SIRM

CORPORATE INVESTIGATIONS IN 2026

Balancing Technology and Trust

Contents

Introduction

Corporate investigations are undergoing a period of rapid transformation in the face of technological and regulatory change. Once viewed largely as reactive and mobilised in response to crises, investigations are now increasingly central to how organisations understand and manage risk while meeting growing regulatory expectations, maintaining market reputation and boosting internal standards and company culture.

We have produced this report to explore the prevailing trends in corporate investigations today. Drawing on insights from professionals across the legal, compliance and forensic fields, it brings together seven articles that illustrate how the discipline is evolving in response to AI, the prevalence of digital data, and the shifting enforcement priorities of US regulators.

A central theme running throughout the report is the growing importance of trust. This is explored from multiple perspectives, beginning with our roundtable discussion, where senior practitioners reflect on the evolution of internal investigations and the increasing professionalisation of the discipline. A key takeaway from this conversation is that effective investigations now hinge not only on technical capability, but also on credibility: organisations must be able to demonstrate to regulators and internal stakeholders that concerns are taken seriously, assessed rigorously and resolved fairly.

This challenge is amplified by changes in how concerns are raised. As explored in our article on whistleblowing, organisations are contending with an expanding volume of reports, alongside the emergence of malicious or misleading submissions – including those enabled by AI. This creates a delicate balancing act: ensuring robust investigative processes while preserving the integrity and intent of speak-up frameworks. At the same time, the evidential landscape is changing. S-RM's digital forensics experts examine the growing role of data and analytics in investigations, from the expanding range of digital evidence available to investigators, to the increasing importance of evaluating its provenance and authenticity. Digital evidence now sits at the heart of many complex matters, but its effective use depends on the careful selection and interpretation of the appropriate data sources.

Alongside these developments, the report highlights the continued relevance of more traditional investigative disciplines. Our

piece on forensic accounting demonstrates how financial analysis remains a critical tool in uncovering misconduct and identifying risk exposure, particularly in complex, cross-border contexts.

Throughout this report, a clear message emerges: as technological solutions and data-rich investigations continue to grow, the human element remains indispensable. As explored in our article on the enduring role of investigators, judgement, experience, ethics and interpersonal skills are critical to effective outcomes. Whether conducting interviews, assessing credibility or navigating sensitive internal dynamics, human expertise cannot be replaced.

The report concludes with a fireside chat examining the increasing complexity of regulatory and compliance environments, particularly in regions like Latin America where legal, geopolitical and commercial risks intersect. This discussion underscores the need for legal and investigative teams with deep local knowledge and expertise to help clients navigate these risks.

Taken together, these insights point to a discipline in transition. Corporate investigations are no longer peripheral to business operations; they are a core component of how organisations maintain integrity, respond to scrutiny and make informed decisions in an uncertain world.

We hope this report provides a useful framework for understanding where the field is heading, and practical insights for those of us who operate within corporate investigations.

Marcus Fishburn
Global Head of Disputes & Investigations

01

Investigations roundtable

Emerging trends and enduring principles

S-RM convened three leading voices from the corporate investigations community to consider how the discipline is changing, and with it the demands on those charged with safeguarding organisational integrity.

Together, Pav Gill, Ashu Sharma and Danny Mayhew reflect on the rapid integration of technology into investigative work, acknowledging the gains in speed, scale and analytical power while emphasising the enduring necessity of sound judgement, proportionality and defensible process.

They also return to a constant at the heart of effective investigations: trust. From whistleblower confidence and protection to the independence and credibility of investigative functions, the panellists underscore that a speak-up culture is sustained not by policy alone, but by visible follow-through and fair outcomes. Finally, our panellists chart the growing professionalisation of investigations and look ahead to the next 12 to 18 months to the trends they expect to impact the world of corporate investigations. The result is a forward-looking conversation offering practical insights for practitioners navigating an increasingly complex and highly scrutinised landscape.

Pav Gill
Founder of Confide Platform and Wirecard whistleblower

Pav Gill blew the whistle on Wirecard as its Head of Legal for the Asia-Pacific region. EUR 24 billion in market value was erased, executives were jailed, and the COO is now one of Europe's most wanted fugitives. The fallout triggered regulatory reform across Europe, from whistleblower protections to payments oversight.
Pav is the recipient of the ACFE Cliff Robertson Sentinel Award 2022 (inscribed "For Choosing Truth Over Self") and the Blueprint for Free Speech Award 2021. His story is told in the critically acclaimed Sky Studios documentary Wirecard: A Billion Euro Lie.

Ashu Sharma
Group Investigations Manager, Anglo American

Ashu is a Corporate Investigator with 25 years of experience in mining, banking, law enforcement, and the UK regulatory sector, in leadership and subject matter expert roles. He is a Certified Corporate Investigator, Certified Fraud Examiner, a Certified Compliance and Ethics Practitioner, and is a category A liaison advisor for the International Organization for Standardization. In addition to leading special investigations for a global mining company, he is also Chief Strategy Officer for the Association of Corporate Investigators.

Danny Mayhew
Global Head of Organisational Justice and Smart Assurance, Sanofi

Danny brings over 30 years of global compliance and investigative leadership across life sciences, energy, and law enforcement. As Sanofi's Global Head of Organisational Justice & Smart Assurance since 2022, he leads enterprise-wide ethics and compliance programs across 100+ countries, including the Global Speak-up & Ombuds Office, global investigations, AI-powered monitoring, and disciplinary frameworks. Danny has been a member of the Guide House Pharma Forum since 2017.

Q How have you seen the landscape of corporate investigations evolve over the past three years?

Ashu Sharma "Corporate investigations have become more professionalised and collective. Bodies such as the Association of Corporate Investigators (ACi) and standards like ISO 37008 Internal Investigations of Organisations have helped shift investigations ***from reactive and disjointed activities to a recognised, globally aligned discipline*** with shared principles, ethics, and competencies."

Danny Mayhew "There has been a significant professionalisation of the investigations function itself. Investigators are no longer drawn exclusively from legal or audit backgrounds — we now see multidisciplinary teams combining forensic accountants, data scientists, HR specialists, and former regulators. But ***the most striking shift has been the move from reactive to proactive investigation models.*** Three years ago, most organisations — including many in pharma — were largely waiting for a complaint to land before mobilising investigative resources. Today, the best-in-class programmes are using continuous monitoring, data signals, and behavioural analytics to identify potential misconduct before it escalates."

Pav Gill "Corporate investigations have become faster. The time available to protect the reporter, preserve evidence and decide whether the issue has wider implications has compressed dramatically. The type of issue has also shifted. Bribery, accounting concerns and conflicts of interest are still there, but they increasingly sit alongside cyber-enabled fraud, sanctions exposure, supply-chain failures, and ESG-related allegations and misconduct driven by pressure to meet targets that were never realistic to begin with. The investigation often ends up revealing as much about governance, incentives and culture as it does about the underlying allegation."

Q How has the role of technology impacted your approach to investigations?

Pav Gill "Technology has changed investigations in two directions at once. ***Analytics, forensic review, communications mapping and anomaly detection have made it possible to spot patterns faster than any team of investigators could on their own.*** At the same time, the discipline expected from investigators has gone up. Every data pull, AI-assisted summary and forensic step needs to be explainable, proportionate and properly recorded, because anything less gives the other side something to attack."

Ashu Sharma "***Technology has shifted investigations from reactive to insight-led***, allowing earlier detection, better scoping, and more proportionate responses. For example, AI enabled document review and triage, when properly governed, has had an impact in reducing investigative burden while improving consistency and focus. However, it has also raised expectations around speed, consistency, and auditability."

Danny Mayhew "***Technology has fundamentally changed what is possible in terms of scale and speed.*** Digital forensics capabilities that once required weeks of manual review can now be completed in hours. At Sanofi, we use analytics to monitor transactional patterns, third-party interactions, and process deviations in near real-time, which means our investigations often begin with a much richer evidentiary picture than

was previously possible. ***However, technology is an enabler, not a replacement for judgement.*** The most sophisticated data model still needs an experienced investigator to interpret context, assess credibility, and make sound decisions about proportionality and fairness — technology informs and accelerates, but humans decide. This is particularly important in a regulated industry where the integrity of our processes is itself subject to scrutiny."

How is collaboration between compliance, legal, and investigations evolving?

Ashu Sharma "***We are seeing a move away from siloed functions toward risk-based, multidisciplinary models***, with investigations acting as a coordinating function rather than a downstream recipient of issues."

Danny Mayhew "What I see evolving, and what we are actively building at Sanofi, is ***a more integrated operating model where legal, compliance and investigations share intelligence, align on risk appetite, and coordinate responses in real time***. Externally, I also see a growing maturity in how organisations engage specialist external counsel and forensic firms. The best relationships are genuine partnerships, where external expertise is brought in strategically to supplement internal capability rather than replace it."

Pav Gill "I expect ***closer collaboration between legal, compliance, HR, audit, cyber and external advisers as risks converge***. A sanctions issue can pull in payments, third parties, trade controls and employee conduct in the same morning. A cyber incident can involve fraud, privacy, disclosure obligations and a cultural problem all at once."

What role do whistleblowers play in shaping the future of investigations?

Danny Mayhew "Whistleblowers are, frankly, one of the most important sources of intelligence available to any investigations function. The data consistently shows that internal reports — whether through formal hotlines or informal channels — surface misconduct that would otherwise remain hidden for years. The single greatest driver of whistleblower confidence is evidence that previous reports were taken seriously. ***Organisations that close the loop — even partially — see significantly higher reporting rates over time, which is ultimately what a healthy speak-up culture looks like.***"

Ashu Sharma "***Whistleblowers are a primary source of intelligence, not just reporters of misconduct***. Their contribution must be recognised through better feedback loops, stronger protections, and visible organisational accountability. They already have a role but there is still much work to do to recognise their importance and protect them. That said, ***not all speak-up is whistleblowing, and this is why competent investigators are essential.***"

Pav Gill "***Whistleblowers are often the earliest reliable signal that something is wrong.*** People usually see the problem before the data does: the pressure, the workaround, the fear, the fake explanation and the decision that does not make sense to anyone in the room. The hardest challenge is trust. A company can have a policy, a hotline and a case number, but ***if employees believe the process protects the institution before the truth, the investigation is weakened before it begins.***"

THE WIRECARD WHISTLEBLOWING CASE – PAV GILL

The Wirecard scandal broke in June 2020 when a major part of the German fintech company's business was found to be fraudulent, with a sum of EUR 1.9 billion supposedly held in accounts in the Philippines revealed to be non-existent. Pav Gill led the whistleblowing on Europe's largest corporate fraud. Here, he provides a short case study on how he was able to bring the fraud to light and what lessons he learned about whistleblowing as a result.

"At Wirecard, the person who came to me was from the finance team. The first thing I had to do was protect her. I gave her a code name, "Bobby", that gave away nothing about her, not even her gender, and I held that code name across every internal conversation we had. The second thing was to preserve her account quickly, while the facts were fresh and before fear or second-guessing could start to take over. Sources in this position can begin with real conviction, then become fearful, question themselves and try to pull back from the process. The capture at the front end matters more than almost anything that happens later. We had her give a detailed written statement to external counsel in Singapore so that her account was on the record, signed and crystallised before she could second-guess herself.

That experience pushed me toward what I now think of as a "firewalled investigation". One trusted party handles the source from end to end and liaises with the investigation team on the source's behalf. That keeps the source from being thrown across multiple channels and unfamiliar people, which is one of the fastest ways to lose them entirely.

Recognising whistleblower contributions is not complicated in principle. They want safe channels, protection from retaliation, timely updates and visible evidence that substantiated reports lead to action. Most are not looking to become public figures. They want the issue taken seriously and they want to know they will not be punished for telling the truth. And too often, neither happens."

What's next for Corporate Investigations? What are the trends to watch in the next 12–18 months?

Pav Gill "In the next 12 to 18 months, speed and triage will matter even more. Companies will have to decide quickly whether a report is credible, who should own it, what evidence has to be preserved and whether there is a regulatory disclosure issue. Slow or defensive handling now carries its own risk."

Ashu Sharma "Greater regulatory scrutiny of internal investigations. The SFO and other law enforcement as well as regulatory bodies are now paying attention. Increased use of AI and data analytics in triage and during evidence review. More expectation of investigator independence and defensible decision-making by employees and the community."

Danny Mayhew "AI-assisted investigations will move from pilot to mainstream. We're already seeing early adopters use large language models to process vast volumes of communications data, identify anomalous patterns, and prioritise case queues. Over the next 18 months, I expect this to become a baseline expectation rather than a differentiator."

SHARPENING YOUR APPROACH

S-RM's advice for organisations to strengthen their investigative procedures

- Build the investigation framework before a crisis arises, with clear intake, triage, evidence preservation, escalation, and remediation processes.
- Invest in skilled, independent investigators and professional standards, with strong training, clear principles, and credible oversight.
- Use technology and AI to support triage, review, and pattern detection, but keep human judgement, fairness, and accountability at the centre.
- Strengthen whistleblowing arrangements through trusted reporting channels, anti-retaliation protections, timely updates, and visible follow-through on substantiated concerns.
- Create integrated ways of working across legal, compliance, HR, audit, cyber, and specialist advisers so responsibilities are clear and investigations are coordinated.
- Prepare for cross-border and regulatory complexity in advance through jurisdiction-specific protocols, local legal input, and disciplined documentation.
- Treat investigations as a source of organisational learning by measuring quality, identifying root causes, and using case insights to improve governance, culture, and controls.

02

From whistleblower to threat actor

Dealing with malicious speak-up reports

Philippa Wilkinson, Associate Director, Disputes & Investigations

Compliance officers are experiencing a wave of spurious reports to whistleblowing hotlines, with AI chatbots being used to generate lengthy, vague and implausible complaints. This especially affects higher profile companies, in particular those with significant scale, consumer-facing brands, or controversies around their operations. Some whistleblowers use AI in good faith to refine and structure their allegations in the most effective way. Unfortunately, this can result in lengthy complaints framed in legalistic language but lacking substance on the underlying issues, and sometimes actively undermining their severity.

Worse, a significant proportion of AI-assisted reports are spurious or even malicious, wasting the time of compliance officers and investigators, and distracting from genuine concerns. A small minority can reach the level of harassment, requiring a change in approach as they escalate. But any hasty attempt to respond forcefully to what internal stakeholders perceive as malicious reports could breach whistleblowing regulations aimed at protecting good faith reporters.

Based on our experience, in this article we set out the practical and technical steps compliance teams should consider when a reporter making spurious complaints shows signs of increasing escalation. We first consider what we define as 'nuisance' behaviour, such as repeated false complaints which could be characterised as harassment. We then explore the options that open up once a reporter crosses the line into malicious activity – such as threatening, defamatory or even criminal behaviour – to defend against this threat.

Dealing with the initial report

Based on both external regulations and a carefully developed whistleblowing policy, compliance teams have a duty to take seriously every report submitted via formal or informal whistleblowing channels. Even if a report contains multiple red flags, such as conspiratorial language or implausible exaggerations, initial triage should proceed as normal. Even genuine whistleblowing allegations can come couched in extreme and emotional language, especially if the whistleblower is already experiencing intense pressure or retaliation from immediate colleagues.

The process should include responding to the reporter promptly, requesting key details and clarifications from them, and carrying out an initial review to corroborate any sufficiently specific allegations. This might include confirming whether named employees, suppliers or customers actually exist, and whether the specific allegations are plausible in the context of the company's operations. For example, when a client of ours received an allegation that their raw materials were being diverted from a factory to manufacture illegal recreational drugs, the team was quickly able to rule out this scenario by comparing lists of chemicals they procured with known drug precursor lists. The investigation continued, but was downgraded to a case of potential theft. The original whistleblower report looked like a precursor to an extortion attempt, but by not panicking and taking some early investigative steps, the client put themselves in the position to send a carefully-calibrated and defensible response, after which the reporter stopped communicating.

> **"An overly dismissive approach exposes the company to criticism during audits or regulatory reviews [...] In the worst case scenario a hasty dismissal of the report could be characterised as a cover-up"**

Compliance officers cannot give in to the temptation to skip this initial review and immediately dismiss a report due to the perception created by the presentation of the allegations. An overly dismissive approach exposes the company to criticism during audits or regulatory reviews of the compliance function. In the worst case scenario, if a specific allegation later turns out to be accurate, a hasty dismissal of the report could be characterised as a cover-up. Based on the findings of the initial review, any sufficiently specific and plausible allegations should result in an investigation, in line with the company's policies.

Minimising contact

Some nuisance reporters escalate their behaviour by making repeated false allegations anonymously via formal and informal whistleblowing avenues. AI has driven a noticeable increase in the volume and length of these communications, by facilitating very rapid drafting and hallucinating superficially plausible details. These repeated communications can accelerate when not met with an immediate or public response to their allegations. To avoid overwhelming already stretched compliance teams, a simple workflow can be put in place to extract any new details and manage the wider impact.

Nuisance reporters sometimes begin directly emailing increasing numbers of employees, usually starting with the most senior, or even board members. If they are an insider with a grievance, they may have access to address books or mailing lists with large numbers of employees. Left unaddressed, this can drive speculation and affect morale among employees. Some thought should therefore be given to engaging senior stakeholders and addressing communications received by large numbers of staff, to reassure them without compromising the confidentiality of any ongoing investigation. Internal IT teams can also adjust settings on mailing lists intended for internal use to block all emails from external domains. If a nuisance reporter starts targeting a company's clients, then it is critical that a communications strategy is put in place immediately to mitigate the commercial risk.

In dealing with a reporter escalating from whistleblower reports to nuisance communications, companies should continue to abide by their existing policies and templates for communications. Short, formulaic responses avoid giving nuisance reporters ammunition or motivation to escalate to a campaign of harassment, as well as respecting the confidentiality of any ongoing investigation. Once reasonable investigative steps have been carried out (and assuming the allegations cannot be substantiated), all contact can be cut. Certain steps can be taken to minimise the impact of repetitive communications, most importantly blocking known email accounts. However, a determined nuisance reporter can easily create new email accounts. Another method is to fingerprint the reporter's spelling, choice of vocabulary and turns of phrase – and filter out communications on that basis. For example, S-RM worked on one matter where a nuisance reporter's unique misspelling of the word 'corrupt' meant that their outreach to various of the client's employees was easily blocked. Companies can work with their IT teams to

tighten spam protection, as well as data loss prevention measures which make it harder for insiders with a grievance to exfiltrate sensitive documents for use in this type of harassment campaign.

As long as the allegations are only received internally, especially via dedicated whistleblower hotlines, caution is recommended regarding any proactive steps, for example to identify the reporter. Even though the investigation may have determined the reports to be completely unsubstantiated, and stakeholders perceive that they are being harassed, under whistleblower protection regulations any steps that could be characterised as retaliation might have negative legal and reputational consequences. In cross-border situations, even where the harassment is taking place in a jurisdiction with no whistleblower protections, the group may need to adhere to more rigorous standards than its subsidiaries.

This approach may feel frustrating, especially to any senior stakeholders who have been targeted. However, in this scenario the company has very limited ability to influence the behaviour of the nuisance reporter, beyond avoiding any action which could drive an escalation. Ideally, remaining passive will gradually let a nuisance reporter deescalate and disengage.

Crossing the line

When a malicious reporter crosses the line into possible lawbreaking, a range of options open up. The malicious activity could include blackmail, threats of physical violence, hacking or other theft of confidential information, or defamatory public statements. Legal advice is important to determine whether a nuisance reporter has turned into a truly malicious reporter whose actions justify proactive steps.

> **"If a malicious reporter has improperly obtained, or even published, confidential information, a digital forensic investigation can determine the source of this data."**

If a malicious reporter has improperly obtained, or even published, confidential information, a digital forensic investigation can determine the source of this data. Whether the information has been leaked by an insider, such as a disgruntled employee, or obtained by an external threat actor, understanding the method and extent of the data leakage is critical to ensure any vulnerabilities are patched and legal action can be taken if required. Alongside the digital forensic investigation, open source intelligence ('OSINT') research can support by looking into contact details and social media activity related to the malicious communications or posts to identify information that may assist with attribution.

If an insider has downloaded and shared sensitive documents, or is themselves the malicious reporter, digital forensic experts can gather evidence on corporate systems to demonstrate how, when and by whom the data was accessed and exfiltrated. This can be used to support defensible disciplinary action against any insider threat, as well as any future litigation.

Depending on confidentiality considerations, it may be helpful to make a police report locally, for example if any threats of violence are made, even if this is merely to create a paper trail. Beyond this, understanding who and where your threat actor is, as well as their communications, can also inform a threat assessment. A threat assessment analyses the motivation, capability, credibility, and intent of a threat actor, and can be used to fortify a company's approach to the security of employees and facilities in response.

The culture question

Attempting to determine the motivation of an anonymous malicious reporter tends to be speculative and unproductive. The exception is when it becomes apparent that the source is an insider originally motivated by an arguably justified grievance. It may then be appropriate to take the opportunity to consider cultural issues highlighted by the malicious activity. Remediating cultural problems is not giving in to a malicious reporter's blackmail, but protecting the business from future crises with the same root cause. In one situation we saw, the entrenchment of cliques within a company's local subsidiary led to toxic behaviours in the workplace, and eventually a disgruntled employee exfiltrated confidential documents and shared them with former employees for use in a campaign of harassment. Left unchecked, the toxic aspects of the workplace culture risked alienating more employees and driving a cycle of weaponised false allegations.

03

Navigating FTO exposure in the Americas with forensic accounting

Amalia Coyle, Associate, Corporate Intelligence
Yannine Pasula, Director, Corporate Intelligence
Richard Fogarty, Head of Disputes & Investigations, Americas

In its crusade against drug trafficking organizations in the Americas, as well as globally, the second administration of US President Donald Trump has employed an ever-broadening brush to draw up its list of Foreign Terrorist Organizations ("FTO") and Specially Designated Global Terrorists ("SDGT"). This includes the most recent designations of the Clan del Golfo, a Colombian drug cartel, and the Cartel de los Soles, an alleged network of high-ranking Venezuelan officials connected to ousted president Nicolás Maduro, captured by US forces in January 2026. Launched at the very beginning of Trump's second term in January 2025, the anti-cartel campaign promises only further escalation, and with it a minefield of legal, compliance, and reputational risks for businesses operating in the region. In this complex landscape, forensic accounting to identify the true source of funds plays a critical role in helping businesses and legal counsel identify, quantify, and mitigate financial exposure to FTOs and SDGTs.

The expanding FTO risk landscape in the Americas

The current US stance, though significantly more stringent and far-reaching than in previous administrations, is not unprecedented, and nor are the risks of FTO designations for companies doing business in the Western hemisphere. In 2007, multinational banana producer Chiquita Brands International ("Chiquita") pleaded guilty to US federal criminal charges for making payments to the Autodefensas Unidas de Colombia ("AUC"), a Colombian paramilitary group designated as an FTO in 2001. Chiquita's board of directors disclosed the payments to the US Department of Justice in 2003 after a senior Chiquita officer and board member raised the issue of the company's ongoing payments to a designated FTO. At the time of the plea, Chiquita agreed to pay a USD 25 million fine, though the repercussions for the company have continued as recently as 2024, when a federal jury in Florida found Chiquita liable in a long-running civil case for the deaths of people killed by the AUC and ordered the company to pay USD 38.3 million to 16 family members of the deceased.

Beyond the Americas, the more recent case of French building materials company Lafarge SA ("Lafarge") also reflects the potentially severe repercussions of FTO designations. In October 2022, Lafarge and its Syrian subsidiary pleaded guilty to conspiring to provide material support to the Islamic State of Iraq and al-Sham ("ISIS"), a designated FTO since 2004, and the al-Nusrah Front, designated as an FTO from 2014 to 2025. As a result, Lafarge was ordered to pay criminal fines and forfeiture totalling nearly USD 778 million.

Notably, when Chiquita pleaded guilty to supporting an FTO in 2007, only four organizations in the Americas were designated as FTOs, including the AUC. The designation of an additional 15 Americas-based organizations as FTOs since the beginning of 2025 [1] has already made prosecutorial waves, with US authorities bringing charges against a number of individuals and entities for providing material support to FTOs. In many cases, these charges have expanded to include other predicate crimes, such as drug trafficking. In March 2026, for example, a federal grand jury in Ohio brought charges against two Chinese pharmaceutical companies and six Chinese nationals for narcotics trafficking and money laundering conspiracies as well as providing material support to the Cartel del Golfo, a Mexican cartel designated as an FTO since February 2025.

[1] This figure does not include Primeiro Comando da Capital (PCC) or Comando Vermelho (CV) due to be added in early June 2026

Thought not exactly linear, logic dictates that with the almost four-fold increase in organizations designated as FTOs in the last two years compared to pre-2025, exposure to FTOs and their activities as well as potential prosecutions and regulatory scrutiny will also increase significantly.

The pressure and scrutiny that companies face extends beyond US authorities and into the media. In April 2026, US law enforcement reportedly executed a federal search warrant at the headquarters of Ikon Midstream, a Texas-based fuel trader, as a result of an October 2025 exposé by Reuters implicating the company in alleged fuel smuggling into Mexico. Reuters accused Ikon Midstream of exporting a shipment of diesel in March 2025 which ended up in the possession of a Mexican company suspected of being a front for the Cartel de Jalisco Nueva Generación ("CJNG"), a Mexican cartel designated as an FTO.

Companies must also contend with the very real prospect of further FTO designations, including the reportedly looming designation of the Brazilian criminal organizations Primeiro Comando da Capital ("PCC") and Comando Vermelho. [2] The PCC has recently been linked to multiple actors in the Brazilian financial services sector, including financial institution Banco Master SA and brokerage CBSF Distribuidora de Títulos e Valores Mobiliários SA (formerly Reag Trust), which were forcibly liquidated by Brazil's central bank in November 2025 and January 2026, respectively, as a result of a major fraud scandal.

> **"Forensic accounting is essential in reconstructing financial data, tracing illicit funds, and translating complex financial data into defensible legal evidence."**

Why forensic accounting matters in FTO investigations

In scenarios such as these, when a potential risk exposure has already been identified, whether by the authorities, media, or the public, forensic accounting is essential in reconstructing financial data, tracing illicit funds, and translating complex financial data into defensible legal evidence. It is critical to bring in forensic accountants at the outset of an investigation, as they will be key contributors to multidisciplinary investigative teams by identifying problematic activity and patterns within the financial data. More specifically, forensic accountants can uncover disguised payments; highlight internal control

[2] On May 29, 2026 the US Department of State did designate Comando Vermelho (CV) and Primeiro Comando da Capital (PCC) as Specially Designated Global Terrorists (SDGTs) and intends to designate both groups as Foreign Terrorist Organizations (FTOs), effective June 5, 2026.

vulnerabilities where oversight and proper approvals are lacking; quantify funds moved through complex accounting schemes over multiyear spans; simplify bank records; and document key evidence at every step – all important data in the context of identifying exposure to FTO activity.

> **"Forensic accounting can also complement the efforts of companies taking a proactive approach — including self-disclosure—to potential FTO exposure."**

Proactive risk management and internal investigations

Forensic accounting can also complement the efforts of companies taking a proactive approach—including self-disclosure—to potential FTO exposure. In November 2025, Kodiak Gas Services Inc ("Kodiak"), a Texas-headquartered provider of natural gas services, disclosed in its quarterly report to the Securities and Exchange Commission that it had identified certain payments to local government officials in Mexico related to one of its affiliates that may have indirectly benefitted individuals associated with FTO and SDGT-designated cartels. Kodiak reportedly retained outside counsel to conduct an internal investigation, which concluded that payments likely were made to persons associated with an SDGT to protect Mexican employees from threats of harm or harassment and to ensure worksite access.

For companies undertaking this type of internal investigation and implementing proactive measures, forensic accounting assists in due diligence measures, understanding requirements such as beneficial ownership of third parties, detecting and preventing hidden transaction patterns, and implementing proper approval matrices. A routine proactive risk assessment can evaluate whether policies and procedures are implemented and whether ongoing transaction monitoring and data analytics are consistent with the company's risk-based appetite, as well as highlighting any internal control gaps that may leave clients with significant exposure. In short, forensic accounting and investigative expertise are key in helping companies ensure regulatory compliance and strengthen both their risk mitigation and potential legal strategies.

The parallels between the Kodiak self-disclosure and the origins of the Chiquita case, 20 years apart, make clear that despite the precarious and unpredictable expansion of FTO and SDGT designations, forensic accounting expertise remains a consistently critical skillset to help address and mitigate these risks.

04

The range and value of digital evidence in internal investigations

Amy Francis, Head of Digital Forensics

Internal investigations are no longer constrained by what individuals remember, record in formal documents, or choose to disclose in interviews. In most organisations, day-to-day activity leaves a detailed digital footprint across devices, communication platforms, cloud environments and enterprise systems. When an issue arises – whether suspected misconduct, fraud or the theft of sensitive information – the initial focus often turns to interviews, document review and email searches. But behind these traditional sources sits a richer record: the digital traces left by everyday activity.

For legal and investigations teams, the implication is clear. Digital evidence is not merely supplementary. In many internal investigations, it is central to establishing what happened, when it happened, who was involved and why. It can corroborate witness accounts, challenge incomplete narratives, identify new lines of enquiry and, in some cases, provide the only reliable record of events.

The challenge is rarely the absence of data. It is knowing where to look, what to preserve, and how to prioritise the sources most likely to answer the questions at the heart of the investigation. Taking the same approach in every case – for example, beginning with an email review and expanding from there – is not always the most effective or proportionate way to proceed. Different allegations create different evidence profiles and understanding that at the outset can materially affect the speed, cost and outcome of an investigation.

WHAT IS DIGITAL EVIDENCE?

Digital evidence encompasses any data created, stored or transmitted through electronic systems that can assist in establishing facts relevant to an investigation. In practice, this extends far beyond emails, documents or chat messages. Common sources include:

- **End user devices:** Laptops, desktops and mobile phones can show how an individual interacted with files, applications and communications platforms. They may contain locally stored documents, deleted data, user activity records, and evidence of files being opened, copied, downloaded, compressed, transferred or removed.
- **Communications platforms:** Corporate email, Microsoft Teams, Slack, SMS, WhatsApp and other messaging platforms can show correspondence between individuals, identify wider participants, and provide context around key events.
- **Enterprise systems:** Microsoft 365, Google Workspace, document management systems, financial platforms, HR systems, databases and other business applications often contain audit records showing sign-in activity, file access, permission changes, downloads, deletions and administrative actions. These records can be particularly valuable where the issue concerns access to sensitive information or manipulation of business records.
- **Other log sources:** Network logs, security tooling, VPN records and data loss prevention tools can provide further visibility over suspicious behaviour, data transfers and unusual access patterns.

The value of digital evidence

When leveraged properly, digital evidence can help establish a clear chronology of events: who accessed a system, when a file was opened or downloaded, whether data was transferred, and how activity developed over time. This is particularly important where witness recollections are incomplete, inconsistent or influenced by hindsight.

It can also provide insight into intent. Communications may show whether an action was accidental, authorised, concealed or coordinated with others. System records may show whether behaviour was consistent with an individual's normal role, or a departure from expected activity.

Digital evidence can also corroborate or challenge accounts, linking activity to particular users, devices, accounts or locations. When multiple sources are analysed together, they can provide a more complete and defensible understanding of events than any single source could provide in isolation.

In short, digital evidence enables an investigation to move beyond assertion and towards a clearer, more reliable understanding of the facts.

Different cases, different evidence profiles

Not all digital evidence is equally valuable in every investigation. The right sources to prioritise depend on the allegation, the systems involved, the individuals under review and the decisions the organisation may need to make.
This is where early scoping becomes critical. A well-scoped investigation does not simply ask, "What data do we have?" it asks, "What are we trying to prove or disprove, and which sources are most likely to help us do that?" That distinction can prevent unnecessary review of low-value material, reduce cost, and allow the investigation team to identify key evidence quickly.

1

Data/IP theft

In cases of suspected intellectual property theft or misuse of sensitive information, the central questions are practical and technical. What information was accessed? Was it downloaded, copied or transferred? Did the individual have permission to access it? Where did the data go? In these investigations, the priority is to follow the data.

The most valuable sources will usually be audit logs from enterprise systems containing sensitive data, the user's laptop or desktop, and supporting logs from network or security tools. Corporate email may also be relevant, particularly where files were sent externally to third parties or, more commonly, personal email addresses.

Forensic analysis in these matters often focuses on unusual access to sensitive files, large downloads from cloud platforms, transfers to external destinations, remnants of deleted files, synchronisation with personal cloud services, or evidence of files being copied to USB devices.

2

Behavioural misconduct

Employee misconduct investigations often have a different evidence profile. The issue may concern harassment, bullying, conflicts of interest, misuse of company resources, inappropriate communications, or breaches of policy. Here, the central questions are often less about data movement and more about conduct, context and intent.

The most relevant sources are usually communications platforms and user devices. Corporate email and Teams or Slack messages may capture formal or semi-formal interactions between the individuals involved. Mobile devices can be particularly valuable where personal messaging, SMS, WhatsApp, photographs, screenshots or call records are relevant and lawfully available for review. A single screenshot or forwarded extract can be persuasive, but it may not show the full conversation (see Trust and authenticity in a digital age). Reviewing material from the source system or device can help establish whether the extract is complete, whether messages were deleted, and whether the context changes the meaning of the exchange.

In misconduct matters, digital evidence is often most valuable when used alongside interviews and HR records. It can support a complainant's account, challenge a respondent's explanation, identify witnesses, or show that an issue formed part of a wider pattern.

3

Financial misconduct

Fraud and financial misconduct investigations usually require a combination of transactional, system and communications evidence. The issue may involve false invoicing, manipulation of approvals, conflicts of interest, diversion of payments, misuse of expenses, or circumvention of controls. The central questions are likely to include what happened within the financial system, who authorised or enabled it, and whether the activity was intentional.

The most important sources are often enterprise systems containing financial records, such as accounting platforms, ERP systems, procurement tools and relevant SaaS applications. System logs can show who created, amended or approved transactions, whether access controls were bypassed, and whether unusual activity occurred at key points in the process. Corporate email and messaging platforms along with computers used by the individuals involved can then provide communications to help show intent, identifying discussions about contracts, invoices, vendors, approvals, payment timing or commercial pressure.

In these matters, no single source is likely to provide the complete picture. The value comes from connecting records across systems to build a timeline of events: the transaction in the financial platform, the approval in the workflow tool, the email explaining the urgency, the document stored on the laptop, and the login record showing who accessed the system at the relevant time.

The importance of early forensic scoping

The early stages of an investigation are often the point at which the most important decisions are made. They are also the point at which evidence is most vulnerable.

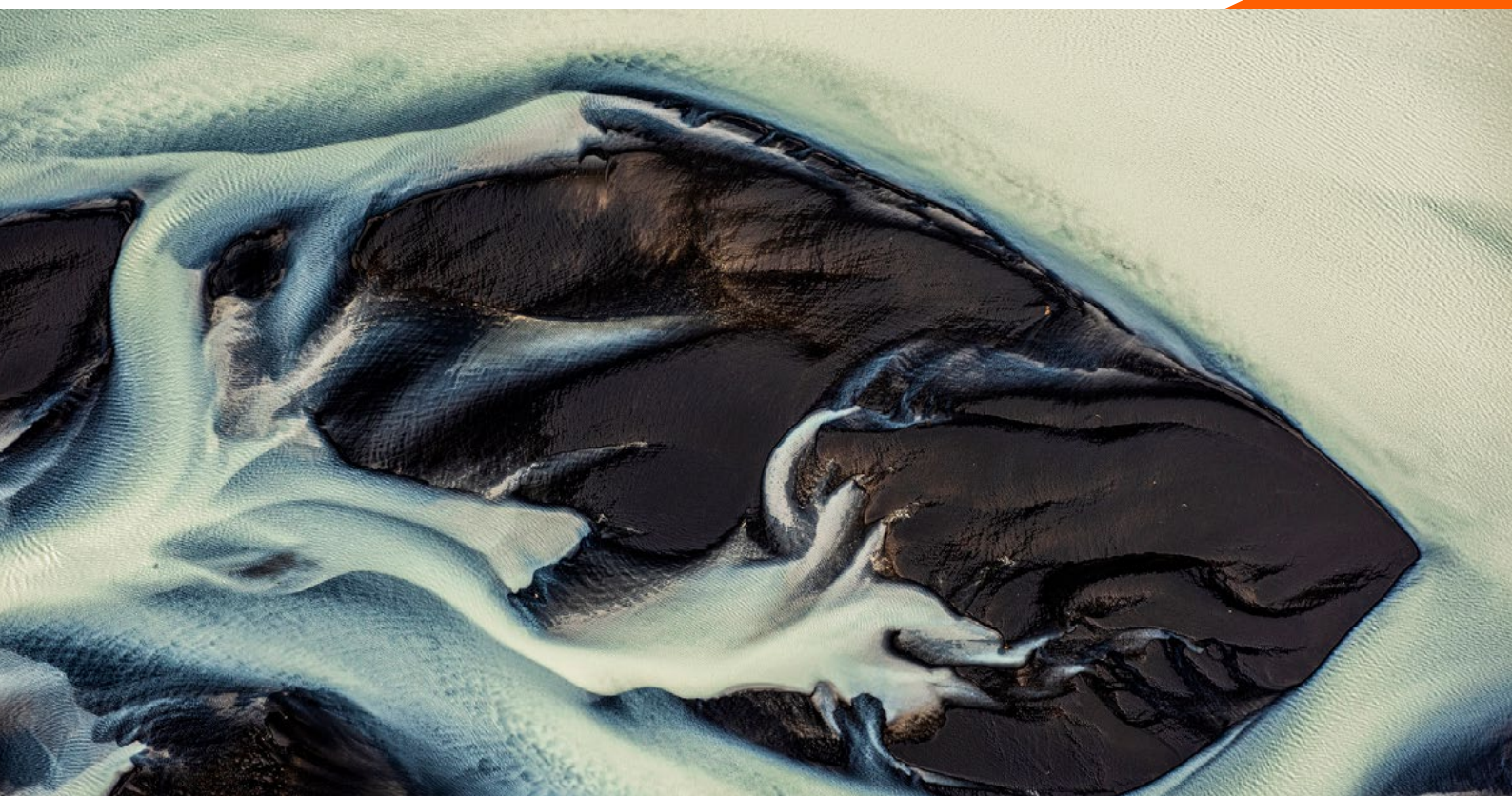
Digital evidence can be overwritten through continued use of devices. Forensic artefacts and system records may be replaced by newer activity. Data can be deleted accidentally through retention policies or deliberately by individuals who become aware of an investigation. Access can also become more difficult over time, particularly where employees leave, devices are returned or wiped, accounts are deactivated, or legal and practical windows for preservation narrow.

Whilst proportionality remains important, early involvement of digital forensics specialists helps mitigate these risks. It ensures that evidence is preserved in a timely and defensible manner, before gaps appear that cannot later be repaired. It also allows the investigation team to understand, at the outset, which evidence sources are likely to be most valuable given the nature of the allegation and the organisation's infrastructure.

Conclusion

Digital evidence has changed the way internal investigations are conducted. It provides a level of detail that witness recollections and document review alone often cannot achieve. It can establish timelines, attribute activity, reveal intent, and test competing accounts of events. But its value depends on knowing where to look and how to interpret what is found. An IP theft investigation, an employee misconduct matter and a financial misconduct review may all require digital evidence, but they will not necessarily require it from the same sources. The most effective investigations recognise this early and align evidence collection with the questions that need to be answered.

For legal and investigations teams, the message is clear: digital evidence should be scoped deliberately, preserved quickly and analysed in context. With early forensic input, organisations can move faster, reduce evidential risk and reach conclusions that are not only better informed, but more defensible.



05

Trust and authenticity in a digital age

Ryan Shields, Associate Director, Digital Forensics

Investigations have traditionally operated on a relatively stable premise that once digital evidence is obtained, a degree of reliability can be assumed. A signed document carries weight. A message thread reflects a conversation. A photograph captures an event. While interpretation has always required care, the authenticity of the underlying material was rarely questioned unless there was some specific reason to doubt it. Now, that premise is increasingly difficult to sustain.

As the capabilities of technology increase, the inherent trust in digital evidence decreases. Documents are now handled in complex eco-systems. Communications are dispersed across platforms and can be easily curated or taken out of context. Even visual media can now be altered or generated with a level of realism that challenges traditional assumptions.

In this environment, it is no longer sufficient for investigators to find evidence and analyse its meaning; they also need to consider what can be established about its origin, integrity and completeness. For legal and investigations teams, this shift is not theoretical. It directly affects how evidence collection should be approached, how conclusions are formed, and ultimately how decisions are defended.

Reliability of digital evidence

In investigations, documents and communications are often a central focus for investigative teams. They establish timelines, record decisions, and provide insight into intent. However, both are increasingly susceptible to forms of manipulation and alteration that are not immediately visible.

Documents often present as final and authoritative but may represent only one version of a broader history. Edits can be made without obvious traces, earlier drafts may be unavailable, and documents can be selectively disclosed in ways that reinforce a particular narrative.

Communications present a different, but related, challenge. Message threads are frequently encountered in fragmented form such as incomplete screenshots or partial exports. These can be highly persuasive, particularly where they appear to show contemporaneous exchanges. Yet they may omit surrounding context, exclude participants, or fail to reflect deletions and edits – which can make completeness difficult to establish in practice. In more extreme cases, entire message conversations can be fabricated prior to disclosure.

Media – images, audio and video files – tend to arise less frequently in investigations but carry their own risks. The growing accessibility of manipulated media and deepfakes means that authenticity can no longer be assumed, and this material requires careful handling.

Taken together, these issues point to a broader conclusion. The challenge is not that digital evidence is unreliable, but that its reliability cannot be assumed from its format or presentation. Each source must be understood in terms of how it was created, what it may omit, and how it aligns with other available information.

> **“The challenge is not that digital evidence is unreliable, but that its reliability cannot be assumed from its format or presentation.”**

The constraints of investigations

If the nature of evidence has changed, so too must the way it is assessed. However, investigations operate under constraints that make this more difficult in practice.

Access to evidence often presents early challenges. Relevant data may sit across personal devices, corporate systems, and third-party platforms. Legal and regulatory considerations may restrict what can be collected or reviewed, particularly in cross-border matters. And in many cases, investigators are reliant on materials provided third-hand by individuals, rather than obtained directly from source systems.

Time is also a critical factor. Investigations are frequently conducted under pressure with decisions required at an early stage – e.g. whether to escalate an issue, take disciplinary action, or make a regulatory disclosure. These decisions cannot always wait for comprehensive forensic analysis.

There is also a question of proportionality. Not every issue justifies extensive technical analysis. In many cases, early involvement of forensic expertise during evidence collection can mitigate many of the authenticity questions that would otherwise arise later.

Reframing the task: from accepting evidence to testing it

In this context, the objective is not only to gather and review evidence, but to test it. This requires a shift in mindset. Rather than asking whether a document, message or file appears credible, the more useful question is: what would need to be true for this evidence to be reliable?

From this starting point, a structured approach can be applied.

- First, consider provenance. How has the material been obtained? Evidence gathered directly from source systems by forensic experts will generally carry more weight than material provided informally or selectively by individuals.
- Second, assess integrity. Are there indicators that the material may have been altered? This does not always require detailed forensic analysis; experts can quickly identify inconsistencies in formatting, file properties, or content which can be sufficient to raise questions.
- Third, evaluate completeness. What is not present? For communications, this may include missing messages or participants. For documents, it may involve the absence of drafts or supporting materials. Gaps are not always problematic, but they should be identified and understood.

This approach does not eliminate uncertainty but instead provides a baseline for early decision making.

FIGURE 1

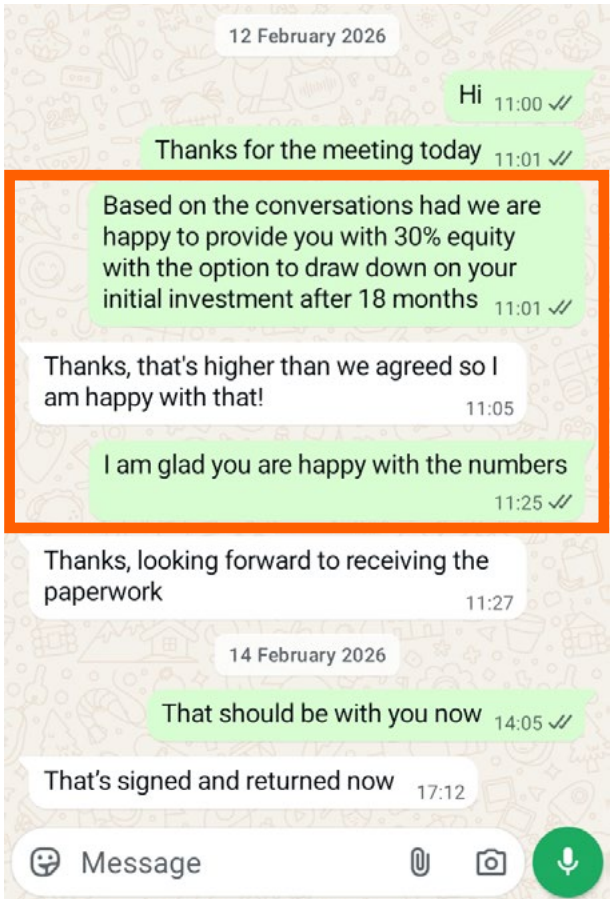
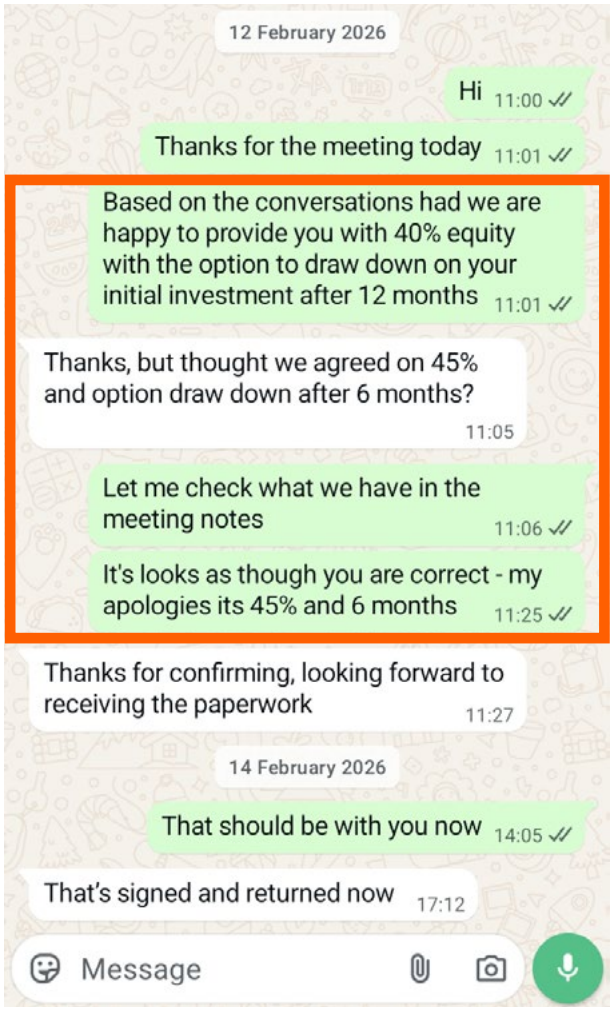


FIGURE 2



Consider Figure 1– the screenshot appears to be a series of messages exchanged between two users on WhatsApp. From an evidential perspective, the conversation appears straightforward: the messages are ordered chronologically, and the timestamps indicate when the exchange took place.

Now consider Figure 2. Both screenshots appear legitimate, yet the contents of the messages, specifically the details of the contractual agreement, are different. This is where many disputes arise: two seemingly genuine sets of screenshots are presented, each convincing to the casual observer, but contradictory to one another and therefore contentious in their veracity.

When a screenshot is provided in isolation, the image itself effectively becomes the sole source of evidence for that conversation, and one that – as illustrated above – can be easily manipulated. This example raises important questions that legal experts and forensic examiners must consider when evaluating evidence: who created the screenshots, when were they captured, and from what underlying data source were they generated? Without access to the original message databases stored on the device or within the messaging application's backups, it is often difficult for forensic investigators to answer these questions with certainty.

Knowing when to escalate is important. Not every issue requires detailed forensic analysis, but some undoubtedly do. The challenge lies in identifying the threshold. Indicators for escalation may include:

- material inconsistencies between different sources of evidence;
- gaps that cannot be reasonably explained;
- evidence that is central to a high-stakes decision; or
- reasonable concerns about potential manipulation or selective disclosure.

Where one or more of these factors are present, deeper analysis is more likely to be justified.

Practical implications for legal and investigations teams

One of the most important steps in any investigation now occurs at the outset: identifying where evidential risks are likely to arise.

If a case is expected to rely heavily on chat communications, for example, early consideration should be given to how complete those records are likely to be, and whether access to source devices or systems will be required. This upfront framing allows early mitigation of authenticity and completeness risks, reducing the need to revisit assumptions later in the process.

Certain types of evidence – particularly message extracts and standalone documents – can be highly persuasive. They appear clear, direct and contemporaneous. In practice, they are also the forms most susceptible to selective presentation or manipulation (as demonstrated in our example).

Investigators need to resist the instinct to treat such material as determinative in isolation; instead, it should be viewed as one component of a broader evidential environment which should be tested against other supporting information.

For legal teams, this has implications for how findings are articulated. Conclusions that rely heavily on a single piece (or even a single category) of evidence, without verification or acknowledging its limitations, are inevitably more vulnerable to scrutiny and challenge.

Communicating in terms of confidence, not certainty

The binary distinction between "authentic" and "inauthentic" is often too rigid for the realities of digital evidence. A more effective approach is to frame conclusions in terms of levels of confidence, supported by clear reasoning. This means explaining not only what the evidence suggests occurred, but how much weight can reasonably be placed on it. This allows decision-makers to understand not only what the evidence shows, but how robust that assessment is.

For example, a conclusion based on a complete WhatsApp exchange extracted from the source device, will carry significantly more weight than one derived from a small number of screenshots provided by a single individual. Both may point in the same direction, but the level of confidence is materially different.

For decision-makers, this distinction is critical. It provides a clearer understanding of the evidential position and any vulnerabilities therein. From a legal perspective, conclusions that acknowledge the varying weight attached to different items of evidence, and their inherent limitations, are more robust and ultimately more defensible.

Conclusion

The evolving digital landscape has not diminished the importance of digital evidence in investigations. If anything, it has increased it. What has changed is the basis on which that evidence can be relied upon.

Documents, communications and media remain central to establishing facts and understanding behaviour. However, their reliability can no longer be inferred from their appearance or format. Each must be considered in terms of its origin, integrity and context.

For legal and investigations teams, the implication is clear. The task is no longer simply to collect and review evidence, but to assess it critically and recognise where limitations may impact confidence levels. This does not require perfect information. It requires a structured approach, sound judgement, and a willingness to engage with uncertainty rather than overlook it.

06

The enduring value of human expertise

Ana Pereu, Associate Director, Disputes & Investigations

Exponential advances in artificial intelligence, machine learning, and data analytics mean that corporate investigations – once dominated by painstaking manual reviews and human intuition – are now increasingly augmented by tools capable of crawling all corners of the internet and processing vast datasets at unprecedented speed. Whether it is e-Discovery tools sorting through millions of documents in seconds or open-source intelligence ('OSINT') platforms mapping out global connections in real time, these advances have given investigators a powerful advantage.

Despite these technological advancements, one principle remains constant: technology serves to assist rather than replace the investigator. The enduring value of human expertise lies not merely in interpreting machine-generated outputs, but in asking the right questions in the first place, exercising judgment under uncertainty, and navigating the complex interplay of legal, ethical, and emotional factors that no algorithm can yet fully replicate.

Technology's strengths and blind spots

Today's investigative landscape is shaped by tools that thrive on vast scale and complexity. E-Discovery platforms, employing predictive coding and natural language processing, can sift through large amounts of data to pinpoint crucial documents, delivering impressive gains in efficiency and reductions in cost. Similarly, forensic accounting software is adept at highlighting suspicious activity within intricate financial systems, while digital forensics solutions are capable of piecing together timelines from fragmented electronic traces. Yet, for all their technical prowess, these tools operate within predefined parameters; they can detect patterns, but they do not necessarily interpret meaning and context.

Consider a cross-border bribery investigation involving thousands of internal communications. A machine-learning model may surface emails containing keywords or items of interest, yet without contextual understanding it may miss sarcasm, attempts at obfuscation, or culturally specific euphemisms. For instance, an understanding of the industry, key players and modus operandi of a corruption scheme can make it very clear if references to "marketing support", "business development expenses" and "after-sales services" are in fact meant to disguise facilitation payments. More critically, on the other side of the equation, there is a risk it may over-prioritise benign communications, creating false positives that obscure genuinely problematic conduct.

> **"Experienced professionals recognise that language is nuanced, intent is rarely explicit, and risk often lies in what is implied rather than stated."**

It is here that the human investigator becomes indispensable. Experienced professionals recognise that language is nuanced, intent is rarely explicit, and risk often lies in what is implied rather than stated. The ability to read between the lines – to understand tone, context, and behavioural patterns – is not something that can easily be codified.

The legal and regulatory imperative

Human oversight is not merely a practical necessity; it is increasingly a legal and regulatory expectation. In jurisdictions such as the United Kingdom and the United States, regulators have signalled that while the use of technology in investigations is encouraged, it must be accompanied by demonstrable oversight and

accountability to ensure defensible outcomes, transparency, and compliance with legal obligations. The October 2025 guidance and interim report published by the Civil Justice Council within the Courts and Tribunals Judiciary clearly states that the use of AI must have "*an appropriate degree of oversight, and within a regulatory framework that ensures compliance with well-established professional and ethical standards if public confidence in the administration of justice is to be maintained.*" Therefore, reliance on automation without adequate human validation might risk challenges to the process further down the line. Where investigative processes involve profiling or significant decisions based on automated analysis, organisations must ensure meaningful human involvement to ensure accuracy, avoid bias and safeguard individual rights.

Similarly, data protection frameworks such as GDPR have implemented additional rules around automated decision-making. For instance, Article 22 applies in the AI context, as it stipulates that automated decision-making can only be carried out where "necessary for the entry into or performance of a contract; authorised by law [...]; or based on the individual's explicit consent." In the context of litigation and regulatory enforcement, authorities may expect investigative findings to reflect reasoned judgment. A conclusion derived solely from technological outputs may be viewed as incomplete or unreliable.

> **"Scepticism also plays a critical role. Investigators must constantly question the reliability of sources, the completeness of data, and the assumptions underpinning their analysis."**

Human emotion, behaviour, and the limits of data

Corporate investigations are, at their core, about people. They involve allegations of misconduct or ethical breaches, often with deeply personal consequences. Technology can identify anomalies, but it cannot fully account for human behaviour. For instance, in an internal fraud investigation, financial analysis may reveal irregular transactions, but understanding the underlying motive – whether financial distress, coercion, or organisational culture – requires human engagement. Interviews, a cornerstone of investigative work, depend on rapport-building, empathy, and the ability to detect inconsistencies in verbal and non-verbal cues. These are inherently human skills.

Scepticism also plays a critical role. Investigators must constantly question the reliability of sources, the completeness of data, and the assumptions underpinning their analysis. Technology, by contrast, operates on the premise that the data it processes is both accurate and sufficient. This creates a risk of over-reliance – a phenomenon sometimes referred to as "automation bias" – where outputs are proffered and accepted uncritically. Experienced investigators, on the other hand, can recognise that the absence of evidence is not evidence of its absence, and that the most significant findings may lie outside the dataset entirely.

OSINT, HUMINT, and the art of corroboration

The volume of information available through social media, corporate registries, satellite imagery, and other publicly available sources provides a rich tapestry of data points. When combined with advanced analytics, these tools can reveal networks, affiliations, and patterns that were previously invisible. However, OSINT is inherently 'noisy' and susceptible to misinformation, obfuscation, and gaps in coverage. Verifying the credibility of sources, distinguishing signal from noise, and corroborating findings remain fundamentally human tasks.

This is where human intelligence (HUMINT) also retains its unique value. Conversations with well-placed sources, contextual or cultural insights from local experts, and on-the-ground perspectives provide depth that no database can replicate. In many cases, the most critical insights emerge not from the digital realm but from information closely held by a small number of people. The most effective investigations integrate OSINT and HUMINT, with human intelligence acting as the bridge between data and its proper interpretation.

Forensic accounting: Beyond the numbers

In forensic accounting, technology has enabled sophisticated analysis of financial data, from transaction monitoring to network analysis of fund flows. Advances in AI have further transformed this landscape, allowing for the automated review of vast volumes of financial documents and records. AI algorithms can swiftly identify unusual patterns, anomalies, or discrepancies in financial data that might otherwise go unnoticed. For example, machine learning models are capable of detecting subtle irregularities across multiple accounts, flagging repeated or linked transactions that fall outside established norms. Natural language processing (NLP) tools can extract and interpret key information from contracts, invoices, and correspondence, helping to uncover hidden relationships or inconsistencies within documentation.

> **"AI can highlight potential issues but cannot always provide the nuanced interpretation required to distinguish between deliberate wrongdoing and genuine mistakes or acceptable practices within a firm's risk appetite."**

Yet even with financial misconduct, the numbers do not tell the whole story. Determining whether an irregular transaction constitutes fraud, error, or legitimate business practice requires judgment and an understanding of accounting principles, relevant regulatory guidance, industry norms, contractual frameworks, and organisational context. Human expertise remains crucial, as AI can highlight potential issues but cannot always provide the nuanced interpretation required to distinguish between deliberate wrongdoing and genuine mistakes or acceptable practices within a firm's risk appetite.

For instance, a series of payments to a third-party consultant may appear suspicious in isolation. AI-powered systems can flag these as anomalies based on frequency, value, or recipient profile, but a human investigator could identify the context and justification for such arrangements. By combining AI-driven analysis with professional judgment, forensic accountants are able to navigate complex data landscapes, ensuring that findings are both accurate and

meaningful. This synergy between technology and expertise enhances the effectiveness of financial investigations, allowing organisations to respond to potential risks faster and more comprehensively.

The "human in the loop": A model for the future

The concept of the "human in the loop" is often framed as a safeguard – a necessary check on technological processes. While this is true, it is equally important to view it as a source of value.

Human expertise enhances technology by refining its inputs, interpreting its outputs, and challenging its assumptions. In practice, this means embedding human judgment at every stage of the investigative lifecycle:

- Designing search parameters and review protocols in e-Discovery.
- Validating and contextualising findings from forensic and OSINT tools.
- Conducting interviews and assessing the credibility of sources.
- Synthesising evidence into coherent, defensible conclusions.

As technology advances, investigative tools are poised to become ever more refined, autonomous, and central to the investigative process. Within the realm of corporate investigations, where facts are often disputed, motives remain unclear, and the stakes are always high, the need for sound judgment, a healthy dose of scepticism, and steadfast ethical values is paramount. It is the human element that ensures investigations are not only thorough, but also fair and principled. In this landscape, the value of the human investigator endures – not despite technological progress, but because of it. As investigative tools grow in sophistication, the expertise required to steer, interpret, and critically evaluate their findings is indispensable. The future of investigative work does not lie in choosing between human judgment and machine efficiency; it is built upon their collaboration. And within that partnership, the human in the loop remains not just relevant, but essential.

07

Fireside chat

Rising regulatory and compliance complexity through the lens of Latin America

In this fireside chat, Richard Fogarty, S-RM's Head of Disputes & Investigations for the Americas, and William Barry, Global Chair of Miller & Chevalier, discuss the challenges facing clients operating in Latin America. Together, they share insights on the evolving risk landscape in the region, providing examples of compliance and regulatory concerns that have far-reaching consequences beyond its borders. They also examine how the US national security strategy measures are adding more complexity for investors and companies operating in the region.

Rich Fogarty: Will, thanks for joining me today. Let's dive straight in. We're here to talk about Latin America but let's start with the US. One could argue that Latin America is playing – not a disproportionate – but a very significant role in the focus of the current administration. There are tariffs and sanctions issues and then FTOs [Foreign Terrorist Organizations] – the designation given by the US to foreign groups engaging in terrorism that threatens national security.

Will Barry: You're right Rich, I certainly agree around the emphasis looking southward from the United States right now, the administration has a clear view that security doesn't just mean who is crossing the border physically, it means economically too – is the US being advantaged or is China or another power infiltrating the markets throughout South America? We of course look at Venezuela and the US action to remove Nicolas Maduro in January 2026, that was an extraordinary example of American power. But for me, what's happening in Mexico right now – whether that's the FTO issue you mentioned or TCO [Transitional Criminal Organizations] issues or tariff evasion – is huge.

> **"If you're going to participate in the US-Mexican marketplace, it's no longer enough to think about whether you might come across a stereotypical bribe of a government official. There are a much broader set of concerns that go beyond the individual transaction all the way up to the C-suite."**

As a result, if you're going to participate in the US-Mexican marketplace, it's no longer enough to think about whether you might come across a stereotypical bribe of a government official. There are a much broader set of concerns that go beyond the individual transaction all the way up to the C-suite. For example, with the FTO initiatives, while you may uncover that somebody paid a bribe at customs – and that's always been a serious issue – you have to look at whether the *New York Times* or the *Wall Street Journal* is going to report tomorrow that your company is supporting terrorism.

Rich Fogarty: Exactly. We're already seeing public examples of companies with concerns around their exposure to FTOs carrying out comprehensive reviews to discover that exposure. And to your point on the broader set of concerns, I feel we're almost looking at something akin to "strict liability". Technically, the threshold is much lower in terms of what material support of a terrorist organisation might look like.

I also want to note here that the US recently stated it was not going to go forward with the USMCA [United States-Mexico-Canada Agreement] review in July unless strong anti-corruption measures were implemented within these agreements, and a warning that there would be investigations and potential

indictments of public officials coming down the road. Indeed, shortly after the comments on USMCA, the DOJ [Department of Justice] announced the indictment of Governor Rocha in Mexico. How does this fit into the context of your clients' concerns? Does it raise connections to the FCPA [Foreign Corrupt Practices Act] or is it still very much focused on state players and politics?

> **"The FCPA has become a component of national security – that is, it is layered into other criminal activity."**

Will Barry: I'd say client concerns are consistent with what is messaged by the US administration. For example, when it announced the pause on the FCPA in February 2025, clients continued to look at FCPA but potentially weren't going to be as interested in the more de minimis, perhaps technical violations, as opposed to what we historically called 'grand corruption'. And you can combine that with the way the FCPA has become a component of national security – that is, it is layered into other criminal activity. For example, years ago you would say 'here is an FCPA case', but today there's an FCPA case that's part of a wire fraud that is part of a money laundering case, or a sanctions or trade fraud issue.

Rich Fogarty: Another country in the news at the moment is of course Brazil and the Banco Master issue. This is a groundbreaking scandal in the country potentially reminiscent of Operation Lava Jato. Banco Master [a mid-sized lender], and its CEO, Daniel Vorcaro, are embroiled in a huge bank fraud that really, we're in the nascent stages of at the moment. But my sense is that the ripple effects of this scandal will reach far and wide. And there are other issues coming out of Brazil, tied to US pressure again, right?

Will Barry: Yes, this resonates with me. If I take the latter point first, the US administration has made it quite clear that it has a list of countries that are friends and Brazil is not on that list. As a result, there is increased exposure to companies that are operating out of or in Brazil. When we look at the Banco Master case and the allegations being levelled – inflated assets, misleading descriptions of financial products, corruption etc. – you end up with significant issues being raised regarding the banking system itself. And much like Lava Jato, corruption allegations get tied to the political establishment. On top of all that you have the interconnectedness of the global banking system. Suffice to say, it's a massive development!

> **"You need the right partners to guide you, whether you are an investor, private equity, hedge fund, family office – really any entity exposed to Latin America operations."**

Rich Fogarty: When we think about this complexity, the risks that clients face operating in the countries we've spoken about here – and in the region more generally – look, there's opportunity alongside the risk right? But you need the right partners to guide you, whether you are an investor, private equity, hedge fund, family office – really any entity exposed to Latin America operations. Having local knowledge and networks, fluency in the languages, etc, enables clients' teams to interpret nuanced issues and navigate local contexts effectively, which is particularly

important in sensitive legal and compliance matters.

Will Barry: Absolutely, and I will say first, the strength of Miller & Chevalier's Latin America facing practices was one of the main drivers for me joining the firm 10 years ago. I've been practicing in and around Latin America for a couple of decades and the fact that I can go into a room in Brazil or in Mexico, in Colombia, in Argentina, and have native or fluent lawyers from Miller & Chevalier in the room with me who have lived in country, who have spent years working there is a massive value add.

And secondly, when it comes to partners, local experience is key: for example if it is evidence collecting in the region then you need to be conscious of the requirements under multiple regulatory regimes, and that the evidence might end up in a courtroom in New York City as opposed to a conference room in Buenos Aires. You need trusted partners such as S-RM that have the combined understanding of the legal underpinnings of the request and the receipt, collection and analysis of the evidence – the whole process – and are linguistically accurate.

Rich Fogarty: Thanks Will, and another example on this theme, if you're in Mexico with a large customer base you may think you know who the beneficial owners of those clients are – but actually there's a good chance in certain circumstances that the true owners are not going to appear in the public record and they may be problematic. In that case you need human intelligence on the ground to help.

Will Barry: Exactly! Or we can flip that, conscious of the focus on cartels and FTOs, there are times you do know who the beneficial owner is. You just might not understand the importance of it until it's too late!

Rich Fogarty: Very true. Thank you Will, I know you and the team at Miller & Chevalier are ready to support companies meeting these challenges, as are S-RM.

William P Barry, Member, Firm Chair
William Barry is the Chair of Miller & Chevalier. He is a trusted advisor to multinational companies, boards of directors, foreign trustees, hedge funds, private equity funds, universities, and senior officers and executives. For 30 years he has solved complex problems involving multi-jurisdictional investigations and litigation, as well as enforcement, compliance, and transactional issues. He helps his clients emerge from crises and resume focus on their business.

Miller & Chevalier
Founded in 1920, Miller & Chevalier is a Washington, DC law firm with a global perspective and leading practices in Tax, International Law, Litigation, ERISA, White Collar Defense and Internal Investigations, Government Contracts, and Government Affairs.

Acknowledgments

Edited by

Marcus Fishburn
Global Head of Disputes & Investigations
m.fishburn@s-rminform.com

Contributors

Amalia Coyle
Associate, Corporate Intelligence
a.coyle@s-rminform.com

Amy Francis
Head of Digital Forensics
a.francis@s-rminform.com

Richard Fogarty
Head of Disputes & Investigations, Americas
r.fogarty@s-rminform.com

Yannine Pasula
Director, Corporate Intelligence
y.pasula@s-rminform.com

Ana Pereu
Associate Director, Disputes & Investigations
a.pereu@s-rminform.com

Ryan Shields
Associate Director, Digital Forensics
r.shields@s-rminform.com

Philippa Wilkinson
Associate Director, Disputes & Investigations
p.wilkinson@s-rminform.com

S-RM is a corporate intelligence and cyber security consultancy. We provide intelligence, resilience and response solutions to organisations worldwide.

Founded in 2005, we have 400+ experts across nine international offices, serving clients across all regions and major sectors.

Find out more at www.s-rminform.com

S-RM