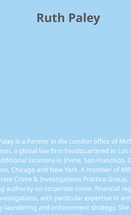
From prevention to attribution: The next frontier of corporate liability

Ruth Paley discusses a planned change to the law that could have wide-reaching impact across all sectors



Ruth Paley

Ruth Paley is a Partner in the London office of Michelman & Robinson, a global law firm headquartered in Los Angeles with additional locations in Irvine, San Francisco, Dallas, Houston, Chicago and New York. A member of M&'s Corporate Crime & Investigations Practice Group, she is a leading authority on corporate crime, financial regulation and investigations, with particular expertise in anti money laundering and enforcement strategy. She can be contacted on +44 (0)20 3334 8333 or at rpaley@mrllp.com.

For many in the UK compliance community, the headline development of the past year has been the arrival of the new failure to prevent fraud offence under the Economic Crime and Corporate Transparency Act (ECCTA). It is a significant change, and there's no doubt it has added to the investigations, training and monitoring burden for larger firms.

But the development that matters most has attracted far less commentary. Alongside failure to prevent fraud, ECCTA introduced a statutory route for attributing offences to companies via senior managers, a shift that the Crime and Policing Bill now seeks to expand to cover all criminal offences.

A significant rebalancing of risk

Under s196 ECCTA, if a senior manager, acting in the ordinary course of their job – within the 'actual or apparent authority' of their role – commits an economic crime offence, the organisation can now also be held liable, and subject to an unlimited fine.

The definition of 'senior manager' is not the same as that applied by the FCA in the Senior Managers and Certification Regime (SMCR). For the purposes of s196, titles aren't relevant; function is. What matters is whether an individual plays a significant role in decision-making or in managing a substantial part of the business or its activities. The relevant population extends well beyond traditional leadership: regional managers, product heads, key operations leaders, financial controllers, HR chiefs and the senior figures who govern risk, compliance and audit may all fall within the scope.

This isn't a question of whether the individual was authorised to commit the criminal act, but whether the type of act sits within the ordinary run of their role. If it does, then, for the purposes of attribution, the act becomes the company's own, even where the business had no knowledge of the misconduct, derived no benefit from it, and may have been its only victim.

This development alone marked a significant rebalancing of corporate criminal risk. But the Crime and Policing Bill goes a step further. It proposes that the same attribution model should apply to ***all*** criminal offences, not just economic crime, pulling into scope areas such as health and safety, fire and building regulations, environmental permitting, food safety, data governance, cyber security and even non-financial misconduct where it is connected to the individual's role.

> **If a senior manager, acting in the ordinary course of their job – within the 'actual or apparent authority' of their role – commits an economic crime offence, the organisation can now also be held liable, and subject to an unlimited fine.**

No reasonable procedures defence

There are three reasons why this is so consequential for corporates. First, unlike failure to prevent bribery, tax evasion or fraud, the shield of 'reasonable or adequate procedures' isn't available . A gold-standard framework may reduce the likelihood of misconduct occurring, and it may shape the public interest assessment in the organisation's favour, but it does not offer a statutory defence to liability once the act is committed.

Secondly, the test doesn't include a requirement that the individual acted to benefit the organisation. It is enough that the act fell within the ordinary scope of their managerial role. A CFO who misstates the accounts to perpetrate a fraud is still acting in their ordinary role of overseeing the preparation and distribution of financial statements, even though no one gave them authority to do the job badly – or criminally. Whether the individual acted for personal gain, through negligence, or even with malice towards the organisation isn't determinative. This represents a sharp departure from models that tether corporate liability to notions of corporate benefit or connivance.

Thirdly, and perhaps most overlooked, is the role of recklessness. In many offence types outside economic crime, recklessness is sufficient for criminal liability. Health and safety, environmental and data protection regimes all contain offences that can be committed recklessly. Under the proposed extension, a senior manager who knowingly takes an unjustifiable risk in the course of their role could expose the company to liability, even in the absence of intention.

> **Unlike failure to prevent bribery, tax evasion or fraud, the shield of 'reasonable or adequate procedures' isn't available.**

A shift in focus

The compliance implications come into focus when applying the test to real financial services scenarios.

- This could arise as part of market-abuse controls: for instance, a head of surveillance dealing with an overwhelming surge in alerts during a period of volatility and deciding to switch off certain monitoring thresholds to keep workflows manageable. Suspicious trading during that window might go undetected. Because surveillance oversight sits squarely within their role, the omission could, under the Bill's extension, be treated as the firm's own act.
- Reading across into other areas of screening such as transaction monitoring alerts, politically exposed persons (PEPs) and sanctions screening, another example might see a regional payments director faced with a high-value, time-critical transaction and potential sanctions hit instruct staff to process it manually 'while we re-check the match'. If the payment is later found to have breached sanctions, that operational judgment, routine in managerial terms, could be attributed to the company in law.
- Data governance is another area of exposure. A senior technology manager might, under pressure to deliver a platform upgrade, postpone critical security patches or disable certain access-controls 'temporarily' to keep customer systems online. If a cyber incident follows, exposing sensitive client data, and because safeguarding data integrity and system security sits within their day-to-day remit, that decision, a typical operational trade-off, could, under the expanded attribution model, be treated as the firm's own criminal breach.

These examples illustrate that the most significant risks may arise not from obscure criminal provisions but from decisions made under pressure in the ordinary flow of business. The frontline for corporate exposure becomes the point where senior judgement is exercised. For compliance officers, this requires a shift in focus. The traditional framework of policies, controls and training remains essential, but it must now be accompanied by a more acute understanding of where real-world decision-making authority sits and how it is exercised.

Practical actions

With that in mind, firms may want to consider the following practical actions.

- **Build a clear and regularly refreshed picture of the senior-manager population.** Mapping this group by function rather than title helps reduce blind spots. Alongside this, identify everyday activities where criminal exposure can arise (for example, onboarding exceptions, discretionary pricing, client entertainment, surveillance adjustments, operational work-arounds, system overrides, data-access decisions or actions involving safety, cyber or environmental controls) then consider where additional challenge or documentation is sensible.
- **Strengthen the consistency and quality of decision-making records.** When senior managers make high-impact calls under pressure, contemporaneous notes, short risk summaries and clear escalation routes can be critical in showing what was known and considered at the time. Even brief records can materially shape the public-interest assessment if issues arise.
- **Revisit governance around 'temporary' operational fixes.** Many incidents begin with short-term workarounds, like pausing a control, disabling an alert, extending a threshold or delaying remediation. Ensuring that these decisions carry a short, written record, a time limit, or second-line visibility can help prevent ad-hoc fixes from becoming embedded risks.
- **Review escalation pathways for higher-risk judgement calls.** Decisions such as overriding a sanctions alert, adjusting surveillance thresholds, approving unusual transaction flows, or granting high-risk data access may justify defined routes to Compliance, Legal or Risk before a final call is made. Targeted second-line review in functions with significant discretion (e.g. onboarding, payments operations, trading supervision, fraud decisioning or data governance) can surface issues earlier.
- **Keep notification duties in mind.** Suspected misconduct capable of being attributed to the company may trigger obligations under directors and officers or crime policies well before any enforcement action. Firms need to align internal investigation processes with policy thresholds and establish pre-agreed mechanisms for engaging insurers or brokers while protecting privilege.
- **Apply the same discipline to audit-committee engagement.** Where potential criminal exposure intersects with financial reporting (provisions, contingent liabilities etc), auditors may need early sight of emerging facts. A concise briefing that separates what is known from what remains under investigation can help maintain transparency and avoid later difficulties.

When considering whether to prosecute, the authorities will continue to apply the familiar two-stage test for charging decisions. Evidential sufficiency remains the threshold question. But in practice, the public interest stage will have growing importance for organisations. Factors such as early self-reporting, victim remediation, structural reforms, leadership accountability, and evidence of a credible compliance framework can weigh meaningfully against charge. Conversely, repeated issues, ineffective controls, or delayed engagement may push in the opposite direction. The message for compliance officers is clear: the public interest case is built over months or years, not in the aftermath of a dawn raid.

The key message is that organisations need to act now to embed stronger challenge, better documentation, and more thoughtful escalation around senior decision-making. Firms already know that even experienced managers can make imperfect decisions when under pressure. Systems must be designed not only to guide behaviour but to catch mistakes before they crystallise into criminal exposure. In all of this, compliance's role as a central mechanism for managing the organisation's criminal-law identity is stronger than ever.

The firms that take this shift seriously, and equip their compliance functions to lead the adjustment, will define the new standard. Those that hesitate may find the law has moved on without them.

> **The key message is that organisations need to act now to embed stronger challenge, better documentation, and more thoughtful escalation around senior decision-making.**