ended write-off in about a year. And now this thinking is at the core of what we do. If you ask the right question in the right way to the right person during an application – fraud and misrepresentation melts away to negligible levels.

In Conclusion, a Shameless Plug

All you need to do what we described is a scalable, real-time risk analysis, identification and risk resolution system to deliver it. You should call us and ask how we can help you do it.

VeracityID Detects Suspicious Claims.

Known Fraudsters. Fraud Rings. Social Network Connections to Fraudsters. Suspicious Early Claims. Pre-Existing Damage Claims. Suspicious Endorsements & Changes Around Claims. Anomalous Policy & Claims Patterns.

VeracityID Delivers Practical Solutions

Real-Time Quote Monitoring & Intervention. Omnichannel Solutions. API as a Service Vendor Network. Suspicious Connections Detection. Social Network Analytics & Investigations. Customer Lifecycle Event Monitoring. Dynamic Web & Mobile Interview & Data Capture. User-Configurable Boolean Rules Engine. Continuous Risk Monitoring & Scoring. Distributed Cloud Database Analytics Services. Mobile Image Capture & Recognition. GPS & Device Monitoring. Customizable Case Management & Workflow.

About VeracityID

VeracityID is a privately held company. We offer an integrated suite of leading edge, real-time underwriting & claims fraud risk monitoring, detection and intervention solutions for the insurance industry. Learn more about us at www.VeracityID.com or write us at Sales@VeracityID.com.