Key Challenges in White Collar Crime Investigations

More than one-third of businesses in the U.S. are affected by white collar crime and studies have estimated that approximately 40% of large organisations in Europe have been impacted[1]. Fraud, embezzlement, money laundering, insider trading, financial misstatement and intellectual property theft cause annual losses estimated at up to US$1.7 trillion. In recent years, there have been some significant developments in the prosecution of white collar crimes globally, with enforcement activity increasing by more than 50%[2].

The European Commission, U.K., Germany and France have all been increasingly active in their efforts to curb acts of bribery, corruption, money laundering and sanctions violations and more. Amid this increasing regulatory scrutiny, and given the significant financial and reputational damage caused by corporate misconduct, organisations must be proactive in establishing efficient and defensible processes for the corresponding investigations.

Often, seemingly low stakes internal investigations into suspected misconduct quickly escalate by revealing violations of the Foreign Corrupt Practices Act violations or other regulations. In these situations, organisations must be prepared to initiate defensible investigations using forensic methodologies and tactics to respond to authorities whilst maintaining impartiality, confidentiality and compliance. Regulators in each jurisdiction may take a slightly different approach than their counterparts in other countries, which can introduce an additional layer of challenges when an investigation spans multiple jurisdictions.

Key challenges organisations face during these matters may include:

Data Awareness

At the foundation, compliance and investigation preparedness programmes begin with establishing an understanding of the internal data landscape across structured (financial information and databases) and unstructured (communications messages and text-based documents) data sources. However, in many instances, data management processes are not as sophisticated as they need to be for many financial institutions and large corporations. To develop a clear picture of the data landscape, organisations must conduct a data mapping or inventory exercise to bring clarity to the sources of information across the organisation, how they generate, store and share information with other systems, what data types are sensitive or need additional controls, and what business functions and policies are in place around them.

Emerging Data Sources

Recent years have also ushered in an explosion in the use of cloud-based applications and various collaboration tools. The exponential growth in data volume, variety and velocity, and this proliferation of emerging data sources (e.g., cloud-based platforms and chat applications) and off-channel communications (e.g., messaging via mobile devices and ephemeral messaging tools), have fundamentally transformed how data is created, shared, stored and relied upon.

Personal Devices

In an internal investigation, monitoring and collecting messages and other data from personal devices also requires sophisticated and robust governance methodologies and policies, including acceptable use terms that define how business data is handled in bring-your-own-device environments. Failure to monitor all messaging channels can leave an organisation unaware of instances of financial crime or non-compliant behaviour, consequently resulting in enforcement actions.

[1] *SOURCE*: https://jaapl.org/content/37/4/538

[2] *SOURCE*: https://techreport.com/statistics/white-collar-crime-statistics/

Data Co-Mingling

As an extension of the challenges with emerging data sources and devices, and the nature of modern financial operations and transactions, trade and other financial data is increasingly co-mingled with communications data within many institutions' IT environments. Subsequently, there are an array of new challenges in investigations, spanning how communications are monitored for regulatory compliance, identifying the full range of data sources that may be in scope in an investigation, and technical challenges in collecting and analysing data from these dynamic platforms. At the end of the day, fact finding exercises and reports should weave structured and unstructured data together to provide the full context of the facts.

Cross-Jurisdiction Investigations

When a single violation extends to numerous regulatory bodies, it often triggers multiple concurrent investigations, all with unique data disclosure requirements and timelines. Agencies may have conflicting guidelines (such as data privacy rules that prohibit transfer of certain information to agencies in other jurisdictions) and they may also share information about their investigations with international counterparts. Any of these factors may increase the risk, cost and complexity of investigation and disclosure processes.

Conclusion

All investigations, particularly those related to white collar crime, must be approached with the expectation that the results may come under scrutiny. Therefore, organisations must be prepared to quickly initiate and follow defensible forensic procedures and sound investigative processes as soon as an issue arises.

As the number of relevant data sources grows, overall data volumes continue to increase, and the time to collect this data shrinks, risk surrounding white collar crime and regulatory enforcement will continue to intensify. Organisations must understand the enforcement trends and data challenges that can impact their risk profile. Without visibility into where critical data exists across the organisation, exposure cannot be fully understood.

In this environment, leaders should take these risks seriously and work to establish readiness for common investigations challenges. Working with data and investigations experts who know what to expect and how to navigate complex data issues under pressure will help to reduce risk and improve overall regulatory response over the long term.

AVI DAS
Senior Managing Director
+44 7886 802 824
avi.das@fticonsulting.com

JERRY LAY
Senior Managing Director
+41 78 668 68 68
jerry.lay@fticonsulting.com