GIR INSIGHT

AMERICAS INVESTIGATIONS REVIEW 2021

AMERICAS
INVESTIGATIONS REVIEW
2021

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2020
For further information please contact Natalie.Clarke@lbresearch.com

Published in the United Kingdom
by Global Investigations Review
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL
© 2020 Law Business Research Ltd
www.globalinvestigationsreview.com

To subscribe please contact subscriptions@globalinvestigationsreview.com

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer–client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of September 2020, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to Law Business Research, at the address above. Enquiries concerning editorial content should be directed to the Publisher – david.samuels@lawbusinessresearch.com

ISBN 978-1-83862-267-1

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

Contents

Cross-border overviews

Enforcer overview

Country chapters

Preface

Welcome to the *Americas Investigations Review 2020*, one of *Global Investigations Review*'s special reports. *Global Investigations Review*, for newcomers, is the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing. We tell them all they need to know about everything that matters, wherever it took place.

Throughout the year, *GIR* writes daily news, surveys and features; organises the liveliest events ('GIR Live'); and provides our readers with innovative tools; and know-how products to make life more efficient.

In addition, assisted by external contributors, we curate a range of comprehensive regional reviews – online and in print – that go deeper into developments than the exigencies of journalism allow.

The *Americas Investigations Review 2020*, which you are reading, is one of those reviews. It contains insight and thought leadership, from 28 pre-eminent practitioners from the region. Across 11 chapters, and 160 pages, it is part invaluable retrospective and part primer. All contributors are vetted for their standing and knowledge before being invited to take part.

Together, these writers capture and interpret the most substantial recent international investigations developments of the past year, with footnotes and relevant statistics. Other articles provide valuable background so that you can get up to speed quickly on the essentials of a particular topic.

This edition covers Brazil, Mexico and the United States – each from multiple perspectives, and has overviews on the Department of Justice's use of tools that are not the Foreign Corrupt Practices Act; on evidence gathering; and on how to ensure that history does not repeat – the art of learning the right lessons as an investigation winds down.

Among the highlights for this reader:

- a fine discussion of the *Bogucki* case – in which the US Department of Justice has been accused (by a former member of staff) of misusing mutual legal assistance treaty requests to stop the clock on cases;
- news that Airbus's huge settlement led to raids for other companies – notably Avianca;
- finding a worked example of how to learn the lessons at the end of an investigation (featuring hypothetical company 'ZYX Inc');

- the full breakdown of all corruption related fines and settlements levied in Brazil, complete with graphics; and
- discovering that covid-related corruption is already under investigation in Germany, Italy Serbia and Brazil, and that the new head of Mexico's Federal General Prosecutor's office is over 80 years old (and was chosen for his venerableness in part).

And much, much more.

If you have any suggestions for future editions, or want to take part in this annual project, we would love to hear from you. Please write to insight@globalarbitrationreview.com.

David Samuels
Publisher, Global Investigations Review
London
September 2020

Use of Data to Detect Crime and Evaluate Corporate Compliance

Sean O'Connell and Kevin Gaunt
Hunton Andrews Kurth LLP

In summary

The US Department of Justice (DOJ) has long used data monitoring and analysis to inform its investigatory efforts in certain of its sections. The DOJ is now expanding its analytical reach into other areas, and as the DOJ has expanded its own data analysis efforts, it has also released guidance indicating that it expects corporations to incorporate data collection, monitoring and analysis efforts into their compliance programmes to augment their risk assessments and inform the continued growth and refinement of their compliance protocols.

Discussion points

- The DOJ now expanding the use of data analysis into more and more of its operational units
- The rapid disbursement of relief funds by the US government to taxpayers and corporations has placed pressure on DOJ to monitor the use of those funds for fraud and other criminal activity
- The DOJ recently released updated guidance on the factors its prosecutors should consider in evaluating corporate compliance programmes, with this guidance now encouraging companies to use a data-driven approach
- DOJ guidance stresses the evaluation of whether corporate compliance personnel have sufficient access to relevant sources of data related to compliance monitoring

Referenced in this article

- DOJ, Evaluation of Corporate Compliance Programs
- DOJ, Evaluation of Corporate Compliance Programs
- DOJ, National Crime Information Systems
- DOJ, Operation WireWire
- Hunton Andrews Kurth LLP, COVID-19 Complaint Tracker

Introduction

In the four months since the covid-19 shutdown orders were issued in the United States, over 3,500 lawsuits have been filed in state and federal courts challenging decisions made by corporations, insurance companies and governmental entities grappling with how to safely operate during a pandemic. Tech-savvy law firms saw the unprecedented changes in virtually every aspect of American life and modified their data analysis resources to create litigation trackers. One example of these is Hunton Andrews Kurth's COVID-19 Complaint Tracker, which is a comprehensive database of state and federal litigation involving covid-19 claims compiled to provide clients and the public with real-time data to inform their business practices and avoid litigation. In today's global economy, the analysis of large amounts of data drives informed business decisions. Unfortunately, data analysis is increasingly fetishised as a technical cheat code that falsely promises to unlock insights that human analysis cannot. Accordingly, those selling data analysis have the least influence in fields where the data is the strongest and most well-known, and the most influence in fields where the data is complex and misunderstood by its users, and can be misused to confirm pre-existing biases.

Federal law enforcement is no different. Although the US Department of Justice (DOJ) seeks different goals than global companies, it has long obsessed over how to use data analytics as a way to fight crime. White-collar crime components of the DOJ have used data analysis for decades – with varying degrees of success – to detect, investigate and prosecute criminals. Recently, the DOJ revised its guidance on how it evaluates corporate compliance programmes. The guidance now encourages companies to employ a data-driven approach to monitoring and updating their compliance programmes on an ongoing basis. As we will discuss, the shift from using data to detect crime to requiring corporations to analyse data as a factor in determining corporate compliance is both significant and problematic.

Fighting crime with big data

The world generates 2.5 quintillion bytes of data a day. That data leaves digital footprints that are typically harmless, but can help the DOJ solve crime in several ways. For example, DNA and fingerprints can be stored in databases and used to identify suspects more quickly. A look at a document's metadata can tell investigators when accounting records were changed to cover up a fraud scheme. Data can also help law enforcement recognise crime trends and take appropriate action.

However, the exponential growth in data can also choke investigations that employ traditional methods to detect and prosecute white-collar crime. The DOJ knows this and is attempting to modernise and find ways to efficiently sift through big data. For example, on 4 May 2020, assistant attorney general Brian Benczkowski announced that, in order to fight covid-19 related fraud related to the over US$525 billion of Paycheck Protection Program (PPP) loans that have been disbursed, the DOJ would employ data analysis similar to what it has employed for a decade to detect healthcare fraud. He emphasised that the DOJ will expand its existing data analysis efforts to include 'looking at other financial products and other trading behaviour at desks at major financial institutions' and said that 'this is the type of case and the use of data that we expect to become the norm in the Criminal Division in the future'. He encouraged banks, trading firms and other financial institutions to start scrutinising their own trading data in order to detect misconduct and self-report it to the appropriate authorities before the DOJ finds the data on its own.

Despite Benczkowski's forward-looking statement, federal law enforcement has been trying to use data analysis for several decades. For instance, the following DOJ list has several crime information systems that are available to both the criminal justice community and non-criminal justice agencies:

- National Crime Information Center;
- Law Enforcement Enterprise Portal;
- National Data Exchange (N-DEx);
- Next Generation Identification;
- National Instant Criminal Background Check System;
- International Justice and Public Safety Network;
- Internet Crime Complaint Center (IC3); and
- the Financial Crimes Enforcement Network's Suspicious Activity Reporting System.

Other civil enforcement agencies and self-regulatory bodies also use data analysis platforms that may result in criminal referrals to the DOJ to investigate. Those platforms include:

- the Financial Industry Regulatory Authority's Office of Fraud Detection and Market Intelligence; and
- the Securities and Exchange Commission's Analysis and Detection Unit.

As an example regarding the above, the N-DEx system bills itself as a service enabling criminal justice pros to connect the dots among data to make better conclusions and predictions. Law enforcement professionals, however, will often consult multiple databases to increase the accuracy of their investigations.

In the past 10 years, the DOJ has looked to the private sector to help them detect crime through the use of data. Recognising that its own data mining resources are insufficient, the DOJ has contracted companies like Palantir and DataWalk to analyse financial crimes like healthcare fraud and money laundering.

Regardless of the area of white-collar crime, the promise of these companies to the DOJ is always the same: speed. Data analysis that would take special agents weeks can now be done in minutes with an algorithm that will allow attorneys and investigators to quickly identify and monitor connections, money flows, patterns of suspicious activity and statistical outliers. Indeed, it is standard practice for certain sections of the DOJ to obtain the probable cause needed to execute a search warrant based solely on data analysis. Despite these tools at their disposal, the DOJ's white-collar crime prosecutions have declined over the past decade. There are many causes for this decline, but one key indicator for the DOJ sections that have been able to prosecute a similar number of cases over the past 10 years is that they chose data sets to analyse that go to their core competencies, with an eye towards developing admissible evidence at trial. Therefore, it is necessary to examine how different sections of the DOJ's Criminal Division use different data sets.

The Health Care Fraud Model

When it came to the covid-19 pandemic response, it was no accident that, when confronted with the problem of having to police the potential fraud arising out of the US$525 billion dispersed as part of the PPP loan, assistant attorney general Benczkowski chose to rely on how the DOJ's Health Care Fraud (HCF) Section had analysed data to prosecute a variety of healthcare fraud crimes. Simply put, no DOJ unit has done more to detect crimes using data than the DOJ's HCF Section. Despite declines in other white-collar crime prosecutions generally, there has been a dramatic increase in healthcare fraud prosecutions over the past three years. In 2017, 220 individuals were charged with healthcare-related crimes, with 309 being charged in 2018 and 344 being charged in 2019.

Before looking at the type of data that is analysed, it is important to underscore that the HCF Section's goal when performing data analysis is elegant in its simplicity: spot trends and outliers in Medicare and Medicaid billing patterns that point to possible healthcare fraud. In other words, rather than rely on traditional methods of waiting for often unreliable tipsters and whistleblowers to provide information to federal agents, the DOJ formed specialised task forces that use data mining to spot surges in billing patterns that are unusual and suspicious. After suspicious activity is spotted, traditional law enforcement techniques are used to investigate and make the case, if there is one. By using data analysis as a first step, the DOJ can perform a preliminary investigative step without the fear of the existence of the investigation becoming public and risking a subject's reputation unnecessarily. Because of its success, this data analytics program was expanded to tackle the opioid epidemic in regional hot spots for opioid abuse in 2017.

Examining the type of data that is analysed by the HCF Unit reveals that, despite the large number of data points from multiple sources, the data itself is abundantly relevant to determining whether a defendant committed healthcare fraud. For example, in order to identify targets, healthcare fraud investigators may examine the following sources of data.

Type of data	Possible uses
PII (CLEAR/Accurint): SSN, aliases, related entities and people	• Helping establish background information • Finding other business that may be involved in the scheme (eg, shell companies owned by relatives) • Distinguishing between entities with similar names
Medicare enrolment data: Business ownership, who works there, when they applied, current status with Medicare, sanctions/administrative actions	• Determining Medicare 'opt-out' status • Comparing statements on application to ownership of business from information above
Historic Medicare trends: Top 10, high-risk providers, metrics specific to providers and entities	• HCF trends by district • Entity relationships • Quick referencing to check strength of possible target
Real-time Medicare trends: CMS Medicare databases	• Determining billing by a provider during a period in which he or she was out of the country • Understanding exact billing codes that a provider was using for a particular fraud scheme

Type of data	Possible uses
Disciplinary history (professional boards/open source): License suspension, revocation, sometimes malpractice settlement information	Distinguishing higher-risk providers; identifying prior court cases
Consolidated Data Analysis Center Models (Office of Inspector General (Department of Health and Human Services))	• Ranking prescribers, pharmacies, or home health aides within a district • Verifying the strength of already open cases
TRICARE/Palantir Compounding Pharmacy Data	• Checks if a key federal partner already has an open case
Open/New Cases (Federal Bureau of Investigation; Office of Inspector General (Department of Health and Human Services); Internal Revenue Service)	• Checks if a key federal partner already has an open case
Automation of Reports and Consolidated Orders System, Drug Theft Loss, Suspicious Orders Report System (Drug Enforcement Agency)	• Connects manufacturer, distributor and pharmacy data • Helps assess pharmacy risk level
Suspicious Activity Reports and Currency Transaction Reports (Financial Crimes Enforcement Network)	• Identifying suspicious transactions • Identifying banks to subpoena or investigate further

Once this data is analysed, further data can be analysed to determine how strong the evidence is against a particular defendant:

Type of data	Possible uses
Data by provider (Providers include clinicians, home health agencies, durable medical equipment providers, pharmacies, labs, among others)	• Identifying overall patterns between procedures billed, diagnoses, volume of practice • Providing background on the business practices of a specific entity (ie, group level versus individual) • Can check for complexity of patient population based on level of treatment • Provides insight as to the specialty of a clinician
Data by referral source	• Determining referral patterns between clinicians and entities • Identifying potential relationships based on patient transfers, volume and appropriateness
Time studies (how many and what type is billed in a day)	• Complex procedure analysis (Note: Many factors can skew the results)
Beneficiary data	• Full beneficiary history including all claim types from all providers (Parts A, B, D) • Determining best beneficiaries to interview • Identifying relationships between beneficiary and providers, including possible primary care physicians
Ping-pong analysis/shared beneficiary analysis	• Shows movement of beneficiaries going back and forth between providers • Very helpful for home health cases and cases in which a fraudulent provider closes down and beneficiaries need to shift to continue treatment

By analysing relevant data in a systematic way, federal investigators will have a well-developed case theory against the target before the first potential witness has been interviewed. With the success of the HCF Section's data analysis, it should come as no surprise that the DOJ is attempting to overlay these data analysis methods onto other DOJ white-collar crime sections. The PPP loan was an obvious choice to adopt the HCF Section's data analysis method because of the similarities with Medicare's 'pay then chase' policing strategy. In an attempt to repeat the HCF Section's success, many other DOJ white-collar components will look to adopt similar investigative methods.

Other uses of data by the DOJ

The success of the HCF Unit's use of data analysis is the next evolutionary step in the long-standing historical efforts by the DOJ and the Federal Bureau of Investigation (FBI) to use advanced methods to solve crime. From the first generation of FBI agents that used scientific laboratories to determine unique chemical elements to catch bank robbers to the Internal Revenue Service (IRS) recreating spending habits to prove tax evasion, data analysis has always been a necessary tool on the federal crime fighter's utility belt. The Fraud Unit's Foreign Corrupt Practices Act Section, the Money Laundering Asset Recovery Section, the Antitrust Division, the Securities Exchange Division and the Tax Division all use advanced data analysis to detect and prosecute crimes.

The global nature of the world economy has also caused federal law enforcement to police foreign entities more than ever. In multinational investigations into fraud, tax evasion and the Foreign Corrupt Practices Act, federal law enforcement is required to coordinate with international law enforcement entities. For example, in 2018, 74 individuals were arrested for their role in a multimillion dollar business email compromise (BEC) scam campaign. The FBI worked with law enforcement agencies from four countries – including Nigeria, Canada, Mauritius and Poland – to take down a ring of cybercriminals responsible for a series of BEC schemes. According to the DOJ, the scams led to a staggering US$14 million in phony wire transfers. Investigators used data from the IC3 to identify and track 'money mules' who then led investigators back to the BEC fraudsters themselves.

As another example, the DOJ's Civil Rights Division is also using big data analysis to prove disparate treatment against minorities in American cities. In its investigation of Baltimore's Police Department (BPD), the DOJ used aggregate data about police–community contacts. By using police encounter data, the DOJ was able to show that the Baltimore police violated people's Constitutional rights. The Civil Rights Division focused on the following data sets:

- relevant policies and training materials used by the BPD;
- the BPD's database of internal affairs files;
- a random sample of about 800 case files on non-deadly force incidents;
- files on all deadly force incidents since 2010 that the BPD was able to produce through 1 May 2016;
- a sample of several hundred incident reports describing stops, searches and arrests;
- investigative files on sexual assault cases; and
- databases maintained by the BPD and the State of Maryland containing information – including location – on hundreds of thousands of pedestrian stops, vehicle stops and arrests.

The results from the data analysis revealed the following constitutional violations. First, where location data was available for stops, investigators assessed the number of local stops relative to the number of local residents and determined that two districts accounted for almost half of all the stops in Baltimore. Second, using the pedestrian stop data, and combining it with data on citations and arrests, DOJ investigators demonstrated that over 96 per cent of stops did not lead to a citation or arrest, which is a data point that is indicative of police harassment. Third, data on arrests and searches demonstrated that hundreds of arrests and search warrants per month, on average, were legally unfounded. Data maintained by the State of Maryland shows that, from 2010 to 2015, the BPD made thousands of arrests and executed hundreds of search warrants where the reviewing officials declined to charge or found no contraband.

The Baltimore investigation also reinforces the limitations of data analysis. The BPD did not examine complaints and therefore could not track or remediate problems caused by officers. While failing to maintain data does not create the same visceral reaction that a demonstrable constitutional violation does, the two problems are related and equally sinister. Inaccurate tracking of any of this data renders it as having little evidentiary value and actually hides problems that companies and government entities need to know about or risk reinforcing morally dubious behaviour. This is known as tech-washing: people who use data analysis systems assume that they are somehow more neutral or objective, when in reality, they interpret the data in accordance with their biases.

A separate problem occurs when federal investigators seek data sets that are simply too tangential to crimes that they are charged with investigating. In 2017 and 2018, the IRS tried to use smartphone location data to track tax criminals. Once the Supreme Court required federal investigators to obtain a warrant before obtaining historical cell tower data in 2018,[1] federal investigators began to look for alternative means of obtaining such data. Here, the IRS allegedly paid a third-party data firm for large amounts of United States citizens' location data. The location data sold to the IRS was anonymised and designed for advertisers and other businesses for marketing purposes. After a year of paying for the data, the IRS did not renew its contract for the data and it does not appear that the data was used to indict or prosecute any criminals through the data access. Whether the data or methodology was faulty, federal law enforcement commits more unforced errors when they are reaching out of their core competencies to obtain data with relatively low evidentiary weight in criminal tax cases.

DOJ expectations regarding data in evaluating compliance programmes

On 1 June 2020, the DOJ issued its Guidance on the Evaluation of Corporate Compliance Programs (the 2020 Guidance), which was based on a version released in April 2019. As in earlier versions, the 2020 Guidance begins by laying out the 'three fundamental questions' that are at the heart of the DOJ's evaluation of any compliance programme.

- Is the corporation's compliance programme well designed?

[1] Prior to the Supreme Court decision *Carpenter v United States*, 138 S Ct. 2206 (2018), prohibiting the behavior, federal law enforcement routinely subpoenaed cell phone tower data to match with existing evidence to determine where a target was at any given time.

- Is the programme being applied earnestly and in good faith? In other words, is the programme being adequately resourced and empowered to function effectively?
- Does the corporation's compliance programme work in practice?

Notably, the 2020 Guidance directs prosecutors to ask these fundamental questions 'both at the time of the offence and at the time of the charging decision and resolution'. This change highlights the DOJ's interest in examining how a company's compliance programme has evolved over time and particularly whether such company has used the 'lessons learned' from past compliance failures – whether its own or those of similarly situated companies – to enhance its compliance functions.

The DOJ made a number of changes that highlight the need for compliance programmes to be dynamic and data-driven. Throughout the revisions, however, the 2020 Guidance's key theme remains the same as in its prior iterations: compliance programmes should be risk-based, tailored to the specific circumstances of the company and updated regularly in order to ensure optimal ongoing effectiveness.

We highlight two of the key revisions in the 2020 Guidance below.

Emphasis on data analytics

Building on the pre-existing guidance that companies should monitor and update their compliance programmes on an ongoing basis, the 2020 Guidance encourages companies to employ a data-driven approach when doing so. In performing periodic reviews of their foundational risk assessments, companies should utilise 'continuous access to operational data and information across functions'. The revised 2020 Guidance alludes to a number of potential metrics for companies to consider employing, including:

- tracking responses to employee surveys about the compliance culture;
- reviewing statistics on internal audit findings concerning compliance and related disciplinary decisions;
- tracking employee access to policies and procedures to understand which are being utilised; and
- testing employee awareness and use of the company's compliance hotline.

In addition, the 2020 Guidance calls for companies to monitor, track and incorporate 'lessons learned' from both a company's own prior experience and the experience of related companies in the same industry or geographic region.

Compliance resources

The DOJ revised the second fundamental question, which formerly asked only if the compliance programme was effectively implemented, to specifically ask whether the programme is 'adequately resourced and empowered to function effectively'. This question does not focus purely on financial resources. Again, looking towards the application of data-driven compliance efforts, the 2020 Guidance asks whether 'compliance and control personnel have sufficient . . . access to relevant sources of data' related to compliance monitoring and, if not, what the company is doing to address any 'impediments' that might limit such access. Further, the 2020 Guidance asks whether a company's compliance function monitors its own behaviour – meaning its investigations and disciplinary decisions – to ensure consistency. Having processes in place to track and analyse consistency in their own compliance operations will allow companies to ensure fair application of policies and standards, which in turn promotes trust and employee buy-in to the company's culture of compliance.

The reasoning behind this emphasis on data appears to be to make sure middle management gets the message on compliance programmes. 'We wanted to make sure the mid-level management is also echoing that theme, ensuring compliance programmes are adequately resourced and empowered', said Sally Molloy, chief of a Justice Department policy and training unit.[2]

In practice, many global companies with compliance programmes have been tracking compliance data for years. For good reason, as we discussed above, data analysis is a necessary part of informed decision making. Previous DOJ guidance referenced data analysis. For example, the 2017 version of the DOJ's 'Evaluation of Corporate Compliance Programs' placed an emphasis on data. Compliance and legal professionals were expected to leverage data, metrics, and other objective evidence to demonstrate a compliance programme was working. Moreover, companies needed to use and track meaningful data to assess and fix corporate compliance programmes.

Conclusion

The 2020 Guidance is now putting private companies on notice that they must incorporate data analysis into their compliance programmes. This may be easier said than done, as finding and extracting useful data is rarely an easy task for companies. Companies will need competency and technology that is typically beyond an existing corporate compliance department's abilities. Therefore, much more is needed than the collective will to give compliance officers access to data and the technical competency to do it. Even more troubling is that setting up the data analysis and lessons learned would provide a road map and the necessary evidence to prosecute the company should the government start an investigation. For example, the application of analytics and monitoring can not only uncover regulatory oversights, but also point out transactions implicating anti-corruption statutes. These analysis tools can also be successfully employed to detect embezzlements, kickbacks, accounting irregularities and a host of other compliance failures and operational risks. Companies should be able to create these compliance records and data analyses without fear that the government could perform an investigatory end run.

As the government's constant evolution with data mining demonstrates, there is no singular data 'Excalibur' that can easily give you what you want with minimal effort. While it is not always clear which data is being tracked or analysed by the DOJ to detect fraudulent activity, companies should not be deterred from considering how they can use analytics to proactively identify harbingers of potential fraud. Unfortunately, undertaking such efforts implicates important financial and legal considerations that are only beginning to be explored.

[2] https://www.wsj.com/articles/doj-compliance-guidance-places-new-emphasis-on-middle-management-use-of-data-11593212728.

Sean O'Connell
Hunton Andrews Kurth LLP

Sean represents corporations and individuals in white-collar investigations and litigation proceedings. Through his collaboration with nearly every facet of the Department of Justice (DOJ) and related investigatory agencies, Sean has developed substantive knowledge in investigations, enforcement actions and regulatory issues, including criminal fraud statutes, criminal tax statutes, public corruption statutes, the Foreign Corrupt Practices Act, anti-kickback statutes, Health Insurance Portability and Accountability Act and the False Claims Act.

Sean served as a federal prosecutor and civil assistant United States attorney for 13 years and entered the DOJ through the Attorney General's Honors Program after completing a federal clerkship with the Eastern District of Pennsylvania. As the former health care fraud coordinator for the Western District of Texas's United States Attorney's Office and trial attorney with the DOJ's Health Care Fraud Unit, he provides counseling and advisory services to health care clients for regulatory issues, including offering counseling to clients seeking to enhance their compliance programs and supervision systems. Sean also represents corporations and individuals in matters involving white-collar criminal defence, civil and regulatory investigations, corporate internal investigations, congressional investigations and similar matters.

Kevin Gaunt
Hunton Andrews Kurth LLP

Kevin helps clients navigate the waters of white-collar defence, internal investigations and regulatory enforcement. He advises on complex compliance issues and has a knack for matters involving data management and technology.

Kevin represents clients in a range of industries, including financial services, telecommunications, student lending, social media and consumer electronics, in matters involving financial crime, data privacy and data breaches, money laundering, the Foreign Corrupt Practices Act, and anti-bribery and anti-corruption violations. He also advises clients on issues relating to national security matters such as the Foreign Agents Registration Act, Office of Foreign Assets Control violations, counterespionage investigations and export control compliance. He focuses on understanding his clients' businesses and needs first, and then providing clear, practical counsel.

With a broad range of practical experience in the arena, Kevin is also well-versed in electronic discovery and the collection, management, and production of electronically-stored information (ESI). He regularly advises clients and other attorneys on thorny issues arising from the use and production of ESI, whether in conducting internal investigations, responding to government subpoenas or during the course of discovery in litigation.

HUNTON
ANDREWS KURTH

With 1,000 lawyers in the United States, Asia, Europe and the Middle East, Hunton Andrews Kurth LLP serves clients across a broad range of complex transactional, litigation and regulatory matters. We are known for our strength in the energy, financial services, real estate and retail and consumer products industries, as well as our considerable experience in more than 100 distinct areas of practice, including privacy and cybersecurity, intellectual property, environmental, and mergers and acquisitions. Our full-service litigation practice is one of the largest in the country, with particular depth in key litigation markets such as Texas, California, Florida and the Mid-Atlantic.

Riverfront Plaza, East Tower
951 East Byrd Street
Richmond, VA 23219
United States
Tel +1 804 788 8200
Fax: +1 804 788 8218

2200 Pennsylvania Avenue NW
Washington, DC 20037
United Sates
Tel: +1 202 955 1500
Fax: +1 202 778 2201

www.huntonak.com/en

Sean O'Connell
soconnell@HuntonAK.com

Kevin Gaunt
kgaunt@HuntonAK.com

The *Americas Investigations Review 2021* contains insight and thought leadership from 28 pre-eminent practitioners from the region. Across 11 chapters, spanning around 160 pages, they provide an invaluable retrospective and primer.

Together, these writers capture and interpret the most substantial recent international investigations developments of the past year, with footnotes and relevant statistics. Other articles provide valuable background so that you can get up to speed quickly on the essentials of a particular topic.

This edition covers Brazil, Mexico and the United States – each from multiple perspectives, and has overviews on the Department of Justice's use of tools that are not the Foreign Corrupt Practices Act; on evidence gathering; and on how to ensure that history does not repeat – the art of learning the right lessons as an investigation winds down.

Visit globalinvestigationsreview.com
Follow @GIRAlerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-267-1