Published by Financier Worldwide Ltd

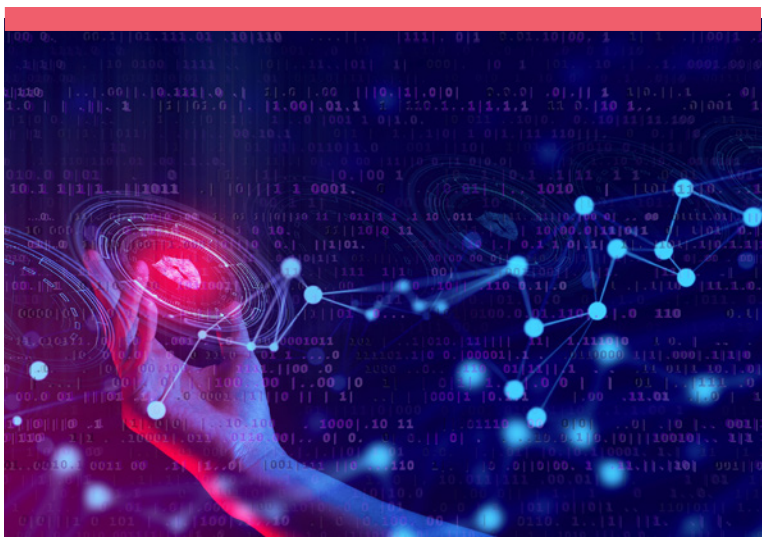
SPECIAL REPORT Q&A **REPRINT** February 2025

Data analytics for fraud detection and prevention

FW discusses data analytics for fraud detection and prevention with Roxanne Wang, Mason Pan and Jared Crafton at BDO USA, P.C.

Q&A: Data analytics for fraud detection and prevention

FW discusses data analytics for fraud detection and prevention with Roxanne Wang, Mason Pan and Jared Crafton at BDO USA, P.C.



THE PANELLISTS

ROXANNE WANG
Senior Manager, Data Forensics
BDO USA, P.C.
T: +1 (312) 730 1384
E: rwang@bdo.com

Roxanne Wang is a forensic data science specialist with over nine years of experience, focusing on developing data-driven solutions for corporate, legal and public sectors to address regulatory and compliance challenges. She has led projects in over 10 countries, advising corporations and government agencies on high-risk issues through advanced analytics. Her investigative experience includes addressing bribery, corruption, asset misappropriation, Ponzi schemes, employee misconduct and beyond.

MASON PAN
Managing Director, Data Forensics
BDO USA, P.C.
T: +1 (202) 644 5444
E: mpan@bdo.com

Mason Pan is a seasoned consultant with over 17 years of experience in data analytics and technology, aiding global corporations in managing critical business events by addressing risks like fraud, financial crime, bribery and corruption. He specialises in forensic analytics, cross-border investigations, and regulatory compliance, helping clients assess and respond to misconduct allegations through data analysis. He employs a risk-based, analytics-led approach tailored to client needs, providing practical solutions for efficient investigations.

JARED CRAFTON
Forensic Technology Practice Leader
BDO USA, P.C.
T: +1 (617) 378 3689
E: jcrafton@bdo.com

Jared Crafton is head of BDO's forensic technology practice, bringing over 20 years of experience advancing the scientific maturity of his client's investigations, compliance programmes and litigation matters. He leads a team in the areas of e-discovery, managed document review, forensic data analytics, privacy & data protection, and data breach advisory services. His personal book of business focuses on forensic data science providing clients with effective strategies for tackling complex data environments with easy to understand analyses and mitigations.

FW: What steps can companies take to improve the effectiveness of data analytics and mitigate some of the downside risks that may arise from its deployment?

Wang: To improve the effectiveness of data analytics and mitigate risks, companies need to ensure source data for the fraud detection model is accurate and complete. Working with teams such as finance, legal and IT will help ensure data is comprehensive and aligned with business needs. It is also important to perform the necessary validations to check data integrity before building an analytics model. Companies also need to avoid bias in their fraud analytics model by ensuring that risk factors are weighted appropriately based on business context and past fraud risks. Skewed results can occur if certain factors are overemphasised or neglected, leading to missed risks or false positives. Regularly reviewing and adjusting the model helps ensure it reflects the full spectrum of evolving fraud threats. Finally, companies should operationalise workflows to act on insights. A clear, structured process for reviewing, escalating and resolving issues ensures timely action on fraud risks, strengthening the compliance framework.

FW: What essential advice would you offer to companies on designing and implementing advanced data analytics techniques to identify patterns, anomalies and potential instances of fraud within their operations? What are the key issues that need to be considered?

Wang: When designing advanced data analytics for fraud detection, companies should begin by assessing where the compliance programme currently stands in its maturity journey. This foundational understanding allows a company to tailor its approach to addressing specific needs and risks. Next, it should incorporate insights from an industry context, past investigations and known compliance risks. For example, in manufacturing, risks

like purchase order fraud may be more critical, while service-based companies may face different challenges that require distinct risk models. Another key element of success is incorporating a feedback loop. Regularly reviewing findings and adjusting the analytics model to reflect new risks, ensures it evolves with the business. Finally, collaboration across legal, compliance, finance and IT teams is essential to align the model with regulatory requirements and drive actionable outcomes.

FW: In your opinion, where does fraud rank among the risks and threats facing businesses today? How have techniques and exploitations grown and evolved in recent years?

Pan: Fraud is a significant risk for global businesses, expanding beyond internal misconduct to include regulatory violations such as export controls, sanctions, price fixing and cyber crime. These areas are increasingly prosecuted by the US Department of Justice (DOJ), reflecting a shift influenced by geopolitical tensions and global competition. Fraudsters are now leveraging artificial intelligence (AI) and generative AI (GenAI) technologies to scale their fraudulent activities, making schemes more sophisticated and harder to detect. This technological edge allows them to automate and enhance traditional fraud methods, such as phishing and social engineering, on a larger scale. Consequently, companies must not only guard against crimes against the company but also comply with complex international regulations and advanced technological threats. The evolving fraud landscape necessitates a proactive and comprehensive approach to risk management, integrating advanced technological defences to stay ahead of these sophisticated threats.

Accurate, complete and timely data forms the backbone of effective fraud detection.

JARED CRAFTON
BDO USA, P.C.

FW: What legal and regulatory requirements are having a significant impact on the fraud risk landscape? How can technology assist companies to achieve and maintain compliance?

Pan: The DOJ's expectations for compliance programmes emphasise using data analytics and AI to proactively detect misconduct. The DOJ's 'Evaluation of Corporate Compliance Programs' highlights the necessity for anti-fraud resources, including compliance and internal audit teams, to access critical data for identifying high-risk behaviours and transactions. Technology aids compliance by enabling transaction monitoring, especially around third parties, to detect fraud and control deficiencies. End-point detection technology is crucial for preventing the exfiltration of sensitive data and intellectual property, thereby safeguarding against trade secret theft. Additionally, communication monitoring and sentiment analysis can identify potential disgruntled employees, providing early warnings of internal threats. By integrating these technologies, companies can enhance their compliance frameworks, ensuring they meet legal requirements while effectively mitigating fraud risks and protecting their assets.

FW: In what ways is data analytics being used in the fight against fraud? What benefits can it provide in detecting and preventing fraudulent patterns or behaviours?

Crafton: There is a long history of analytics and forensic data science being used to fight fraud. By recognising patterns and trends within datasets, analytics

tools can identify anomalies that signal potential fraud. Predictive modelling leverages historical data to forecast fraud scenarios, enabling proactive measures. Real-time monitoring allows for immediate detection and response to suspicious activities, while anomaly detection algorithms flag deviations from normal behaviour for further investigation. Workflow platforms allow for tracking the review of potential anomalies and fraud cases. Machine learning (ML) models can be applied to reviewed cases to continuously improve the accuracy of underlying analytics, learning from new data to better identify fraudulent activities. The benefits are substantial and include increased accuracy in detection, efficiency through automation, proactive fraud prevention, comprehensive insights and enhanced decision making. By harnessing data analytics, companies can protect their assets and reputation, staying one step ahead in the fight against fraud.

FW: How critical is the quality of underlying data to successfully detecting fraud? How should companies go about curating, cleaning and validating data to ensure its accuracy and completeness?

Crafton: In the fight against fraud, the quality of data is paramount. Accurate, complete and timely data forms the backbone of effective fraud detection, enabling precise analysis and anomaly detection. When data is flawed, it can lead to false positives and missed fraudulent activities, wasting resources and potentially causing harm. To ensure data integrity, companies must implement strong data governance frameworks, defining clear standards and responsibilities. Data integration tools help consolidate information from various sources, while cleaning processes correct errors and remove duplicates. Validation techniques, including cross-referencing and anomaly detection algorithms, verify data accuracy. Regular audits and employee training emphasise the importance of maintaining high data standards. Leveraging AI and ML further automates data management and provides the possibility of cleaner data with less effort. By prioritising data quality, companies can significantly improve their ability to detect and prevent fraud, making high-quality data a crucial ally in this ongoing battle.

FW: Looking ahead, how are fraud risks likely to evolve in the months and years ahead? As companies fight back, do you believe data analytics will be integral to their defensive strategies?

Crafton: The proliferation of AI has unlocked new ways to commit fraud, both within companies and from external threats. While fraud schemes generally stay constant, the methods used to perpetrate

The evolving fraud landscape necessitates a proactive and comprehensive approach to risk management.

MASON PAN
BDO USA, P.C.

Regularly reviewing findings and adjusting the analytics model to reflect new risks, ensures it evolves with the business.

ROXANNE WANG
BDO USA, P.C.

these schemes are always evolving. Technologies like deepfakes, GenAI and Agentic AI have empowered fraudsters to expand their reach and execute fraudulent activities on a larger scale. Traditional attacks such as phishing, social engineering and insurance fraud are becoming increasingly sophisticated with the help of technology. In this high-stakes game, those dedicated to preventing fraud must enhance their skills to keep pace with the perpetrators. Fortunately, there are more individuals focused on developing solutions than those creating problems. The fraud analytics industry, with its decades of experience in using AI to combat fraud, stands ready to provide the skills companies need to stay ahead. In this ongoing battle against AI-driven fraud, it is indeed an arms race. However, with the right tools and strategies, companies can maintain an advantage. ■

This article first appeared in the February 2025 issue of Financier Worldwide magazine. Permission to use this reprint has been granted by the publisher.