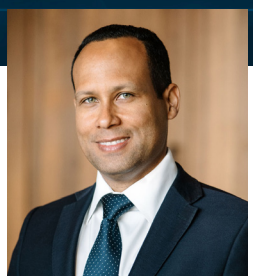
Uncovering Misconduct Hidden in Business Data

OCTOBER 2021



Steven Neuman
Partner, StoneTurn
sneuman@stoneturn.com
+55 11 2844 8311

Patrícia Latorre
Partner, StoneTurn
platorre@stoneturn.com
+55 11 2844 8238

by Steven Neuman and Patrícia Latorre

Would-be fraudsters at public and private companies generally go to great lengths to keep their misconduct hidden from even the most seasoned investigators and internal auditors. Companies and their counsel are therefore increasingly relying upon assistance from data analytics to uncover fraud, waste and abuse before it creates more significant financial and reputational issues down the line.

Forensic reviews of business data, bolstered by data analytics, help to root out misconduct and can increase the efficiency of internal auditors and investigators, allowing business leaders to focus on and more effectively manage identified risk areas. Further, as the world learned from the coronavirus pandemic, effective methods of remote work are critical to business longevity. Even when in-person management oversight is limited, data analytics can often uncover patterns and pinpoint potential issues in ways that even seasoned human auditors cannot.

Similar to the aftermath of the 2008/9 global financial crisis, which saw a

16.8% increase in financial statement fraud during the 2009 recession, multinational organizations should expect increased fraud, waste and abuse to come to light post-pandemic. The good news is that a forensic data analytics approach can also be used to strengthen internal controls for enhanced compliance at this critical time.

Data Analytics Defined

Organizations generate massive amounts of transactional, operational and other business data each day. Data analytics helps to unlock critical insights within that data to effectively mitigate business, legal and regulatory risks. Data analysts combine computer science, mathematics, statistics, problem-solving and technology to better serve companies and counsel. The result is a process of inspecting, cleansing, transforming and modeling data with the goal of discovering useful information and suggesting conclusions to support decision-making.

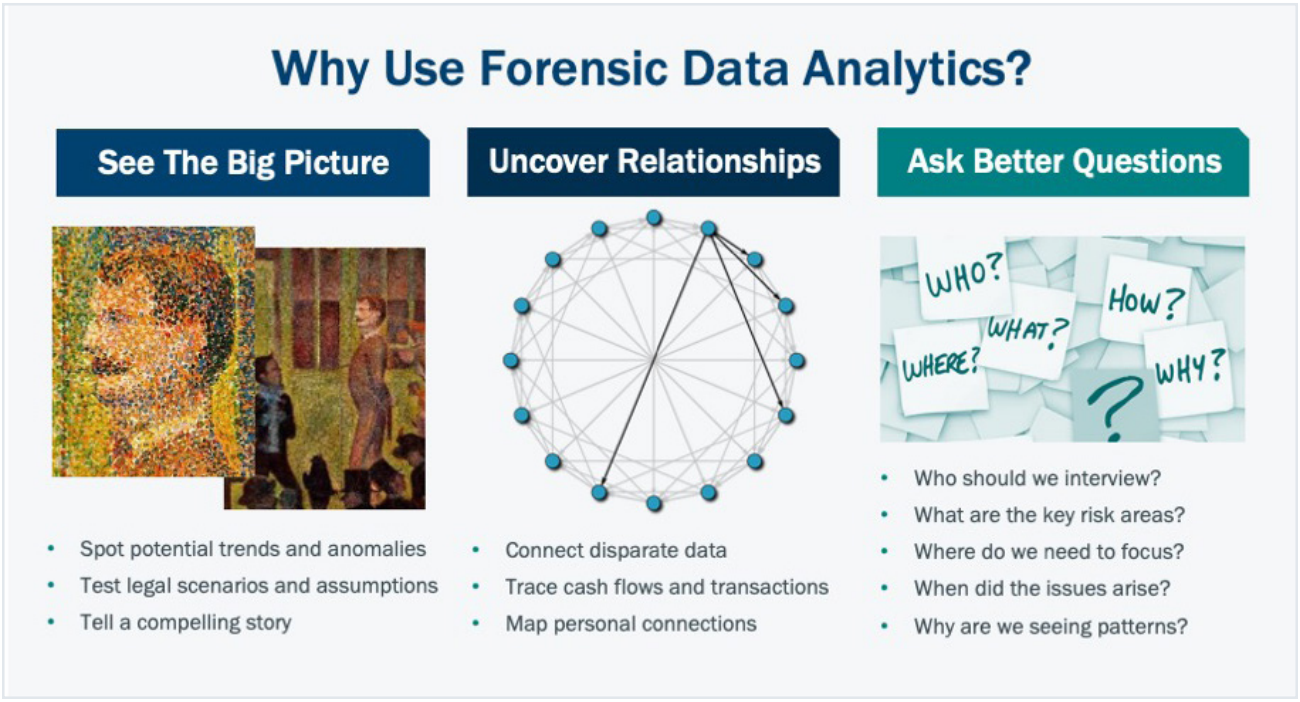
Analysis of both structured and unstructured data is a proven tool for identifying high-risk transactions, individuals, suppliers, customers and third-party relationships. Structured data is highly organized and typically formatted in rows and columns, allowing it to be readily analyzed in relational databases. Conversely, unstructured data does not necessarily have a pre-defined format or organization, which can make it challenging to aggregate, process and summarize efficiently. Examples of unstructured data may include text, video, audio, mobile activity, social media activity, satellite imagery, surveillance imagery, etc. Data analytics can help connect these disparate structured and unstructured data sources, which can then be assessed for meaningful insights.

Because data analytics can potentially uncover that 'needle' in the haystack of data that exists in most organizations, more and more regulators are utilizing data analytics tools to narrow their own focus for regulatory inquiries and enforcement actions. Across every industry and geography, regulators have raised the bar and increasingly expect corporations (and their outside advisers) to employ data-driven methods to prevent, detect and investigate compliance issues.

When Is Data Analytics Most Helpful?

Given that data-driven techniques can be utilized in real-time for useful insights, data analytics can be helpful at every stage of the investigative process. Post-incident, these tools can be leveraged for: data request and extraction, preliminary assessment, detailed analyses and testing (either incident-focused or as part of holistic root cause analysis), as well as the presentation (often via visual modeling) and summary of findings. Pre-incident, data analytics can be used as part of a robust transaction monitoring program for early detection of potential compliance issues, similar to a home smoke detector signaling an issue before a four-alarm blaze erupts.

Whenever it is employed, data analytics aids forensic accountants, compliance professionals and investigative teams in seeing the bigger picture, uncovering relationships and asking the right questions, as illustrated on the following page:



Because these reviews are focused on information, forensic data analytics can help company leadership and their counsel effectively mitigate fraud and abuse even under remote working conditions. Collecting, assimilating and analyzing critical datasets to carry out compliance and/or internal audit procedures can generally be performed virtually to successfully guard against fraud and abuse – whether oversight resources are in short supply overall or spread across a multinational organization's geographic footprint.

Taking Data Analytics a Step Further—Transaction Monitoring

Various data analytics tools such as SQL, R, Tableau, and Python (including TensorFlow, Keras, and scikit-learn packages) are increasingly common in monitoring transactions and assessing potential compliance issues on both a proactive and reactive basis. Whatever approach companies use, transaction monitoring programs— the use of contemporaneous compliance analytics to proactively and reactively identify suspicious business arrangements and/or payments— can quickly identify if an employee engaged (or attempted to engage) in a transaction with an unauthorized third party, for example, provided that the organization maintains approved vendor and customer lists, terminated or denied third-party relationships, and/or high-risk vendors data.

If an organization cannot easily access and query the data fields necessary to identify high-risk transactions, technology-enabled transaction monitoring tools can help in limiting the scope of the investigative team. Outlier transactions that do

not meet pre-defined criteria are automatically elevated for further evaluation. Data analytics can then be employed to review this dataset to limit the number of false positives requiring human follow-up. As an example, payment anomalies identified by transaction monitoring can be assessed via data analytics to determine:

- **Was a due diligence/competitive bid review performed on the vendor prior to transacting with them?**
- **Have third parties charged prices above fair market value? (This may be an indication of a bribe payment).**
- **Are transactions involving government officials being monitored in accordance with country-specific regulations and internal policies?**
- **Have high-risk transactions, such as discounts and commissions, been assessed for reasonableness?**
- **Are big-ticket gifts, charitable event sponsorships or donations being made to politically-exposed persons?**
- **Have consulting fees, service fees or other monies been sent to vendors in order to facilitate third-party payments?**

Conversely, organizations relying on random sampling or other limited data sets when testing internal controls rarely have material findings or implement meaningful enhancements to audit procedures. After all, not all data sources are created equal. Data quality is an essential component of data analytics and transaction monitoring.

We have seen companies rely on local business units to provide information from data sources, which are available to them for purposes of performing their daily tasks. Far too often, however, a system's front-end users are not fully aware of the complexity of the data tables that might only be properly accessible through back-end queries.

This common misstep can create significant risk for the company, such as deriving an audit conclusion based on incomplete or inaccurate information.

Leveraging Transaction Monitoring

Although each organization is different based upon its unique risk profile, the following steps are generally undertaken in creating a successful transaction monitoring program:

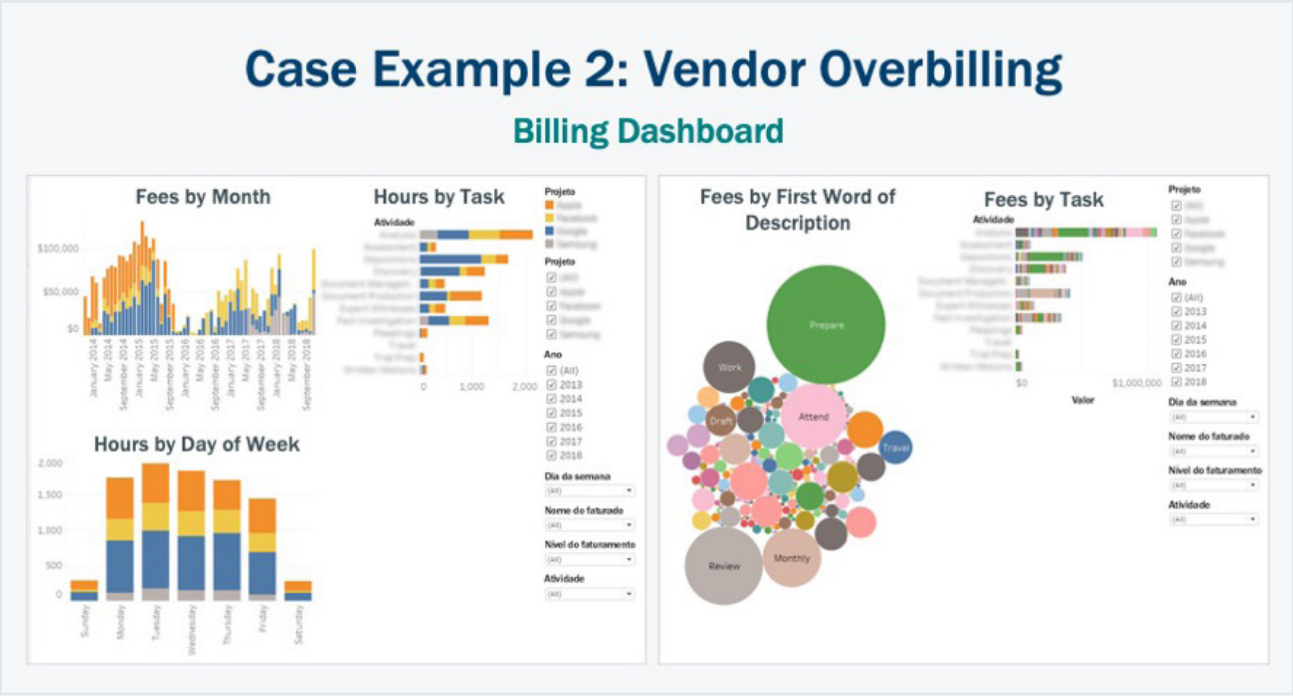
- **Conduct a risk assessment at a business unit- and geographic-level**
- **Use rules-based tests to identify risk indicators**
- **Collect, assimilate and analyze the data, including conducting benchmarking (also referred to as evaluative testing) to compare data sets against averages**
- **Aggregate that information in a useful way to risk-score transactions, vendors, etc.**
- **Design protocols for whether and how to conduct additional investigation**
- **Train resources to investigate and document the response to suspicious transactions**

Consider the real-world scenario (pictured below) which demonstrates how transaction monitoring and data analytics can work seamlessly together. After business leaders raised concerns that a services vendor was over-billing their organization, including duplicate invoices and potential illicit payments through third parties, a team of forensic accountants and data analysts aggregated five years of PDF invoices into a structured database with thousands of time and expense entries. The multidisciplinary team then created both Tableau visualizations of billing patterns and anomalies, as well as performed a detailed review of underlying data for "red flags."

As a result, the analysis identified an individual likely inflating vendor charges by failing to appropriately manage projects. Further, the team found excess fixed charges hidden as time entries and flagged potential duplicative and overlapping charges.

As part of corrective efforts after individuals were disciplined, the same team demonstrated how a vendor payment transaction monitoring framework could be used to strengthen controls. The program would rapidly identify outlier transactions, such as invoices above a certain threshold, as well as any duplicate charges.

Clearly, transaction monitoring tools do not have to be complex to be effective. Compliance leaders are often overwhelmed by where to start when it comes to technology-based enhancements. Starting small can deliver a quick win as well as a roadmap that is repeatable for added value across the enterprise. Of course, for organizations with broader technology appetites, transaction



StoneTurn

monitoring can be utilized to identify not only potential compliance issues but also business and operational insights, trends and other findings that can reign in spending and increase efficiency.

Focusing on FCPA for the Best ROI

While organizations across a range of industries can benefit from customized data analytics and transaction monitoring, compliance practitioners are often asked to demonstrate the 'upside' to the organization or return on investment (ROI) before adopting these measures. In this scenario, anti-corruption efforts often provide the compelling business case needed for multinationals to begin leveraging data analytics or transaction monitoring before robust risk information becomes available.

Enforcement of the Foreign Corrupt Practices Act (FCPA) has long been a high-priority area for the SEC, resulting in a dozen corporate FCPA enforcement actions totaling over $6.4 billion in 2020 – including two of the largest resolutions ever: Goldman Sachs Group, Inc. at $3.32 billion and Airbus Group SE at $2.09 billion. The FCPA prohibits companies issuing stock in the U.S. from bribing foreign officials for government contracts and other business. Of the more than 60 companies charged with FCPA violations by the SEC alone over the past few years, an analysis of prior enforcement actions reveals top risk account categories. Companies should consider assessing these categories and expense types with data analytics and/or transaction monitoring as a priority: General Business Expenses; Consulting; Gifts, Travel and Entertainment; Commissions; and Marketing.

These expense categories were problems for almost all of the companies charged with violating the SEC's books and records provision. Several companies were cited for irregularities in multiple expense categories.

Lack of adequate internal controls is the most common issue for companies that have landed in trouble with the government. In a majority of these matters, the SEC also alleged control violations, with some companies appearing to have no controls at all. Within this context, a variety of control weaknesses were cited that could be mitigated with data analytics and transaction monitoring such as:

- **No program to monitor employee compliance with FCPA regulations;**
- **Lack of, or inadequate, due diligence regarding third-party agents, and a lack of oversight over foreign agents;**
- **Lack of due diligence into internal accounting controls and anti-corruption compliance programs during an acquisition;**
- **Lack of management authorization for transactions.**

An Assist from Data Analytics

Data analytics tools can be used to analyze both quantitative and qualitative fraud and corruption risks so that controls can be enhanced. For example, amidst corruption concerns in the transportation industry, a forensic data analytics team assessed information across a client's disparate business systems to identify high-risk individuals who received free and discounted products and services.

By comparing this data with a registry of Politically Exposed Persons (PEPs), the team was able to quantify any potential benefits provided to PEPs by the client's employees.

It's easy to see how a robust, data-driven approach such as this may have prevented the significantly reduced $4.13 million penalty levied against Telefonica Brasil in 2019 for providing 194 World Cup tickets to 93 officials, and 38 Confederations Cup tickets to 34 officials.

Further, a transaction monitoring framework could maintain more effective oversight of this high-risk area long-term, allowing any company to identify benefits provided to potential PEPs in near real-time.

Best Practices for Uncovering Misconduct

The first step to leveraging data analytics is for the company to understand all sources of data at its disposal (both internally generated and from external third parties), as well as any potential limitations to those sources. This step is critically important to ensure the company has access to relevant information, particularly in large or multinational organizations that may rely on a range of disparate systems.

The company should also conduct periodic audits to help ensure data integrity, meaning that the data is complete, accurate, and there are sufficient internal controls to prevent undocumented alterations or deletions. With this foundation in place, the company can then determine, as the regulator will likely do, how these sources can be best employed using data analytics to enhance the company's compliance program.

A compliance department might also consider applying data analytics in the context of its risk or gap assessments and strengthen both preventive and detective controls. For example, a data analytics model could be used to pressure-test the thresholds of a time-and-expense policy or identify meaningful shifts in spend by category or vendor. Once a potential high-risk area is identified, data analytics could make use of additional models to help determine the potential effect each might have on the business.

A data-driven assessment will help reveal the high-risk areas to consider for pre-incident monitoring, which is an important step in detecting potential misconduct. The compliance department may also consider using targeted predictive analysis as part of its monitoring program to identifying potentially problematic transactions, such as those involving foreign officials or brokers, at or near real-time. This requires a feedback loop so that suspect transactions are identified and supporting data models continuously refined, thereby teaching systems to uncover more of what are confirmed as potential problems.

When potential misconduct has been identified, the pursuant forensic investigation can also be enhanced with data analytics. In many cases, employing an automated, data-driven approach can replace manual review processes that may be otherwise limited by time and resource constraints. These data analytics tools, which include the use of dynamic visualizations and dashboards, will expose patterns and outliers that can bring clarity to a suspected or alleged malfeasance. Achieving a clear trend analysis result is crucial to understanding the scope of the

potential misconduct and developing an action plan for detailed transaction testing.

Importantly, data analytics tools can also help with the sample selection process by allowing a user to quickly and efficiently navigate large amounts of data to pinpoint transactions that meet certain criteria. Again, this step is a key element for completeness, so compliance professionals should make informed selections that will be further investigated to achieve full coverage over the potential misconduct. Compliance practitioners are often responsible for overseeing risk areas that are audited by other functions (finance or internal audit, for example). Transaction monitoring and data analytics can help break down these siloes to enable effective communication between disparate functions.

Following an investigation, a root cause analysis, as well as an internal controls assessment and enhancement, should be carried out to defend against a similar breach. Data analytics can again be applied in this phase to drill down on the original control gap that allowed the misconduct to take place, and then ensure sufficient remediation through controls enhancements and testing.

An interesting application of data analytics is the "look-back capability." This technique makes it possible to determine if the same misconduct would have occurred in a different set of circumstances. For example, a company can test if a new clause in its time-and-expense policy would have prevented or detected an expense fraud scheme from occurring. Such an analysis would provide the compliance department with invaluable insight into the effectiveness of a draft policy and auditing and monitoring processes before putting time and resources into rolling out the requirements companywide.

Conclusion

Companies cannot afford to neglect data analytics. Unlike traditional approaches to compliance and internal audit— which may not be effective during remote working conditions— a data-driven approach helps to uncover and focus resources on red flags to prevent larger issues down the line. Further, the use of data analytics provides the very type of effective and sufficiently sophisticated "surveillance systems" that regulators are keen to see in place. More importantly, data analytics tools can help counsel and in-house professionals conduct investigations more efficiently and allow professionals to focus their time on identified risk areas and addressing potential misconduct to reduce compliance breaches overall.

1 https://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/occupational-fraud.pdf

2 https://fcpablog.com/2020/12/15/getting-to-6-4-billion-2020s-corporate-fcpa-enforcement-actions-ranked-by-size/

3 https://www.reuters.com/article/us-telef-brasil-sec-soccer/u-s-sec-fines-telefonica-brasil-over-world-cup-tickets-idUSKCN1SF2FB

This article originally appeared in Portuguese in **ComplianceLab's 2021 e-book, *Compliance Applied to Law*.**

About the Authors

Steven Neuman, a Partner with StoneTurn, has 20 years of experience advising clients and companies on compliance, risk assessments, global investigations and monitorships. He brings significant expertise in conducting work on the ground in Brazil and throughout the Latin America region, including Argentina, Colombia, Mexico, Peru and Uruguay.

Patrícia Latorre, a Partner with StoneTurn, has 20 years of external audit and fraud investigations experience. Specifically, she is an external audit specialist in fraud risk assessment and prevention procedures. Patrícia has also led and taken part in anti-corruption engagements pertaining to the Foreign Corrupt Practices Act (FCPA) in Brazil, Spain, United Kingdom, Germany, Holland, Belgium, Portugal and Switzerland.