Mar. 26, 2025

Mergers & Acquisitions

M&A Considerations for the New Frontiers of U.K. Compliance Risk

By Simon Airey, James Dobias, William Merry and Kelly Newsome, *McDermott Will & Emery*

Amidst the high activity and limited bandwidth of any corporate M&A transaction, compliance-related due diligence is often an area of lower focus or a mere check-box exercise. However, corporate marriages made in haste can be repented at leisure, and those acquiring companies can inherit more than they expected. This is particularly the case in light of recent developments in the U.K. that significantly lower the bar for findings of corporate criminality. In this article, we review the recent changes resulting from the passage of the U.K. Economic Crime & Corporate Transparency Act 2023 (ECCTA), consider how it impacts M&A risk for companies worldwide with any U.K. touchpoints, and offer suggestions for what companies should be doing now to mitigate the associated risk.

See "U.K. Enhances Anti-Fraud Efforts With Economic Crime and Corporate Transparency Act" (Jan. 17, 2024).

The Impact of ECCTA

Historically, establishing corporate criminal liability in the U.K. required a prosecutor to prove that the board of directors of a company (or those to whom they, or the company's articles, had specifically delegated authority) were involved in the relevant crime in order for the conduct to be imputed to the company. This was referred to as the "identification principle" and was a tough hurdle to pass in practice. Given the scale of many modern businesses and the diffuse nature of corporate decision-making, it was rare that prosecutors could prove that sufficiently senior personnel were involved in the relevant conduct, and often the reality was that it was more junior employees who were involved. In one high-profile case, even the alleged involvement of the CEO and CFO in the relevant conduct was found not to satisfy the identification principle, as they had not been explicitly authorised by the board to act as they allegedly did.

Until recently, there were only a handful of exceptions to this general rule, most notably, the "failure to prevent bribery" offence under the U.K. Bribery Act 2010 and the "failure to prevent the facilitation of tax evasion" offences under the U.K. Criminal Finances Act 2017. However, time and time again, U.K. law enforcement authorities complained that the U.K.'s corporate criminal liability regime was not fit for purpose in the modern world and that corporates could – outside of these specific exceptions – escape liability by insulating their boards from criminality by their employees.

The passage of ECCTA in late 2023 represented a sea change in this approach, introducing two major reforms relating both to companies incorporated in the U.K. and to non-U.K. companies with a relevant nexus to the U.K. In short, companies can now be prosecuted for a wider range of conduct and for conduct occurring at a much more junior level in the organisation.

Liability for the Acts of Senior Managers

ECCTA introduced liability on the part of companies for the criminal acts of their "senior managers" in relation to a wide range of economic crimes. This represents a significant lowering of the hurdle for liability compared to the identification principle. Since December 26, 2023, when the relevant provisions of ECCTA came into effect, it has been possible for companies to be prosecuted for relevant offences committed by their senior managers, so long as they were acting within the actual or apparent scope of their authority (Senior Managers Regime). This power to prosecute companies is in addition to powers that U.K. prosecutors already have to prosecute individuals for the same offence.

Under ECCTA, "senior managers" are defined as individuals who play a significant role in either (a) the making of decisions about how the whole, or a substantial part, of the activities of the company are to be managed or organised or (b) the actual managing or organising of the whole, or a substantial part, of those activities. This is a broad definition that is likely to be widely interpreted to catch divisional roles and those in group subsidiaries, including overseas. According to guidance issued by the U.K. government, even senior individuals with functional, non-executive roles (*e.g.*, those in sales, marketing, legal, finance, HR or compliance) can fall within the scope of the senior manager definition.

The range of offences within the Senior Managers Regime includes fraud, bribery, theft, false accounting, money laundering, financial regulatory and tax-related offences. False accounting, in particular, is a wide offence under English law and can apply not only to formal accounts but also to any paper or electronic record or document made or required for any accounting process (including invoices, contracts and time entries).

At the time of writing, draft legislation is being considered by the U.K. Parliament to expand the Senior Managers Regime to apply to *all* crimes.

The Failure to Prevent Fraud Offence

ECCTA introduced a new corporate "failure to prevent fraud" offence (FTP Fraud Offence), under which criminal liability can attach to "large organisations" on a strict liability basis for frauds committed by their "associated persons" even if senior management was unaware of the conduct.

The only defence to the FTP Fraud Offence is for the company to establish that it had "reasonable prevention procedures" in place to prevent the relevant conduct. Guidance as to what constitutes "reasonable prevention procedures" was published by the U.K. government in November 2024 and is discussed further below (ECCTA Guidance). Further guidance specific for the financial services sector was published by trade body UK Finance in February 2025, albeit this guidance is non-statutory and advisory only.

The FTP Fraud Offence comes into force on September 1, 2025.

Under ECCTA, "large organisations" are those that meet any two of the following three criteria:

1. more than 250 employees;
2. more than £18 million in total assets; and/or
3. more than £36 million of turnover.

"Associated persons" is widely defined to mean all employees, plus agents and subsidiaries of the organisation, and those who otherwise perform services for or on behalf of the organisation, no matter how junior.

The range of fraud offences within the FTP Fraud Offence is broad and includes offences under the U.K. Fraud Act 2006 (*e.g.*, fraud by false representation, by failing to disclose information and by abuse of position), false accounting (which – as set out above – is expansive in scope) and the common law offence of cheating the public revenue.

By way of example as to the breadth of this offence, a corporate could face criminal liability if any of its employees or service providers – no matter how junior – were to manipulate the timing of payments to improve the reporting of revenues, exaggerate product data to lure in a client or pad revenue figures in order to hit targets. Unlike bribery conduct, which can often be confined to particular industries, business units and geographies, these fraudulent behaviours, many of which occur at low levels in an organisation, are widespread and frequent, and will likely be found to some extent in many – if not most – businesses.

See "How Risk Assessments and Policies Can Ward Off New U.K. Fraud Offense" (Feb. 12, 2025).

Extraterritorial Effect

These provisions have wide extraterritorial effect and will therefore need to be considered even by non-U.K. businesses with relevant U.K. touchpoints (*e.g.*, U.K.-based customers, business operations or assets).

For the purposes of the Senior Managers Regime, a company, wherever incorporated, can be liable for the criminal acts of its senior managers wherever they take place, subject to the jurisdictional reach of the underlying criminal offence. Examples could include where the chief commercial officer of a Swiss company instructs a team member to back-date an invoice issued to a U.K. customer in order to impact when revenue is recognised, or where the head of insurance in a U.S. company approves an insurance claim underwritten by a U.K. insurer while knowing that it is exaggerated.

Likewise, regarding the FTP Fraud Offence, there is no need for the large organisation to be incorporated in the U.K. All that is required is that there is a relevant U.K. link to the fraud (*e.g.*, U.K. victims, U.K. conspirators or where part of the relevant conduct took place in the U.K.). By way of example, a U.S. professional services firm could be criminally liable in the U.K. for failing to prevent an employee in New York from exaggerating time records when working for a U.K. client.

See "The SFO's Five-Year Strategy: Rebooted, Recharged and Ready to Rumble?" (Jun. 5, 2024).

Impact on M&A

In the context of M&A transactions, the significant lowering of the bar by ECCTA for corporate criminality requires those acquiring companies (or their assets) to pay close attention to where risk may lie in their targets and those selling companies (or their assets) to consider what they can do proactively to address these risks.

Properly considering such risks will not only help avoid potential surprises, such as inherited criminal liability, but also potentially act as a driver of value. In particular, purchasers can use any gaps identified in fraud- or senior manager-related compliance controls to argue for a reduction in price. Likewise, sellers can market any proactive steps they have put in place as a differentiator versus their competitors and a source of value.

While there is no one-size-fits-all solution for companies to adopt, there are steps that can be taken immediately to ensure that companies are properly prepared for these reforms.

Due diligence, Representations and Warranties

At a minimum, purchasers should consider updating what may otherwise be template due diligence questions that were designed to address historical bribery risk and are now inapposite to identify the wider risks posed by the Senior Manager Regime and FTP Fraud Offence.

In relation to the FTP Fraud Offence, this would involve a focus on what steps the target has taken to help ensure the availability of the "reasonable prevention procedures" defence and testing whether such steps have been adequately embedded and followed in practice.

In relation to the Senior Managers Regime, the position is more complex as there is no "reasonable prevention procedures" defence. The comfort required is effectively that senior managers at the target have not historically engaged in criminality and will not do so going forward. Due diligence questions, therefore, would aim to uncover who the senior managers are at the target, whether those senior managers face any incentive to engage in risky practices, whether they are sufficiently well trained, and whether monitoring and assessment controls are sufficiently robust to identify any improper conduct. Purchasers may also wish to consider requiring attestations from the target's senior managers that they have complied with applicable laws and not engaged in prohibited behaviours.

In relation to both offences, due diligence questions should also seek to identify any relevant U.K. touchpoints for the target, which would mean that the extraterritorial provisions of ECCTA might apply. Examples would include any U.K. customers, service providers, operations, share listings or assets.

Likewise, representations, warranties and indemnities in contractual documentation should seek to cover these areas, and associated insurance policies should be reviewed to ensure that they are wide enough to cover the new risks.

See this three-part series on managing M&A anti-corruption risk: "Pre-Deal Prep" (Oct. 3, 2018), "Pre-Closing Risk Assessments and Due Diligence" (Oct. 17, 2018), and "Deal Terms and Integration" (Oct. 31, 2018).

Training

Regarding the Senior Manager Regime, sellers looking to reduce risk and respond convincingly to due diligence questions should consider ensuring that potential senior managers across the target are identified and, along with their key reports and team members, provided with enhanced compliance training.

This training should reinforce what behaviours are unacceptable and emphasise the importance of complying with applicable laws and company policies. While, in the context of the Senior Manager Regime, it is no defence for the company to show that it had "reasonable prevention procedures" in place, such training can nevertheless help to reduce the risk of inappropriate behaviour occurring in the first place.

See "Rethinking Click-Through Training: The Pluses and Minuses" (Feb. 26, 2025).

Risk Assessment

Regarding the FTP Fraud Offence, a key first step would be to take account of the ECCTA Guidance as to the meaning and scope of "reasonable prevention procedures" under ECCTA. The ECCTA Guidance is both detailed and complex, and calls for a meaningful response to real risks.

As stated in the ECCTA Guidance, an important first step would be to undertake a comprehensive fraud risk assessment to determine the areas of highest risk across the business. Ideally, this assessment would be undertaken by lawyers so that privilege may apply to the work product, and to avoid the company inadvertently creating a road map to potential liabilities that could be disclosable in litigation or to law enforcement authorities. On the other hand, it might be appropriate to compile the risk assessment specifically with disclosure in mind. Either way, the risk assessment must be very carefully drafted and compiled.

This risk assessment would then help guide corporates as to what other steps will be required to meet the "reasonable prevention procedures" test within the context of the organisation. According to the ECCTA Guidance, the dimensions to consider for the calibration of such additional steps include: tone from the top, appropriate risk-based policies and procedures, third-party due diligence, communication (including training), and monitoring and review.

See this four-part guide to risk assessments: "Types of Assessments" (Jun. 26, 2019), "Techniques and Building a Team" (Aug. 7, 2019), "Where to Look for Risk and Risk Ranking" (Sep. 4, 2019), and "Wrapping Up and Avoiding Pitfalls" (Jan. 22, 2020).

Checklist of Key Points

There is no one-size-fits-all approach, and each organisation will need to consider what will be required in the context of its own business activities and risk profile. However, companies should consider the following:

- Advise key stakeholders of the recent reforms to U.K. law and ensure tailored training is provided to key (or even all) employees.
- Update due diligence questionnaires and scopes to take account of the new legal exposures.
- As part of due diligence, seek access to relevant risk assessments (or appropriate summaries), evidence of "reasonable prevention procedures" and a proper understanding of who the senior managers are, and what related controls are in place.
- Tailor negotiations, representations, warranties, indemnities, pricing and payment provisions according to the relevant risks.
- Update template compliance terms in contracts and consider clarifying (*e.g.*, in the form of the Supplier Code of Conduct) the standards expected of all third parties with whom you work.
- Consider the scope for post-transaction remediation, claims and litigation.
- Consider any impact upon insurance policies, banking covenants and disclosure obligations.
- Be aware that the increased scope of the legal exposures means an increased likelihood that due diligence may uncover possible proceeds of crime. Proceeding with or facilitating a transaction that involves the proceeds of crime could amount to a criminal offence unless you first obtain a formal "defence against money laundering" from the U.K. authorities. U.K. professionals acting on the transaction will also have their own disclosure obligations to consider in such circumstances.

Braving These New Frontiers

Over the past year, we have seen widespread global conflict and economic stress, while countries representing approximately half the world's population have held national elections with significant impacts. Such widespread turmoil not only facilitates the discovery of past wrongdoing but can lead to increased levels of fraud, inappropriate behaviours and corporate insolvencies, in each case increasing exposure for businesses, customers and service providers. Against this background, it is crucial that both purchasers and sellers appropriately consider the risks they face and proactively seek to head off future issues. They should also look at problems and potential solutions holistically, not just through the lens of a single jurisdiction.

Companies that are prepared and proactively address relevant compliance risks head-on can secure significant commercial advantage. The right compliance enhancements, supported by a well-designed risk assessment, can help differentiate a company from its competitors, satisfy shareholder pressure and, crucially, drive value in the M&A process by better insulating the organisation against the real risk of investigation and potential prosecution by well-resourced investigative agencies keen to make use of their new powers.

Simon Airey is a partner based in McDermott Will & Emery's London office. His practice focuses on global, cross-border, and internal investigations; financial and regulatory crime; bribery and corruption; money laundering; tax and fraud inquiries; data breaches; dawn raids; asset tracing; international enforcement; and corporate compliance issues. He serves as co-head of the firm's global investigations and compliance practice.

Kelly Newsome is a partner based in McDermott Will & Emery's New York office. She advises corporations and individuals in white-collar criminal and regulatory matters across the globe. Her practice focuses on the FCPA and other anti-corruption laws and regulations, and she represents clients in a variety of industries, including oil and gas; hospitality and tourism; life sciences, medical device and pharmaceutical; and financial services.

James Dobias is counsel in McDermott Will & Emery's London office. His practice focuses on a range of domestic and international corporate crime and investigations-related matters, including bribery, corruption, fraud, money laundering, tax evasion, data breaches, and associated regulatory and compliance issues.

Will Merry is an associate in McDermott Will & Emery's London office. He has experience in resolving anti-bribery and corruption, anti-money laundering, fraud and sanctions matters in both contentious and non-contentious contexts.