CMS Francis Lefebvre

Corporate Crime Investigations

H1 2026 Report
From Hotline Report to Prosecutor-Ready File



October 2026

The first half (H1) of 2026 confirmed a structural shift in corporate crime enforcement: internal investigations are no longer assessed only by whether they reach the right legal conclusion. They are assessed by whether the company can preserve evidence quickly, reconstruct the misconduct credibly, identify individual responsibility, quantify benefit or harm, and decide whether to self-report before a whistleblower, counterparty, regulator or prosecutor moves first.

The practical question for corporate legal and compliance teams is therefore changing. It is no longer simply **"What happened?"** it is also:

> **"Can we turn this allegation into a reliable, source-attributed, prosecutor-ready factual record fast enough?"**



Nicolas Tollet
Partner

Table of Content

1. United States disclosure timing became part of the investigation design 4

2. France PNF risk, CJIP readiness and criminal evidence architecture 8

3. European Union anti-corruption harmonization, GDPR constraints and sanctions evidence 11

4. Selected global signals UK, Australia and Canada 13

5. The quieter revolution AI and the new discipline of document review 14

6. What investigation teams should change for H2 2026 16

Investigations & Compliance 360°, discover our offer 17

Contacts 18

1 | United States disclosure timing became part of the investigation design

The U.S. Department of Justice (DOJ)

The U.S. Department of Justice's Corporate Enforcement and Voluntary Self-Disclosure Policy (CEP), issued on 10 March 2026, was one of the defining corporate crime developments of H1 2026. It is DOJ's first Department-wide framework in this area: it applies across DOJ corporate criminal matters, except antitrust, replaces the guidance DOJ issued in May 2025, expressly supersedes the pre-existing corporate enforcement policies of individual DOJ components and U.S. Attorney's Offices, and is designed to encourage early voluntary self-disclosure, cooperation, remediation and individual accountability. Most importantly for investigation teams, DOJ expressly encourages companies to disclose at the earliest possible time, even before completing an internal investigation. The policy retains the Corporate Whistleblower Awards Pilot Program exception: where a whistleblower reports both internally and to DOJ, the company may still qualify for a declination even if the whistleblower reports to DOJ first, provided that the company self-reports as soon as reasonably practicable and no later than 120 days after receiving the internal report, and meets the policy's other requirements for voluntary self-disclosure and a declination. That 120-day period is an outer limit, not a grace period.[1]

This changes the investigation calendar. In U.S.-facing matters, voluntary disclosure can no longer be treated as a decision made only after the fact-finding is complete. It should be a parallel workstream from the first days of the investigation. Counsel and forensic teams need an early view of the suspected offence, the individuals potentially involved, the documents preserved, the systems affected, the likely benefit or harm, the existence of aggravating factors, and whether a whistleblower, auditor, customer or regulator may already have reported the matter.

The DOJ policy also makes clear what "cooperation" means in practice. Companies are expected to provide timely, truthful and non-privileged facts and evidence, including facts gathered during the internal investigation, attribution of facts to specific sources, rolling updates, relevant overseas documents where legally possible, information about individuals involved in the misconduct, and preservation, collection and production of documents with provenance information. Where foreign privacy or blocking statutes are invoked, the company bears the burden of establishing the restriction and of identifying reasonable lawful alternatives, and cooperation may include narrowly tailored, time-limited deconfliction, although DOJ states that it will not direct the internal investigation. DOJ states that privilege waiver is not required, but the factual record must be usable.
Several calibration changes matter when weighing a disclosure:

[1] DOJ Corporate Enforcement and Voluntary Self-Disclosure Policy, available here.

[2] DOJ press release, available here.

[3] Bosch executed declination, available here.



First, the definition of aggravating circumstances now reaches recidivism beyond the traditional five-year look-back: prosecutors must consider whether the company has been subject to a criminal resolution in the previous five years or otherwise based on misconduct similar to that under investigation.



Second, the guaranteed 75% reduction from the low end of the U.S. Sentencing Guidelines range for "near miss" disclosures has become a discretionary range of 50% to 75%.



Third, the policy encourages prosecutors, where appropriate, to inform a company as soon as practicable whether it is eligible for a declination under Part I or "near miss" treatment under Part II. It sets no deadline for that feedback.



Fourth, DOJ takes account of a company's size, sophistication and financial condition when assessing cooperation, while ability to pay remains relevant to monetary penalties. Prosecutors should also explain in corporate resolution agreements why a particular amount of cooperation credit was awarded..



Fifth, the destination of a disclosure is treated more flexibly: a good-faith disclosure to a DOJ component that later refers the matter to another appropriate component will qualify, and disclosures made only to federal regulators or to state or local authorities, while not ordinarily sufficient, may still qualify in appropriate circumstances. Uniformity should reduce the incentive to race to a particular component, but component-level practice may still shape how prosecutors exercise the discretion the policy leaves them.

Two H1 declinations show how internal investigations can become the basis for enforcement outcomes.

1. In March, DOJ issued the first declination under the new policy to Balt SAS in a foreign bribery matter coordinated with the French PNF, requiring approximately US$1.2 million in disgorgement. DOJ's declination emphasized that the company identified the misconduct during an internal investigation, voluntarily self-disclosed while the investigation was ongoing, cooperated, provided information about individuals and remediated. Though under the new policy, this case is line with past DOJ practices, and it demonstrates the continued willingness of the department to go after individuals. A separate indictment alleged that a former U.S.-subsidiary executive and a consultant used sham consulting agreements, false invoices and personal email accounts to conceal payments described as consulting fees and bonuses.[2]

2. In June, DOJ's National Security Division issued its first declination under the new policy, to Robert Bosch GmbH, in an export-control matter involving more than US$70 million in reexports by two non-U.S. subsidiaries to Huawei and Entity-Listed affiliates. DOJ cited Bosch's internal investigation, voluntary self-disclosure to DOJ and BIS while the investigation was ongoing, preservation and production of documents, remediation and expansion of trade-compliance resources. DOJ set disgorgement at US$11,430,098 but credited US$7,829,069 paid in the parallel BIS resolution, leaving an incremental DOJ payment of approximately US$3.6 million; BIS separately imposed a civil penalty of US$36,184,680.[3]

A strong internal investigation is not simply a defensive exercise: it can be the factual platform for a declination, coordinated resolution or settlement. That requires early preservation, defensible scoping, source attribution, individual accountability analysis, remediation evidence and privilege discipline.

On the antitrust side, H1 also showed that DOJ and the SEC are expecting more technical forensic work. In remarks prepared for delivery on 14 May, Acting Deputy Assistant Attorney General Daniel Glad of DOJ's Antitrust Division warned that "old crime" can be committed through "new code," focusing on algorithmic pricing, procurement platforms, large language models and digital evidence. DOJ emphasized that automated bid records, pricing-tool inputs, prompts, logs, parameter changes and timestamps may all become relevant evidence. It also highlighted a whistleblower "race," noting that engineers, data scientists, product managers, account managers and compliance professionals may be positioned to identify algorithmic collusion. The remarks were an enforcement signal rather than a new legal standard: Section 1 still requires proof of an agreement.[4]

That is a major scoping point. A cartel, bid-rigging or pricing investigation can no longer stop at emails, meeting notes and sales files. The relevant evidence may sit in pricing engines, procurement platforms, code repositories, model prompts, SaaS vendor communications, algorithmic parameters, user-access logs and change-management records.

The whistleblower "race" is now backed by money. On 29 January, the Antitrust Division announced its first whistleblower reward (US$1 million) for information that led to charges and a deferred prosecution agreement with EBLOCK Corporation, including a US$3.28 million criminal fine. A company may therefore be racing not only another leniency applicant, but insiders with a direct financial incentive to report.[5]

The U.S. Securities and Exchange Commission (SEC)

The SEC's H1 enforcement activity pointed in the same direction. On 27 January, the SEC filed settled charges against ADM and two former executives, and a litigated action against a third former executive, in an accounting and disclosure matter involving intersegment adjustments that improperly shifted operating profit to the Nutrition segment. ADM, without admitting or denying the findings, agreed to a US$40 million civil penalty. The SEC stated that it considered ADM's cooperation and remediation, including an internal investigation, voluntary reporting of findings, outside accounting expert analyses and new controls around intersegment transactions.[6]

On 6 May, the SEC charged 21 individuals in an alleged decade-long insider-trading scheme involving information misappropriated from multiple global law firms, with assistance from authorities including FINRA, the UK FCA, Swiss FINMA and other foreign regulators. DOJ's parallel criminal action was broader, charging 30 defendants in a scheme said to involve nearly 30 M&A transactions and tens of millions of dollars in illicit profits, and describing document-management access, burner phones and encrypted applications, coded communications, shell-company, third-party and foreign brokerage accounts, cash and disguised kickbacks, and alleged obstruction.[7] That case echoes last year's call jointly made by the French Anticorruption Agency (AFA) and the French SEC (AMF) regarding increased risk linking corruption and insider's trading.[8]

[4] DOJ Antitrust Division remarks, available here.

[5] DOJ press release, available here.

[6] SEC press release, available here.

[7] SEC press release, available here.

[8] AFA and AMF Joint Call, available here. See also, Corruption privée et réseaux d'initiés : le nouveau front de la compliance financière, Option Finance, Nicolas Tollet, Olivier Khun and Sara Garbi, September



2 | France PNF risk, CJIP readiness and criminal evidence architecture

France's H1 2026 developments are particularly important for companies exposed to corruption, tax fraud, public procurement offences, market abuse, money laundering, terrorist financing, sanctions or environmental criminal enforcement.

The National Prosecutor's Office (PNF)

The most important French H1 settlement trend was the continued use of the convention judiciaire d'intérêt public (CJIP). Four CJIPs were validated in H1 2026: Bank H. on 8 January, (PMC) on 18 February, and C. Rail Asia and BALT USA LLC on 19 March.[9]



The Bank H.CJIP, signed on 6 January and validated on 8 January, concerned a preliminary investigation into dividend-arbitrage trading through intra-group transactions via the Paris branch between 2014 and 2019, susceptible to characterization as aggravated tax fraud. The public-interest fine was €267,531,000, in addition to €34,464,424 of tax, interest and penalties already paid.[10]



The PMC CJIP, signed on 10 February and validated on 18 February, concerned foreign public-official corruption and laundering, with a €499,150 public-interest fine including €335,000 previously seized, and a three-year AFA-monitored compliance programme within the Carrus group.[11]



The BALT USA CJIP is especially relevant to internal investigations because it followed Balt SAS's disclosure, on 22 May 2023, of facts discovered during an internal investigation concerning a former executive of Blockade Medical, acquired in 2016 and later renamed BALT USA. The CJIP imposed a €1,765,493 public-interest fine, after a €1,168,861 deduction for disgorgement in the parallel DOJ declination, and a three-year AFA-monitored compliance programme within the BALT group.[12]



The C. Rail Asia CJIP is equally important. The matter followed a complaint lodged by C. Rail on 31 May 2017 transmitting an internal investigation report that revealed possible bribery of a foreign public official. The CJIP imposed a €29,745,974 public-interest fine and a three-year AFA-monitored compliance programme for the C. group.[13]

These CJIPs are not just settlement outcomes. They are investigation lessons. In France-facing corporate crime matters, the internal investigation file may become the starting point for a PNF dialogue. It must therefore be capable of supporting a coherent factual chronology, identifying individual conduct, quantifying benefit or harm, explaining controls failures, evidencing remediation and separating legal analysis from non-privileged facts.

The Paris Criminal Court

The Paris Criminal Court's H1 judgments also provide useful forensic roadmaps. Unless otherwise noted, these are first-instance judgments open to appeal, and the lessons below concern the evidentiary features reported in the court's official releases rather than final determinations of liability.

- On 13 April 2026, the court issued judgment in the insider-dealing matter, convicting three individuals, two for unlawful use of inside information and one for complicity, in connection with privileged information about Company A1's planned acquisition of Company A2. According to the court's press release, a bank employee obtained privileged information and transmitted it through a chain to traders, who acquired contracts for difference before the public announcement. The investigation combined AMF analysis with judicial interception of prepaid telephones, and the court relied on the chronology of investments, order modalities, trading volumes and explanations given by the defendants; sentences included up to three years' imprisonment and fines reaching €30 million. Other participants in the information chain had previously been dealt with through CRPC proceedings.[14]
  For internal investigations, the case reinforces the need to reconstruct the entire information chain in suspected deal leaks. Investigators should examine insider lists, deal-room access, bank and law-firm teams, wealth managers, brokers, relatives, derivatives exposure, phone records, messaging data, file downloads, print records and unusual trading by connected persons.

- On 16 April 2026, the court issued judgment in the SIEAM case, concerning public procurement in Mayotte's water and sanitation authority, convicting 11 individuals and six companies. The PNF investigation, opened after reports from the Regional Audit Chamber of Réunion and Mayotte, had concerned 17 individuals and 14 legal persons, some of whom had already been dealt with through CRPC proceedings. The court found that a system of favoritism had been organized and perpetuated, made possible by concentration of powers, defective procurement organization and persistent systemic failures in management and internal control. It also referred to contract-splitting practices designed to defeat competition and favor selected companies; penalties reached four years' imprisonment and fines of €100,000.[15]
  For procurement investigations, SIEAM shows that the evidentiary narrative may be structural, not just transactional. Investigators should reconstruct tender specifications, scoring, amendments, emergency justifications, contract splitting, bid committee composition, conflicts of interest, supplier rotation, subcontracting, payment approvals and relationships between public officials, consultants and bidders.

- The Company L. judgment of 13 April 2026 is a major French corporate-crime development for companies operating in conflict zones or sanctions-sensitive environments. The Paris Criminal Court convicted Company L. and eight individuals at first instance, finding that €5,593,897 had been paid by Company L. Syria to terrorist entities through "security" payments, intermediaries, passage fees and suppliers controlled by those entities. It imposed a €1.125 million fine on Company L. for terrorist financing and a separate €4.57 million customs fine for sanctions violations, payable jointly by the company and certain executives. The court also held that adherence to terrorist ideology was not required where the defendants knew the destination of the funds. Appeals were filed, and the separate judicial investigation into alleged complicity in crimes against humanity remains distinct.[16]
  Beyond the exceptional criminal law considerations of this case, with respect to investigations, it is a reminder to follow the money beyond accounting labels. Payments described as security, access, local tax, facilitation, logistics, customs, consulting or emergency operating costs may require review against terrorist-financing, sanctions and money-laundering risks. The investigation should map intermediaries, local partners, suppliers, cash movements, bank transfers, approvals, accounting entries, chain-of-command knowledge and contemporaneous risk assessments.

[9] PNF CJIP page, available here.
[10] PNF Press release, available here.
[11] PNF Press release, available here.
[12] PNF Press release, available here.
[13] PNF Press release, available here.
[14] Tribunal de Paris Press release, available here.
[15] Tribunal de Paris Press release, available here.
[16] Tribunal de Paris Press release, available here.



The legislative changes

The most investigation-specific French legislative development of H1 was Law No. 2026-534 of 25 June 2026, which materially increased evidence mobility. Specially authorised AMF investigators may now investigate criminal market abuse and connected offences throughout France, gather evidence, identify perpetrators and assist judicial police under letters rogatory. Any public prosecutor, and not only the PNF, may transmit relevant criminal-case materials to the AMF, subject to an investigating judge's favourable opinion where a judicial investigation is under way, and tax and customs officers conducting criminal investigations may, with judicial authorisation, transmit useful material to their administrative-control counterparts. Companies should assume that documents, interview records and transaction data gathered in one channel may migrate rapidly into parallel proceedings.[17]

France also adopted a legislative change that affects whistleblower triage. Decree No. 2026-311 of 24 April 2026 adds Tracfin to the list of external authorities competent to receive whistleblower reports for AML/CFT matters and expands the external-reporting fields of the AMF and ACPR by removing sector-specific qualifiers. The decree enters into force on 1 July 2026.[18] The practical consequence is that French whistleblower reports involving suspicious payments, unexplained intermediaries, sanctions indicators, terrorist-financing risks, market abuse, prudential concerns or complex beneficial ownership should not be treated as generic ethics alerts. The first triage should identify the potentially competent authority (Tracfin, AMF, ACPR, PNF, PNAT or another prosecutor) and trigger evidence preservation accordingly, and whistleblowing notices and routing matrices should be updated. The decree does not, however, create any obligation to transmit internal alerts to Tracfin or prosecutors: protected external whistleblowing, suspicious-transaction reporting, regulatory notification and voluntary disclosure to prosecutors remain distinct channels.

[17] Law n°2026-534 of 25 June 2026, available here.
[18] Décret n° 2026-311 of 24 April 2026, available here.

3 I European Union anti-corruption harmonization, GDPR constraints and sanctions evidence

At EU level, the most significant H1 development was Directive (EU) 2026/1021 on combating corruption, published on 11 May and in force on 31 May 2026. The Directive sets minimum EU-wide standards for anti-corruption enforcement and strengthens the criminal-law framework across Member States, which must largely transpose it by 1 June 2028, with certain preventive obligations due in 2029; it did not itself replace national corporate-crime rules on entry into force.[19]

The Directive matters for internal investigations because it broadens the taxonomy beyond classic bribery. It addresses public- and private-sector bribery, misappropriation, which Member States may but need not extend to the private sector, trading in influence, unlawful exercise of public functions, obstruction of justice, enrichment from corruption, and concealment and laundering of corruption-related offences. It also requires Member States to provide for liability of legal persons for offences under Articles 3–6 and 8–11 where committed for their benefit by leading persons, or where a lack of supervision or control by a leading person enabled an offence by a person under their authority. Fines are mandatory. For specified offences, and at least for liability under Article 13(1), national law must provide for maximum fines of at least 3% or 5% of total worldwide turnover, depending on the offence, or alternatively at least €24 million or €40 million, respectively; possible additional measures include exclusion from public benefits or procurement, disqualification, permit withdrawal, contract rescission, judicial supervision, winding-up, closure of establishments and publication of the decision.
The Directive also requires Member States to ensure that one or more of the circumstances listed in Article 16 can, in accordance with national law, be treated as mitigating. These include assistance to the authorities, effective internal controls and compliance programmes, and rapid voluntary disclosure combined with remedial action. The Directive does not itself create an automatic entitlement to mitigation.

For companies, the investigation taxonomy should therefore evolve. A cross-border corruption investigation should not be framed only as "bribery or no bribery." It should also test influence trading, misuse of entrusted property, procurement manipulation, concealment, obstruction, laundering, conflicts of interest, public-function misuse and third-party facilitation. The likely effect, once the Directive is transposed, is more consistent criminal-law expectations across the EU and stronger cooperation among national authorities.

H1 2026 also produced important CJEU decisions for forensic investigations and investigation-data governance:

- In Darashev (C-312/24), the Court held that data collected by a competent authority for a criminal investigation fall within the GDPR when they are subsequently stored in an employee's personnel file for HR purposes, even within the same public authority. Such storage is lawful only where the national legal basis is clear, precise and foreseeable, pursues a public-interest objective and is proportionate, and retention beyond what is necessary may engage the right to erasure. By analogy, corporate reuse of investigation material for employment, disciplinary or other secondary purposes requires its own purpose, legal-basis, necessity and retention analysis.[20]

[19] Directive (EU) 2026/1021 on combating corruption, available here.
[20] CJEU judgment C-312/24, available here.



- In NTH Haustechnik (C-484/24), the CJEU held that the GDPR does not create a general and absolute prohibition preventing a national court from taking into account evidence containing personal data that may previously have been unlawfully processed by the party submitting it. However, the Court also emphasized that the court's own processing remains subject to GDPR principles, including legal basis, data minimization and protective measures before disclosure. The judgment neither retrospectively legalises the party's collection nor creates an EU admissibility rule independent of national procedure.[21]

The practical point is nuanced but important. A court may later admit evidence, but that does not make the company's collection lawful. Internal and forensic investigations must still document the legal basis for collection, minimize irrelevant personal data, restrict access, maintain retention rules and avoid overbroad searches of private or mixed-use accounts and devices. Sanctions-related investigations also became more complex.

In March 2026, the CJEU's EM System decision (C-84/24), concerning the EU's Belarus regime, confirmed that funds and economic resources of a non-listed company may be frozen where they are owned, held or controlled by a listed person. A listed person's 50% shareholding gives rise to a rebuttable presumption that the company's funds are held or controlled by that person. Both the company and the listed person must have an effective opportunity to rebut that presumption. The Court interpreted "held" and "controlled" broadly.[22]

On 21 May, in T Trust (C-483/23) and the joined cases FZ AR and SX (C-428/24 and C-476/24), the Court clarified the application of asset-freezing measures to trust structures. Investigators should preserve trust instruments, letters of wishes, protector and reserved powers, distribution history, trustee communications and evidence of factual influence.

For sanctions and asset-freeze investigations, the lesson is to investigate control, not merely ownership. Forensic work should examine shareholding, voting rights, governance, appointment rights, contractual control, financing, beneficial ownership, trusts and trust powers, distributions, funds, intermediaries and informal influence. The 50% presumption arose under the Belarus regime and should not be applied mechanically across every sanctions programme.

[21] CJEU judgment C-484/24, available here.
[22] CJEU Press release, available here.

4 I Selected global signals UK, Australia and Canada

The United Kingdom remained an important benchmark for corporate crime investigations in H1 2026

On 1 May, the court approved the SFO's deferred prosecution agreement with Ultra Electronics Holdings for failure to prevent bribery in connection with three public-sector contracts pursued through agents in Oman and Algeria. Ultra agreed to a £10,083,150 penalty, £4,804,831.12 in SFO costs and three years of annual reporting on the effectiveness of its anti-bribery and compliance programme. The SFO opened its investigation after Ultra's self-report concerning Algeria, but withdrew from DPA talks following a late Oman disclosure and disagreement over the company's analysis; negotiations resumed only after changes in ownership, structure and leadership and the provision of all relevant information (the investigation was extended to all jurisdictions in which the company operated). Self-reporting alone was therefore not enough: completeness, candour, remediation and sustained cooperation shaped the outcome.[23]

In June, the SFO's Director stated that corporate cooperation is key to resolution and that prompt self-reporting and full cooperation will generally lead to an invitation to DPA negotiations unless exceptional circumstances apply. The SFO's guidance, updated on 13 October 2026, provides for contact within 48 business hours of a self-report, regular updates and a decision whether to open an investigation within six months. It also states that, wherever possible, DPA negotiations should be concluded within six months after an invitation to negotiate is accepted. These are policy commitments rather than statutory deadlines. An invitation is not a guarantee of a DPA or of court approval.[24]

One UK judgment also carries a privilege warning for investigation teams. In Aabar Holdings v Glencore, the High Court held at first instance that legal advice privilege can extend to qualifying intra-client communications and preparatory materials never sent to a lawyer, where their dominant purpose was to obtain legal advice. The decision is fact-sensitive: it confers no blanket privilege over lawyer-led fact gathering, material outside the defined client group, or documents created for mixed commercial, regulatory or public-relations purposes.

For companies, the UK message is aligned with the U.S. and France: internal investigations should be structured with a possible negotiated outcome in mind. The file should show what was discovered, when it was discovered, how the company responded, what was preserved, which individuals were involved, what remediation occurred and whether the company cooperated genuinely.

Australia also deserves attention

On 2 June 2026, Treasury opened a statutory review of Australia's tax and corporate whistleblowing frameworks. The review is examining whether the laws are working as intended, including access to justice and whether the frameworks incentivize whistleblowing and disincentivize misconduct.[25]

For multinationals, the Australian review is another sign that whistleblower intake, confidentiality, anti-retaliation controls, investigation follow-up and documentation of closure decisions remain board-level governance issues.

In Canada, the Supreme Court heard R. v. Arapakota

On 16 April 2026 and reserved judgment. The case concerns Canada's foreign-bribery offence under the Corruption of Foreign Public Officials Act, including allegations relating to benefits provided to a Botswanan official in connection with business-related letters.[26] (Supreme Court of Canada:)

For companies operating internationally, the case is worth monitoring because foreign-bribery investigations often turn on benefits that are not simple cash payments: travel, hospitality, letters of support, introductions, donations, sponsorships, consulting arrangements and relationship-building expenses.

[23] SFO news release, available here.
[24] SFO speech, available here.
[25] Treasury media release, available here.
[26] Supreme Court of Canada, Decision 42061, available here.

5 I The quieter revolution AI and the new discipline of document review

Underlying all of these enforcement developments is a quieter revolution in how investigations are actually conducted. Over the past two decades, the economics and pace of document review have changed beyond recognition: from mid-2000s DOJ/SEC matters, when first-level review meant teams of dozens of lawyers, to the Lava Jato-era Petrobras and Odebrecht investigations, when finding the truth could still mean travelling in person to physical archives. Today, for many matters, first-level review can be executed in a much shorter time with AI-assisted workflows, and significantly cheaper. That is real progress. But it carries a new risk: the illusion that because a review is faster, it is automatically complete, contextual and legally defensible. AI should be an indispensable tool, never a substitute for investigative judgment.

Two AI fallacies recur. The first is that a forensic platform with built-in AI is enough. That AI usually operates in a closed environment, reasoning only over what has been collected and loaded into the review workspace: excellent for triage, clustering, translation, entity extraction, prioritization and timeline-building from internal material. But an internal investigation is rarely solved from the inside alone. The patterns that matter often require public context: who really owns a counterparty, how its directors and shareholders have changed over time, whether historical versions of a website contradict today's narrative, and whether public registries, addresses, phone numbers or "maiden names" connect people in ways no internal email ever states explicitly.

This calls for a second capability (an open-web research tool designed for public, OSINT-style exploration) used under strict segmentation. The safe approach is to firewall two lanes: a confidential lane (the forensic platform and the confidential dataset) and a public lane (open-web research and public sources such as registries, archives, press and social media). Confidential content must never be fed into the public lane (not snippets, not screenshots, not "just a line") because doing so can create confidentiality, privacy, privilege, contractual and regulatory risk. The value comes from crossing the investigator's own thinking between the lanes, never from crossing the data.

The second fallacy is that AI can connect the dots between documents and the real world. Even systems that summarize and extract entities well still struggle with what investigators actually do: linking weak signals across time, sources, identities and context. Investigations turn on what is odd, missing or implausible; and on what suddenly makes sense once the right external thread is pulled. That is why deliberately wandering between the dataset and public sources to sense what is "fishy" remains investigative craft: navigating corporate registries and shareholder databases, comparing information across jurisdictions, checking archived websites, mapping entities over time, and noticing repeated addresses, shared phone numbers, secondary emails, maiden names, transliterations or "random" company names that in fact fit a family or holding pattern. AI can assist, but it does not reliably do this end-to-end dot-connecting, especially when the dots are scattered across external reality and internal evidence; and it is here that experienced investigators judge not only what links, but what is legally relevant, what is inadmissible, and what is high-risk to collect or use.



The practical consequence is a shift in where the risk lives. First-level review has been transformed: faster issue-spotting, faster stabilization of the narrative, faster identification of custodians and quicker scoping decisions, all at lower cost. But speed creates a new responsibility: the ability to defend what was not seen. Second-level review, where legal significance is determined and privilege, confidentiality, exposure and witness strategy are assessed, must remain human-led. It is also where junior investigators are essential; not as human machines running mechanical review, but as trained lawyers who validate AI outputs, challenge hypotheses and escalate anomalies quickly.

Above all, AI has made qualitative review a discipline rather than an afterthought. The old risk was time and cost; the new risk is subtler: a prompt that narrows too far, a model that misses the outlier, clustering that hides the one document that breaks the case, relevance scoring that reinforces existing assumptions, and a team made falsely confident because the output simply looks coherent. Qualitative review is now the foundation of defensibility. The senior investigator must take the time to do what no tool can: navigate the dataset broadly rather than only the top hits, pressure-test both what the AI selected and what it ignored, roam between the platform and public sources, and apply hard-won experience and skepticism. Paradoxically, AI makes qualitative review more important, not less.
The bottom line for teams being built now is that the competitive advantage in 2026 is not having AI, but knowing how to use it without being fooled by it. That means investing less in the fantasy of full automation and more in five things: governance that segregates confidential and public workflows; training that equips junior investigators to validate, challenge and escalate; documented validation and reproducibility of AI-assisted work; quality control that tests completeness, not only relevance; and senior time reserved for the slow thinking that catches what is fishy. Because in an internal investigation, the one document that is missed is often the one that matters.

6 I What investigation teams should change for H2 2026

The H1 2026 developments point to a concrete action plan.

First, **triage by offence, authority and reporting clock**: A single report may implicate bribery, fraud, tax fraud, market abuse, AML/CFT, sanctions, export controls, terrorist financing, procurement offences or environmental criminal liability. The first assessment should identify the likely regulator or prosecutor, and any mandatory or strategic reporting deadline, before evidence is lost or an external report is made.

Second, **preserve forensic evidence before interviewing witnesses:** Preservation should cover email, messaging apps, collaboration tools, mobile devices, ERP data, payment systems, trade-compliance systems, deal rooms, pricing tools, procurement platforms, code repositories, access logs and third-party systems.

Third, **create a source-attributed factual record:** Regulators and prosecutors increasingly expect more than a narrative. They need to know which fact came from which document, witness, system, log, transaction, device or third party.

Fourth, **quantify benefit, harm and exposure early:** DOJ declinations, French CJIPs, SFO DPAs and SEC settlements all require a credible view of financial benefit, victim harm, disgorgement, penalty exposure or remediation cost.

Fifth, **set the privilege architecture at intake and keep legal advice distinct from source evidence**: This is essential for DOJ cooperation, SFO DPA discussions, French CJIP strategy, cross-border sharing and privilege protection. The mandate, reporting line and decision rights should be fixed, and the jurisdiction-specific privilege analysis completed, before the factual record fragments, without assuming that factual work product is necessarily unprivileged.

Sixth, **treat disclosure and settlement strategy as a parallel workstream:** A company may not have the luxury of completing every interview before deciding whether to approach DOJ, PNF, SFO, AMF, ACPR, Tracfin, BIS, the SEC or another authority.

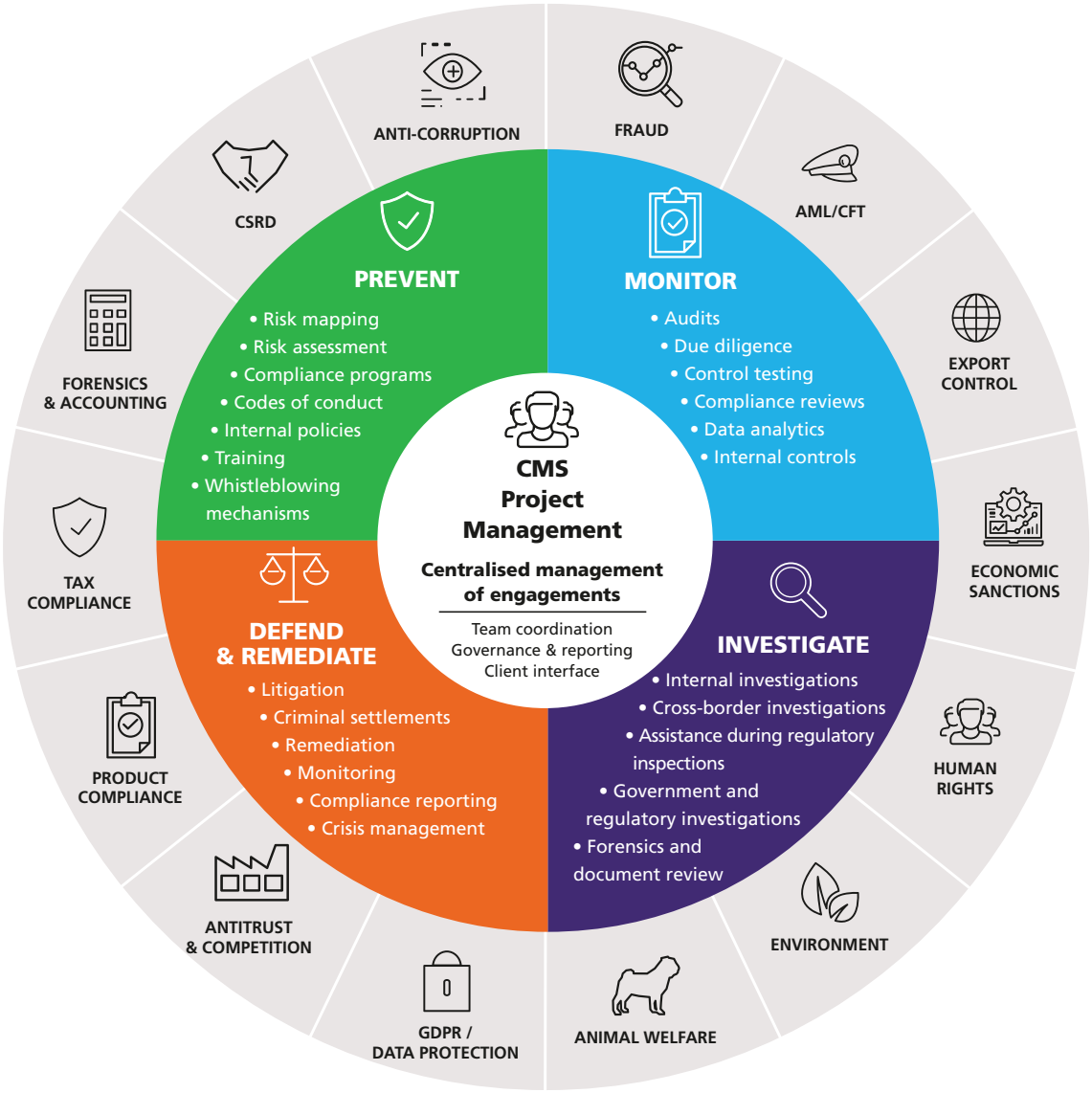
Seventh, **design forensic work for GDPR and local-law defensibility:** Evidence that is technically accessible is not always lawfully collectible or proportionate. Collection protocols, access controls, minimization, retention and deletion should be documented from the start.

Investigations & Compliance 360°, discover our offer

In an increasingly demanding regulatory, litigation and reputational environment, compliance and internal investigations can no longer be addressed in silos. They must be designed as a comprehensive framework, integrating prevention, detection, investigation, remediation, defence and the enhancement of compliance programmes.

CMS Francis Lefebvre supports French and international companies with an integrated "Comprehensive investigations et compliance" offering, providing coverage of the full compliance risk lifecycle, both in France and abroad.

Our aim is simple: to offer our clients a one-stop shop capable of designing, implementing, testing, defending and, if necessary, transforming their compliance and crisis management frameworks, across all relevant areas and in all jurisdictions where they operate.



Contacts

Corporate Crime, Investigations & Compliance



Nicolas Tollet
Partner
E : nicolas.tollet@cms-fl.com



Vincent Desbenoit
Associate
E : vincent.desbenoit@cms-fl.com



Guillaume Roche
Associate
E : guillaume.roche@cms-fl.com



Soraya Saouli
Paralegal
E : soraya.saouli@cms-fl.com

GDPR



Anne-Laure Villedieu
Partner
E : anne-laure.villedieu@cms-fl.com

Customs and international trade compliance, Export controls and EU economic sanctions



Denis Redon
Partner
E : denis.redon@cms-fl.com



Karim Soussi
Counsel
E : karim.soussi@cms-fl.com

Dispute Resolution



Jean-Fabrice Brun
Partner
E : jean-fabrice.brun@cms-fl.com



Olivier Kuhn
Partner
E : olivier.kuhn@cms-fl.com



Chloé Adelbrecht-Vignes
Counsel
E : chloe.adelbrecht-vignes@cms-fl.com



Stivian Kostadinov
Counsel
E : stivian.kostadinov@cms-fl.com



Cécile Rebiffé
Counsel
E : cecile.rebiffe@cms-fl.com



Mylène Garrouste
Associate
E : mylene.garrouste@cms-fl.com



Marie Santori
Associate
E : marie.santori@cms-fl.com

Antitrust, Misleading Practices, Product Compliance and Deforestation



Vincent Lorieul
Partner
E : vincent.lorieul@cms-fl.com



Amaury Le bourdon
Counsel
E : amaury.lebourdon@cms-fl.com

CMS Francis Lefebvre Avocats
2 rue Ancelle
92522 Neuilly-sur-Seine Cedex
France

T +33 1 47 38 55 00

CMS Francis Lefebvre, an entity operating in the form of a French limited professional firm (société d'exercice libéral à forme anonyme or S.E.L.A.F.A.), is a member of CMS LTF Limited (CMS LTF), a company limited by guarantee incorporated in England and Wales (no. 15367752) with its registered office at Cannon Place, 78 Cannon Street, London EC4N 6AF, United Kingdom. CMS LTF coordinates the CMS organisation of independent law firms. CMS LTF does not provide any client services. These services are provided solely by CMS LTF member firms in their respective jurisdictions. CMS LTF and each of its member firms are separate and legally distinct entities, and neither entity has the authority to bind the other. CMS LTF and each member firm are responsible only for their own acts or omissions and not for those of others. The brand name "CMS" and the term "firm" are used to designate all or some of the member firms or their offices.

Further information is available at cms.law.

cms.law/fl

© CMS Francis Lefebvre (October 2026).