REPRINT

CD corporate disputes

CONDUCTING INVESTIGATIONS IN THE NEW NORMAL

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
JAN-MAR 2021 ISSUE

www.corporatedisputesmagazine.com

Visit the website to request
a free copy of the full e-magazine

Guidehouse

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

EXPERT FORUM

CONDUCTING INVESTIGATIONS IN THE NEW NORMAL

PANEL EXPERTS

Sandra Desautels
Senior Director, Financial Services
Guidehouse
T: +1 (646) 227 2627
E: sdesautels@guidehouse.com

Sandra Desautels is a senior director in Guidehouse's global investigations & compliance practice, with over 20 years of investigations experience in the private sector and law enforcement. She assists clients by leading financial crimes investigations and compliance assessments. Her projects are predominantly focused on fraud allegations or money laundering and terror financing suspicions. Financial institutions engage Ms Desautels to help establish or augment their global investigations units and provide specialised training to investigators or transaction monitoring review teams. She also conducts assessments of fraud mitigation, anti-money laundering and anti-corruption programmes.

Daniel Gill
Director, Financial Services
Guidehouse
T: +1 (202) 973 2416
E: daniel.gill@guidehouse.com

Daniel Gill is a director in the global investigations & compliance practice at Guidehouse. He has over 40 years of experience in connection with fraud investigations, forensic accounting, anti-money laundering and asset tracing matters. He previously served 23 years as a special agent with the Federal Bureau of Investigation (FBI) where he conducted a wide variety of financial investigations of major criminal organisations.

Deborah S. Thoren-Peden
Partner
Pillsbury Winthrop Shaw Pittman LLP
T: +1 (213) 488 7320
E: deborah.thorenpeden@
pillsburylaw.com

Deborah Thoren-Peden is a partner at Pillsbury Winthrop Shaw Pittman LLP, where she focuses her Chambers-ranked corporate practice on banking, electronic commerce, privacy, anti-money laundering and Office of Foreign Assets Control (OFAC) regulations. She co-leads Pillsbury's FinTech, payments & Blockchain team, as well as its consumer & retail industry, cyber security, data protection & privacy and unclaimed property teams.

Cassie Lentchner
Senior Counsel
Pillsbury Winthrop Shaw Pittman LLP
T: +1 (212) 858 1211
E: cassie.lentchner@pillsburylaw.com

Cassandra Lentchner is senior counsel at Pillsbury Winthrop Shaw Pittman LLP, where she utilises her unique background in financial services regulations and regulatory relationships to strategically analyse and balance risk with business advancement and development.

Aaron S. Dyer
Partner
Pillsbury Winthrop Shaw Pittman LLP
T: +1 (213) 488 7321
E: aaron.dyer@pillsburylaw.com

Aaron Dyer is a partner at Pillsbury Winthrop Shaw Pittman LLP, where he handles complex civil and criminal litigation as part of the firm's corporate investigations & white-collar defence team, as well as heading the firm's Southern California white-collar practice. In addition to complex litigation and white-collar defence, he focuses his practice on internal investigations, intellectual property (IP) litigation, and criminal and civil trial work, with an emphasis on securities, healthcare, the False Claims Act, and IP theft and piracy.

CD: What do you consider to be among the major trends shaping internal investigations in recent months? To what extent have you seen an uptick in their frequency?

Desautels: The global pandemic has highlighted areas of vulnerability, from internal and external sources. Many diverse industries have seen an increase in referrals for internal investigation. The allegations range from conflict of interest matters to misappropriation of customer and employer funds. Notably, the initial increase of referrals seemed to be a result of heightened awareness and enhanced controls implemented in response to new threats, instead of more incidents.

Lentchner: One growing trend is an increase in investigations alleging internal misconduct triggered by whistleblowers. Some of this increase is due to increased governmental prioritisation of whistleblowers including the Securities and Exchange Commission (SEC) Whistleblower Program. We have also seen reports arising out of the #MeToo movement, as well as the expanding role of boards and corporate social responsibility.

Gill: The pandemic has resulted in significant work for investigation teams for cyber security concerns and a surge in demand for computer forensic services. With the majority of personnel working remotely, the ability to forensically capture and analyse relevant computer data became critical. Companies with in-house capability sometimes identified gaps in their current skills or processes, such as incomplete data capture, or lack of knowledge about data forensic tools to ensure appropriate chain of custody. For investigations that may result in litigation, remediation of such items is critical.

CD: What are some of the underlying drivers and common themes among investigations? How prevalent, for example, are fraud-related investigations?

Desautels: The increase in remote users, combined with the disruption caused by the global pandemic, created a perfect storm for fraud from both internal and external sources. We saw many law enforcement agencies across the globe issue alerts about fraud related to coronavirus (COVID-19) equipment, financing and tenders. There also were warnings about other fraud schemes such as identity theft, money mules and exploitation of children and the elderly. A significant rise in reported cyber crimes was also evident, with criminals eager to take advantage of the increased use of remote workers and virtual environments, many deployed hastily and without robust controls. It is important to remember that when companies make things easier

for customers or employees, they also make it easier for the criminals.

Gill: Criminals have historically responded to disasters and other crises by engaging in conduct seeking to exploit vulnerabilities related to these events. Common themes identified were higher volumes of phishing emails, penetration of inadequately controlled data warehouses, theft of intellectual property – internally facilitated and hacked – push payment fraud schemes and unauthorised participants during virtual group workshops.

Thoren-Peden: There has been a huge increase in ransomware demand in 2020. Some reports indicate there has been a 715 percent year on year increase in detected, and blocked, ransomware attacks. Not only have ransomware attacks been on the rise, but they are also becoming more harmful to companies, as the criminals sometimes encrypt significant portions of a corporate network and then attempt to extort ransoms, often in bitcoin. Companies subject to these attacks have been required to engage in extensive internal reviews of their systems and personnel to determine the impact of an event. Companies impacted by cyber attacks have also undertaken investigations of their workforce's use and storage of data to design better and more secure controls.

CD: To what extent have investigations necessarily evolved and adapted to a changing business landscape and the way companies now operate?

> **"The increase in remote users, combined with the disruption caused by the global pandemic, created a perfect storm for fraud from both internal and external sources."**
>
> *Sandra Desautels, Guidehouse*

Desautels: Investigation teams have had to reprioritise their investigations, based on the available tools and focus of the investigation. Where investigations require forensic data capture or review of physical items, more lead time is needed to coordinate with internal and external partners, such as legal, IT and applicable vendors. Determining whether to proceed with virtual interviews is also an important consideration, with important consequences. For instance, can an employee be

directed to attend an in-person interview at the workplace, or at an alternate site if the regular workplace is currently closed due to COVID-19 restrictions?

Gill: Many companies are also reviewing their internal fraud-detection mechanisms to enhance scenarios and refresh lists and examples of red flags. Several are also compiling guidance on acceptable types of supporting documents and methods of possible corroboration.

Thoren-Peden: Artificial intelligence (AI) and machine learning (ML) are rapidly changing the resources available for an investigation. Forensic analysis of documents and information is being incorporated in investigation tools. AI tools are being incorporated into both regulatory examinations and government enforcement investigations, often to help the government organise and review or analyse huge amounts of data and documents. Similarly, corporations, compliance teams and even internal investigators are developing and using AI and ML technology to help identify risks and investigate risks and concerns.

CD: Drilling down, what changes are you seeing to the approaches, processes and tools used to conduct internal investigations, both remote and on site? To what extent are some of the more recent changes likely to persist into the future?

"Many companies are also reviewing their internal fraud-detection mechanisms to enhance scenarios and refresh lists and examples of red flags."

Daniel Gill, Guidehouse

Desautels: Coordination between investigation teams, HR and the legal department is of increased importance. Proactive measures include updates to confidentiality agreements, remote work policies, the code of conduct or conflict of interest policy, and other related documents.

Gill: Investigation procedures and protocols are also being updated with remote interview considerations, since many companies are implementing permanent remote work options.

Thoren-Peden: Companies are also reviewing investigator tools and resources, and determining whether to supplement needs with specialised vendors, or grow in-house teams.

Dyer: Increasingly, companies are building analytics and investigative controls into their systems to better manage data for both business and investigatory purposes.

CD: Based on your experience, what kinds of challenges have investigators been forced to surmount in recent months? What steps have they taken in response?

Desautels: Investigators have had to quickly adapt to virtual interviews, where typical nonverbal cues are not necessarily captured. Preparation for virtual interviews tends to take longer, with decisions on what technology to use and its capacities to share information and support side conversations, while protecting attorney-client privilege. Decisions regarding the use of technology and planning become strategic, including whether and how to present and share documents. Advanced planning is required for a parties' internet connection being insufficient to allow for video connection, and parties that cannot access certain technology solutions. Related considerations include the review of timelines in service-level agreements and key performance indicators.

Gill: The ability to conduct investigations remotely has become essential. Some organisations have conducted workshops to refresh technology skills and share good practices for conducting interviews via video teleconferencing.

Dyer: Firms have developed checklists of issues to consider when planning a virtual meeting and frequently schedule preparation or test planning sessions in advance of important meetings or interviews to confirm that the selected technology and plans will work as expected.

> **"Increasingly, companies are building analytics and investigative controls into their systems to better manage data for both business and investigatory purposes."**
>
> *Aaron S. Dyer,*
> *Pillsbury Winthrop Shaw Pittman LLP*

Thoren-Peden: As government compliance requirements grow more complex daily, investigators must simultaneously stay current on the new laws and regulations, and enhanced areas of risk.

"As government compliance requirements grow more complex daily, investigators must simultaneously stay current on the new laws and regulations, and enhanced areas of risk."

Deborah S. Thoren-Peden, Pillsbury Winthrop Shaw Pittman LLP

Understanding the trends in illegal activity in the company's sector and geographic area is also crucial. It is critical for regulated companies to stay on top of regulatory actions or consent orders imposed in their industry, as such actions and orders can often identify red flags of risk, and potential means of mitigation of such risk. It is more important than ever for legal and compliance teams to have access to solid investigation processes, whether through their own internal teams or in conjunction with their outside counsel and consultants who may help conduct internal investigations. When an investigation is needed, it is important for a company to carefully assess whether its internal team has

sufficient experience with technical elements of the investigation, such as cyber security reviews or retrieval of forensic data.

CD: Could you provide an insight into data collection and information gathering issues, and related privacy concerns, that typically arise during an internal investigation? What considerations need to be made to address these aspects?

Lentchner: Data privacy is an increasingly critical issue and internal investigations must be planned to ensure that its collection and management is considered. Investigative firms must make sure that they have clear policies and procedures concerning the collection and provide legally required notices, and all data collection processes should be approved by the responsible privacy officer. Planning requires evaluation of the precise types of data that will be collected, its sources, storage and use. It is important to have the right controls for the information flows and sharing so that all required participants have signed appropriate confidentiality agreements and access, through secure means with appropriate access controls, to confidential investigative materials. Equally important is to plan the systems to avoid sharing confidential information with those who have no need to access it and delete or destroy it when it is no longer required. All investigative staff must know any limitations in the collection process that could affect their analysis.

Desautels: Other data collection challenges arise when collecting data remotely, including how to do so without altering the metadata required for investigatory purposes. This raises key issues. For example, does data captured from a laptop via a virtual private network connection include documents on the local drive and desktop? Does the collection of unstructured data from a shared network folder, for instance, create a modified entry? Are there hard copy documents and other media with notes and comments, which were not collected and captured electronically because they are maintained in desks and other storage facilities?

"Planning requires evaluation of the precise types of data that will be collected, its sources, storage and use."

Cassie Lentchner, Pillsbury Winthrop Shaw Pittman LLP

Gill: Investigators must ensure the data collection and e-discovery teams clearly understand the type of data being sought and whether it must be forensically preserved. Equally important for investigators is to know any limitations in the collection process that could affect their analysis.

Desautels: Where the EU General Data Protection Regulation (GDPR) applies, the data collection process should include an approval from the responsible privacy officer to assess whether the request is proportionate to the purpose and scope of the investigation. In addition, the collected data should be safeguarded with appropriate access controls to ensure only authorised persons can see the information.

CD: Looking ahead, how do you anticipate digital technology will evolve in the short and long term as a key part of the investigation process? What solutions and innovations can we expect to see?

Desautels: In the short term, virtual environments will likely deploy increased access controls and quality. Long term, we can expect integration of features such as micro-expression detection, voiceprint identification and analysis, and, possibly, machine transcription of virtual sessions.

Dyer: The success of conducting many investigative activities virtually will likely result in increasing virtual investigations with less physical travel even after the pandemic has subsided. Employers are reimagining their working environment and workforce with increasing technological capacities and with virtual locations for at least some employees. Increasingly, investigative teams must be technologically smart and able to adapt to new technology for clients. CD