This article first appeared in the February 2026 issue of Financier Worldwide magazine.

Permission to use this reprint has been granted by the publisher.

FINANCIER WORLDWIDE corporatefinanceintelligence

SPECIAL REPORT Q&A **REPRINT** February 2026

New FCPA landscape: implications of the DOJ's enforcement reset

FW discusses the implications of the DOJ's enforcement reset on the FCPA landscape with Didier Lavion and Jonathan T. Marks at BDO.

Q&A: New FCPA landscape: implications of the DOJ's enforcement reset

FW discusses the implications of the DOJ's enforcement reset on the FCPA landscape with Didier Lavion and Jonathan T. Marks at BDO.

THE PANELLISTS

DIDIER LAVION
Principal
BDO
T: +1 (917) 770 2196
E: dlavion@bdo.com

Didier Lavion is BDO's anti-corruption & anti-bribery leader and has been in the forensic advisory business for over 32 years. He has assisted large multinational clients in navigating complex regulatory circumstances and guiding them through multijurisdictional internal investigations. His experiences include, FCPA, fraud and financial crimes investigations, AML compliance and lookbacks, and international arbitration, leveraging data analytics and the use of predictive modelling on client projects. He has extensive experience in presenting and reporting to regulator and enforcement agencies.

JONATHAN T. MARKS
Principal
BDO
T: +1 (267) 261 4947
E: jtmarks@bdo.com

Jonathan T. Marks is a principal and a leader in the forensic services practice. He is a globally recognised specialist in forensic accounting, fraud risk, compliance and corporate governance. He advises boards, audit committees and senior executives on complex investigations, financial misconduct and governance failures. With nearly four decades of experience, he leads matters involving white-collar crime, internal controls and regulatory enforcement. He is the creator of the 'fraud pentagon' and a frequent author and speaker.

FW: What does the US Department of Justice's (DOJ's) 'enforcement reset' mean for global compliance programmes?

Lavion: When Todd Blanche, US deputy attorney general, described an enforcement reset, practitioners heard a familiar message. The Department of Justice (DOJ) wants stronger cases supported by stronger evidence. It is not looking to reduce enforcement – it is looking to reprioritise enforcement to better align with cases that affect US interests. Mr Blanche focused on individual accountability, admissible evidence, measurable harm and disciplined case selection. He emphasised the need for corporate cooperation, providing credit when it is provided and pursuing those that decide not to. These themes signal a move toward quality of cases over volume. The DOJ has emphasised that it will be taking cases to trial where it can win and hold responsible individuals accountable. The reset challenges companies to examine whether their programmes genuinely live within the business and address both past and current enforcement priorities. The DOJ intends to pursue actions related to the intersection between companies and transnational criminal organisations (TCO) and cartels. In addition, the DOJ will be applying the full capabilities of the newly formed cross-agency Trade Fraud Task Force. Its principal focus will be to identify tariff evasion, trade and customs fraud, and it has indicated it will proactively monitor data aggregated from Customs and Border Patrol to identify global tariff compliance anomalies and red flags developed from monitoring shipments across the world and into the US.

FW: How should multinational companies recalibrate their risk assessments and internal controls to align with the DOJ's new focus on cases that harm US economic or national security interests?

Marks: Mr Blanche's remarks should prompt companies to rethink how they approach risk assessments. Many organisations still treat it as a 'set it and forget it' or periodic exercise, rather than an ongoing diagnostic tool. Risk scoring may appear elegant, but neat frameworks often mask real vulnerabilities. True risk does not organise itself into convenient categories – it emerges in operations, behaviours, incentives and culture. Recalibration must therefore begin with understanding where the organisation meaningfully touches US markets, regulators and interests. This means mapping where goods are moving, where duties apply, where sensitive technology is shipped and where high-risk intermediaries sit. Organisations must look closely at supply chains, distribution channels, payment flows and government touchpoints, and now even more so, third parties in high-risk cartel environments that might require enhanced due diligence. These areas frame the DOJ's enforcement view and should inform a company's assessment work.

FW: What new risk indicators should compliance teams watch for? How can multinationals strengthen detection and monitoring for high-risk patterns that may suggest links to cartels, transnational criminal organisations, shell companies and money laundering, for example?

Lavion: Risk indicators are evolving rapidly. Mr Blanche's focus on trade fraud, supply chain vulnerabilities and connections to TCOs underscores that traditional red flags are no longer enough. Companies must train themselves to see the signals that appear early in the lifecycle of misconduct. Companies need to include geographic risks of interactions with cartels or TCOs in their risk assessment. These criminal organisations can be integrated into the supply chain, unbeknown to the corporations, and threaten violence, putting employees or assets at risk unless paid not to. Money

service businesses and financial institutions operating in high-risk countries are now expected to enhance their know your customer and transaction alerting processes to better capture potential interactions with criminal entities. Having knowledge of a company's supply chain is heavily dependent on accurate and honest disclosure of a product's origin, pricing, customs declarations and relevant third parties. Evaluating customs and logistics provider contracts and auditing documentation is an added measure needed to ensure compliance.

FW: What practical changes should compliance officers anticipate in terms of timing, engagement and expectations when interacting with enforcement authorities?

Marks: Mr Blanche addressed a point that every practitioner eventually learns: the DOJ values timeliness. Companies often underestimate how closely prosecutors observe the speed and seriousness of a company's response. When Mr Blanche said the DOJ will not allow matters to drift, he was communicating a fundamental principle. Delay is interpreted as avoidance. It never helps the organisation. Compliance officers need to be prepared for rapid mobilisation. Evidence preservation must happen immediately. Custodial mapping must be clear. Document collection requires discipline. Interviews need structure, not improvisation. Leadership must be briefed with the information available at the time. Waiting for the perfect narrative is counterproductive. In practice, companies should expect to walk through their investigative timeline, methodology, custodial decisions, and remediation steps in a clear and defensible manner. The DOJ does not reward performance or optics. It rewards clarity, honesty, readiness and discipline. The companies that understand this tend to navigate enforcement far more effectively than those that treat the process as a communications exercise.

FW: How should companies prepare for the surge in whistleblower activity? With the DOJ reporting record tip volumes, what best practices can multinationals adopt to manage internal reporting channels and respond effectively before regulators intervene?

Lavion: Whistleblower activity is increasing globally, and Mr Blanche's emphasis on admissible evidence strengthens the role of internal reporting. Companies often find themselves in difficult positions not because misconduct occurred but because they did not detect it internally and respond in time. In addition, the newly created Corporate Whistleblower Awards Pilot Program and myriad pre-existing programmes will further incentivise whistleblowers to disclose outside of companies' internal mechanisms. Organisations must ensure their reporting systems are accessible, trusted and responsive. Companies need to design reporting from the point of view of the whistleblower. Channels

Companies should expect to walk through their investigative timeline, methodology, custodial decisions, and remediation steps in a clear and defensible manner. The DOJ does not reward performance or optics.

JONATHAN T. MARKS
BDO

must function across languages and jurisdictions. Non-retaliation must be enforced consistently. Intake must be disciplined. High-risk allegations must reach qualified investigators quickly. A strong whistleblower programme requires surgical triage and escalation, transparency with reporters, appropriate updates, meaningful disciplinary action for retaliation, and integration with other data sources. Hotline trends, audit observations, cultural insights and anonymous tips should inform each other rather than sit in isolation.

A strong whistleblower programme requires surgical triage and escalation, transparency with reporters, appropriate updates, meaningful disciplinary action for retaliation, and integration with other data sources.

DIDIER LAVION
BDO

FW: What does the DOJ's emphasis on individual accountability mean for compliance programmes? How can companies ensure their investigations and documentation support clear identification of individual misconduct early in the process?

Marks: Mr Blanche's comments on individual accountability remain aligned with the Yates and Monaco frameworks from prior administrations. His reminder that individuals go to jail, not companies, should shape both the design of compliance programmes and the conduct of investigations. The DOJ's position of corporate versus individual accountability has been made clear by this year's closure with no-action of several active cases against corporations and decisions to continue prosecution against individuals by going to trial. Individuals have a lot more to lose if implicated in bribery or money laundering allegations. Programmes must be built to identify decision points and the individuals responsible for them. Investigations must track who knew what, when and under what circumstances. This requires inquiries that explore context and documentation that captures approvals, ignored warnings and behavioural indicators. The 'fraud pentagon' is particularly helpful here because it explains the behaviours that support control override and rationalisation. Boards should expect reporting that names individuals clearly and articulates the basis for accountability. If a company cannot identify the actors responsible, the DOJ will view the programme as inadequate and adjust its resolution of a case accordingly.

FW: How critical is voluntary self-disclosure under the new landscape? What steps should compliance officers take to ensure disclosures meet the DOJ's standards for cooperation and remediation – and what benefits can they realistically expect?

Lavion: Voluntary self-disclosure (VSD) remains a major driver of prosecutorial decision making as well as helping develop a pipeline for future investigations by the DOJ. Mr Blanche reaffirmed that the timing and substance of disclosure matter greatly. It cannot be planned after the facts have become obvious. It must be early, candid and

supported by rapid investigation. Compliance officers must ensure that escalation pathways route credible concerns directly to decision makers. Siloed designation of escalation and whistleblower complaints could lead to stalled or unaddressed instances of non-compliance or fraud. Investigative readiness must be built into the programme. Companies should be able to describe exactly when they learned of an issue, how it was escalated, what the response was, how they preserved evidence, and their response to the need for independent evaluation of the facts and circumstances of an issue. The mix of stakeholders will have varied expectations as to how a company responds to potential illegal acts. Management, the board, audit committee, investors and company auditors will each have an expectation of how remediation plans were arrived at and any VSD decisions.

FW: What does the DOJ's shift away from expansive monitorships mean for remediation strategies? How can companies demonstrate credible self-governance and remediation to satisfy DOJ expectations without relying on external monitors?

Marks: Mr Blanche's remarks on monitorships acknowledged a growing view in the practitioner community – some monitorships have become too broad and too costly, with limited control, and they have not always addressed the specific root causes of misconduct. Mr Blanche's shift toward narrower oversight places responsibility for remediation back with the company, imposing outside monitorship only when the benefits of doing so outweigh the costs, and mandating budgets with fee caps that cannot be exceeded unless prior approval is granted. Organisations must design remediations that address why controls failed. This requires a properly executed root-cause analysis that identifies both structural weaknesses and behavioural contributors such as pressure, rationalisation, competence and arrogance. Controls must be tested to ensure they function as intended. Culture must be addressed through tone, incentives, discipline and transparency. Continuous monitoring plays a role here as well. It helps organisations demonstrate ongoing effectiveness rather than one-off improvements. Companies that remediate early and substantively often avoid monitorships entirely. Mr Blanche's remarks reinforce that monitorships appear when the DOJ lacks confidence in a company's ability to govern itself. ■