Economic Crime and Corporate Transparency Act

What Multinationals Need to Know about UK Corporate Prosecutions

5 December 2024

GIBSON DUNN

MCLE CERTIFICATE INFORMATION

MCLE Certificate Information

- Approved for 1.5 hours General PP credit.
- CLE credit form must be submitted by **Thursday, December 12th.**
- Form Link: https://gibsondunn.qualtrics.com/jfe/form/SV_6lKLIILLQYdvv4G
  - Most participants should anticipate receiving their certificate of attendance in four to eight weeks following the webcast.

- **Please direct all questions regarding MCLE to CLE@gibsondunn.com.**

TODAY'S PRESENTERS

Allan Neil
Partner / London, UK

Chris Loudon
Of Counsel / London, UK

Amy Cooke
Associate / London, UK

Marija Bračković
Associate / London, UK

John W.F. Chesley
Partner / Washington, D.C., USA

Moderator

Topics

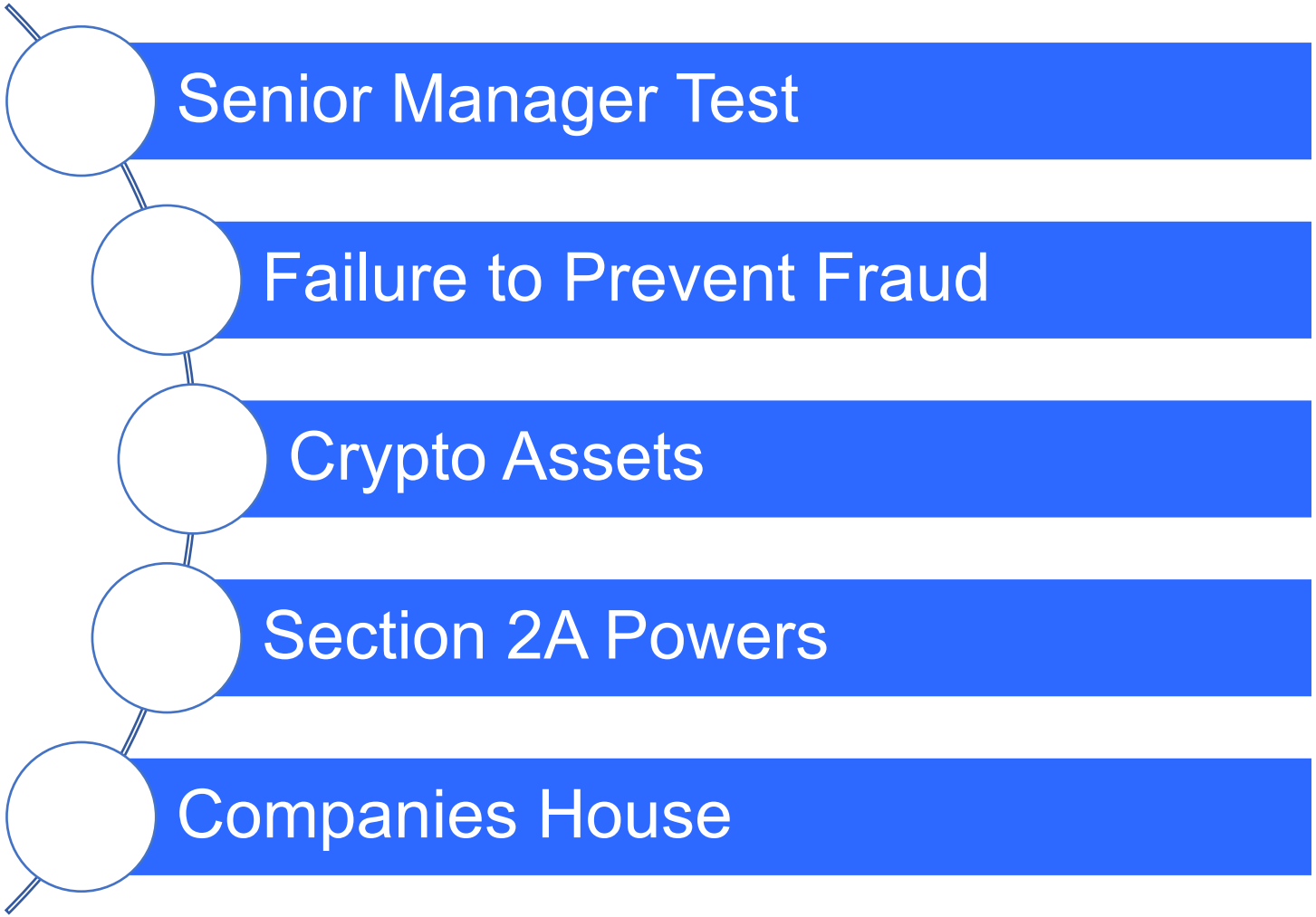
INTRODUCTION

1

ECCTA Overview

- The Economic Crime and Corporate Transparency Act (ECCTA) made fundamental changes to the UK's approach to tackling financial crime
- Most significantly, it introduced new law governing:
  - the attribution of criminal liability to corporate entities (which came into force on 26 December 2023); and
  - a new corporate offence of failure to prevent fraud (which will come into force on 1 September 2025)

ECCTA
Key Issues



SENIOR MANAGERS

2

UK Corporate Criminal Liability Redefined
"Directing Mind and Will" Principle

Prior to ECCTA, UK law provided that a corporate entity could not be held criminally liable for acts committed by an employee unless the offence was committed by a person who was "*the directing mind and will of the corporation*"

The "directing mind and will" standard has been narrowly defined by UK courts as:

"*Normally the board of directors, the managing director and perhaps other superior officers of a company [who] carry out the functions of management and speak and act as the company*"

– *Tesco Supermarkets Ltd v. Nattrass* [1971]

This standard was confirmed by *The Serious Fraud Office v. Barclays PLC & Anr* [2018], which dismissed fraud charges against Barclays plc on the basis that, on the facts presented, even the CEO and CFO did not represent the "*directing mind and will*" of the bank

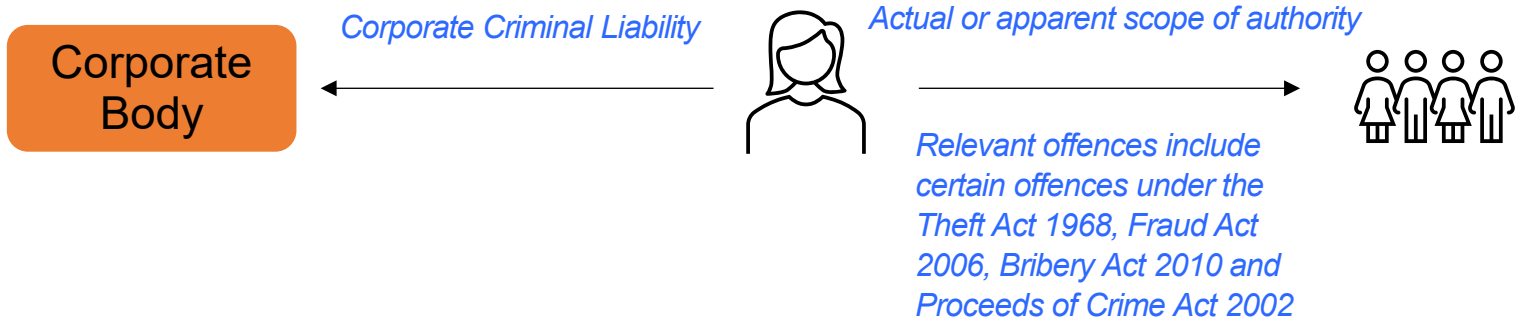
UK Corporate Criminal Liability Redefined

ECCTA Standard

The new standard for corporate criminal liability under ECCTA is as follows:

> *"If a senior manager of a body corporate* or partnership… acting within the actual or apparent scope of their authority commits a relevant offence… the organisation is also guilty of the offence"*

This provision is effective as of December 26, 2023, and is not retroactive



*Body corporate includes a body incorporated outside of the UK but does not include a corporation sole or a partnership not regarded as a body corporate under applicable law

UK Corporate Criminal Liability Redefined
Senior Managers

Senior manager means an individual who plays a "*significant role*" in:

- "*the making of decisions about how the whole or a substantial part of the activities*" of the corporate are to be "*managed or organised*," or
- "*the actual managing or organising of the whole or a substantial part of those activities*"

This could be argued to include:

- a desk (unit) head,
- a functional or country head and/or
- individuals with oversight of teams or sections of the business

UK Corporate Criminal Liability Redefined

Actual or Apparent Scope of Authority

Actual or apparent scope of authority is not defined in the legislation:

- actual authority would likely be evidenced by job descriptions, board resolutions and minutes and HR documentation;
- apparent authority may be more difficult to define, but courts will likely look to the interpretation applied in the context of civil fraud committed by agents - this considers, *inter alia*, whether the principal represents or holds out that its agent had authority even if that is wider than the agent's actual authority

Issues to consider include:

- individuals with loosely or ill-defined roles in an organisation, e.g., "Chief Change Maker," and
- inflated job titles that do not match an individual's actual role

UK Corporate Criminal Liability Redefined

Relevant Offences

Relevant offence means an economic offence listed in ECCTA Schedule 12 (see Appendix A)

Schedule 12 offences include (amongst others):

- fraud, theft, false accounting,
- false statements by directors,
- undertaking regulated business without proper authorisation,
- money laundering offences and/or
- bribery, including bribery of a foreign public official

Attempts or conspiracies to commit such offences, as well as aiding, abetting, counselling or procuring the commission of a Schedule 12 offence are covered

The Criminal Justice Bill 2023 proposes to extend this to all criminal offences

UK Corporate Criminal Liability Redefined

Extraterritoriality

- Most UK criminal offences require that part of the offence takes place in the UK
- A limited category of offences can be prosecuted where no acts take place in the UK, but the offender has a close connection to the UK

> *"Where no act or omission forming part of the relevant offence took place in the United Kingdom, the organisation is not guilty of an offence under subsection (1) unless it would be guilty of the relevant offence had it carried out the acts that constituted that offence (in the location where the acts took place)."* ECCTA Section 196(3)

- The effect of this provision is to preserve this position with respect of corporate liability

Most importantly, corporations will not be liable for offending outside of the UK simply because the senior manager involved has a close connection to the UK

UK Corporate Criminal Liability Redefined

Comparison with US *Respondeat Superior* Standard

In the United States, the main theory for imputing the actions of individual representatives to a company is *respondeat superior*

The common law doctrine of *respondeat superior* ("let the master answer") provides a corporation may be criminally liable for the actions of its directors / officers / employees / agents if those actions were:

- within the scope of their duties, and
- intended, at least in part, to benefit the corporation

U.S. v. Agosto-Vega, 617 F.3d 541, 552-53 (1st Cir. 2010)

Corporate criminal liability may be imposed even if the "*actions were contrary to corporate policy*" and actually detrimental to the company, provided there was "*intent to benefit the corporation*" *U.S. v. Automated Med. Labs., Inc.*, 770 F.2d 399, 407 (4th Cir. 1985); *see also* *U.S. v. Basic Constr. Co.* (711 F.2d 570, 572-73 (4th Cir. 1983) (imposing corporate criminal liability for the actions of low-level employees)

FAILURE TO PREVENT FRAUD OFFENCE

3

Failure to Prevent Fraud Offence
Key Elements (1 of 2)

ECCTA also creates the new corporate offence of failure to prevent fraud

Under section 199 of ECCTA, a large organisation will be criminally liable if:

- a person associated with it,
- commits a relevant fraud offence,
- to benefit (directly or indirectly) the organisation, its subsidiary or a client of the organisation

An affirmative defence is available where the organisation can show it had reasonable procedures in place to prevent fraud

The Home Office published guidance on the offence on 6 November 2024. This offence is not yet in force, and will not be until 1 September 2025

Failure to Prevent Fraud Offence
Key Elements (2 of 2)

Large organisation: includes a body corporate or partnership that satisfies **at least two** of the following criteria in the financial year prior to the alleged fraud offence:

- more than £36m (approx. $45m) global turnover;
- more than £18m (approx. $23m) balance sheet total; and/or
- more than 250 employees

Associated person: employee of the large organisation or employee of a subsidiary, agent, subsidiary undertaking or person otherwise performing services for or on behalf of the organisation

Benefit: includes intended benefit to the organisation, its clients or a subsidiary. This is broader than the UKBA, which focuses more narrowly on intended benefit to the organisation

The offence will apply even if the associated person's primary intent is to benefit themselves and their secondary intent is to benefit the organisation, its clients or a subsidiary

Failure to Prevent Fraud Offence
Underlying Fraud Offences

Relevant fraud offences

The offences in scope are listed in Schedule 13 (see Appendix B) and include:

- Fraud offences under the Fraud Act 2006:
  - Fraud by false representation
  - Fraud by failing to disclose information
  - Fraud by abuse of position
- Participating in a fraudulent business
- Obtaining services dishonestly
- Cheating public revenue
- False accounting
- False statements by company directors
- Fraudulent trading

Failure to Prevent Fraud Offence
Jurisdictional Reach (1 of 2)

A large organisation may commit the UK offence even if it is not incorporated or formed in the UK, if an act or economic impact occurs in the UK

The failure to prevent fraud offence will be engaged if the employee or associated person commits a relevant fraud offence in part in the UK

For some offences (including the principal Fraud Act offences) it is sufficient that the gain or loss occurred in the UK

The Home Office Guidance states:

> *"The offence will only apply where the associated person commits a base fraud offence under the law of part of the UK. This requires a UK nexus. By UK nexus, we mean that one of the acts which was part of the underlying fraud took place in the UK, or that the gain or loss occurred in the UK"*

Failure to Prevent Fraud Offence Jurisdictional Reach (2 of 2)

Failure to Prevent Fraud Offence Consequences

- On conviction of a failure to prevent fraud offence, a company will be liable for an unlimited fine
- A conviction may also have other consequences, such as confiscation proceedings or debarment and may expose individuals to risk of criminal or regulatory proceedings
- A company may be able to negotiate a Deferred Prosecution Agreement (DPA) if the Serious Fraud Office deems that the conduct and circumstances of the offending are appropriate
- A DPA will only be considered if the company can demonstrate that it has fully cooperated with the SFO's investigation. DPAs must be approved by a court

Failure to Prevent Fraud Offence
Comparison with UKBA

Key Element of Offence	Failure to Prevent Fraud *Sections 199-201 of ECCTA 2023*	Failure to Prevent Bribery *Section 7 of the Bribery Act 2010*
Defendant	**A relevant body which is a large organisation →** *£36m+ turnover, £18m+ balance sheet, 250+ employees*	**A relevant commercial organisation →** *no financial/employee threshold*
Associated Person	**A person associated with the organisation →** employee, agent, subsidiary undertaking or anyone who performs services for or on behalf of organisation or an employee of subsidiary undertaking	**A person associated with the organization →** anyone who performs services for or on behalf of the organisation including employees, agents and subsidiaries
Underlying Offence	Commits a **fraud offence**	**Bribes** another person
Intent	To benefit (directly or indirectly) the **organisation, its subsidiary, its clients or its client's subsidiary**	To obtain/retain business or an advantage in the conduct of business for the **organisation**
Statutory Defence	At the time the fraud offence was committed, it had **reasonable prevention procedures** in place designed to prevent persons associated with the body from committing fraud offences	It had **adequate procedures** in place to prevent bribery
Jurisdiction	The failure to prevent offence will be engaged if the underlying fraud offence can be prosecuted in the UK. Most underlying offences will require part of the offence to take place in the UK, such as the gain/loss	Applies to all companies incorporated in the UK or which carry out business or part of a business in the UK. It is irrelevant where the acts or omissions which form part of the underlying offence take place

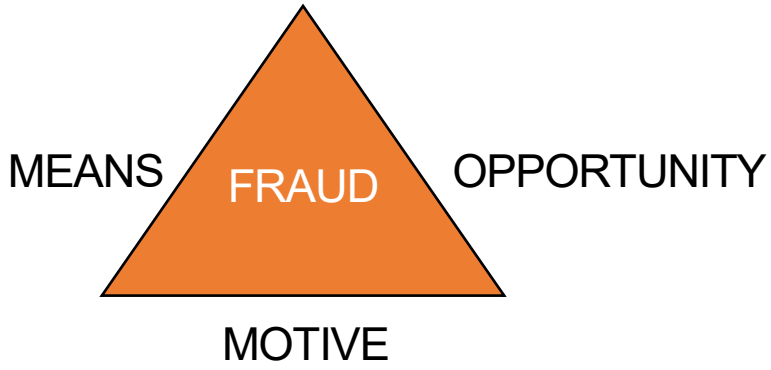
REASONABLE PREVENTION PROCEDURES DEFENCE IN PRACTICE

4

Reasonable Prevention Procedures Defence
Risk Assessments (1 of 7)

The first and most important element of the reasonable prevention procedures defence is a fraud risk assessment. We note that:

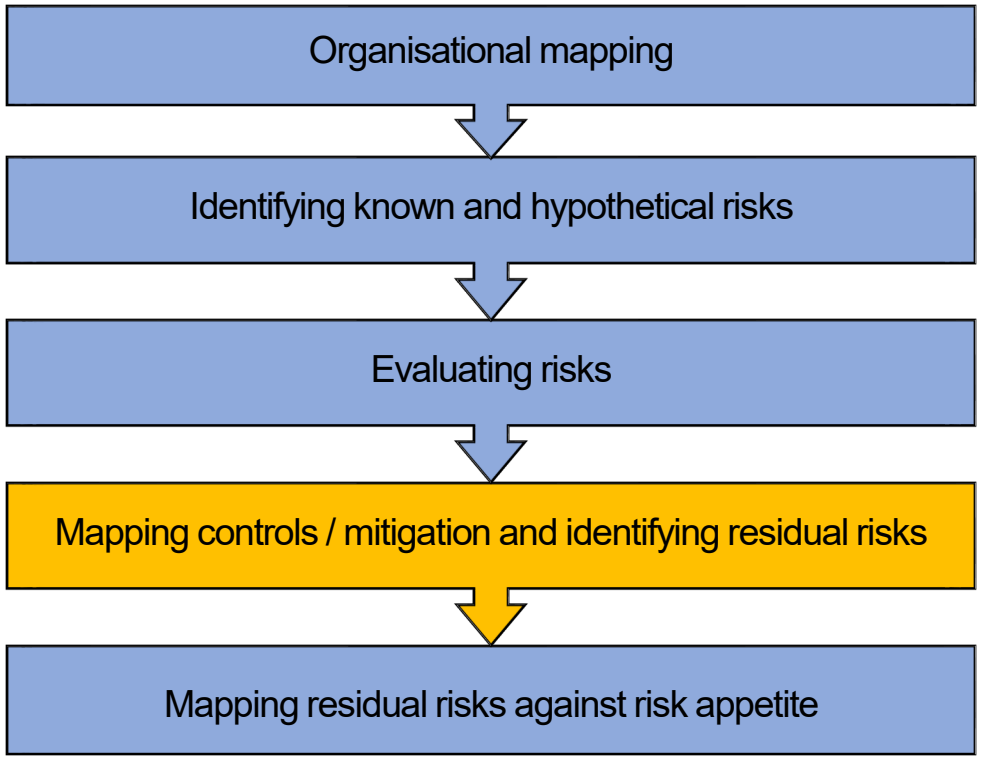
- many companies will already be conducting fraud risk assessments or will be considering fraud risk through existing internal and/or external audits;
- these need to be reviewed and tailored to reflect the particular risks presented by the FTPF offence; and
- the utility of applying Albrecht's fraud triangle (cited in the Home Office Guidance) when conducting fraud risk assessments



The Home Office Guidance states that *"it is not necessary or desirable for organisations to duplicate existing work. Equally, it would not be a suitable defence to state that because the organisation is regulated its compliance processes under existing regulations would automatically qualify as "reasonable procedures"*

Reasonable Prevention Procedures Defence
Risk Assessments (2 of 7)

Fraud risk assessment methodology: there is no fixed, 'one-size-fits-all' methodology for conducting a risk assessment. Most risk assessment methodologies will include the following steps:



A fraud risk assessment will usually be conducted through an appropriate mix of targeted document reviews (focusing on relevant policies and selected documentation), interviews conducted by expert counsel (to protect privilege), and consideration of relevant metrics

Reasonable Prevention Procedures Defence
Risk Assessments (3 of 7)

Organisational mapping

- Relevant when conducting either an enterprise-level review or a thematic review
- The aim is to obtain an accurate snapshot of the business to understand its structure, including its business units, their operating models, incentives, formal and informal reporting lines, vulnerabilities to fraud and relevant policies and procedures

Associated persons

- Key component of organisational mapping is identifying the company's associated persons
- Although companies are likely to have conducted an analysis of their associated persons in the context of their UK Bribery Act procedures, this should be updated to reflect the broader application of the FTPF offence
- This exercise must be conducted with care, as associated persons are likely to present a significant fraud risk vector

Reasonable Prevention Procedures Defence
Risk Assessments (4 of 7)

Identifying and assessing risks

- Entails considering how business is conducted and understanding – and evaluating – the risks of fraud. The process of documenting current risk should be carried out on a regular (usually annual) basis
- A mechanism should be put in place to capture fraud risk presented by new ventures or operational changes by way of off-cycle risk assessments.
- Care should be taken to ensure that documentation generated in the context of the risk assessment process is privileged (albeit some material may be disclosed in due course in order to evidence the affirmative defence)
- Factors to consider when assessing risk include business unit risk, process risk, third party/intermediary risk, transaction risk, and geographical risk. These factors should, however, be assessed against the backdrop of the specific trends and risks presented by the industry in which the company operates

Reasonable Prevention Procedures Defence Risk Assessments (5 of 7)

Industry Risk

Is there a high churn of employees and movement between buy and sell-side?
Have salaries recently been negatively impacted by, for example, an industry-wide slow down?

Business Unit Risk

Are there performance-incentivised sales teams?
Are there offices operating with a high-level of autonomy?
Are there business units with a history of inadequate oversight and supervision?

Process Risk

Are billing processes carried out with little supervision?
Are there processes in place to review new contracts or contract variations?
Does AI or other emerging technologies present a fraud vector?

Third Party/Intermediary Risk

Is the business heavily reliant on the use of agents and contracted sales people?
Do third parties operate with a high-level of independence?
Is there a risk of contagion as bad actors move between companies?

Transaction Risk

Does the business process a high volume of transactions?
Are there numerous low to medium value transactions that do not trigger review or scrutiny?

Jurisdictional Risk

What is the jurisdictional exposure of the business to the failure to prevent fraud offence?
Does the business operate in jurisdictions with a high level of law enforcement interest in fraud offences?
Does the business operate in jurisdictions with a high rate of fraud offending?

Reasonable Prevention Procedures Defence
Risk Assessments (6 of 7)

Evaluating inherent risk

- Entails evaluating the likelihood of fraud risk crystallising. This can be done as a Red Amber Green (RAG) rating, narrative or %
- Analysis is often recorded as a matrix with the likelihood of risk crystallising on one axis against the impact on the other. This measures the inherent risk

Mapping controls / mitigation and measuring residual risks

- Existing anti-fraud systems and controls are mapped against identified fraud risks
- Controls include measures put in place by the compliance function, such as relevant anti-fraud policies and procedures
- Mapping should also consider relevant operational measures including the collection of relevant accounting data-points and thresholds or data gathered by human resources on employee churn and exit interviews
- The controls mapping process should consider not only the existence of controls but their implementation and effectiveness. The strength of these mitigation measures will inform the residual risk

Reasonable Prevention Procedures Defence
Risk Assessments (7 of 7)

Mapping residual risk against risk tolerance

- The residual fraud risk must be considered and mapped against the company's risk tolerance. The outcome of the risk assessment should be used to identify and inform whether and how the company needs to strengthen its systems and controls
- The outcome of the risk assessment process should be documented under privilege. There should also be a clear record demonstrating that the outcomes of the risk assessment were carefully considered by relevant stakeholders and that any recommendations were actioned within a reasonable time
- Firms operating in the regulated sector have been criticised for conducting risk assessments which were then simply ignored or moth-balled. It is likely that a similar approach would be adopted by a prosecutorial body considering a reasonable prevention procedures defence
- In this regard the Home Office Guidance states that a risk assessment should be *"dynamic, documented and kept under regular review*

Reasonable Prevention Procedures Defence
Policies & Procedures (1 of 2)

Anti-fraud policy

- Should include a clear statement that the company prohibits fraud and easy-to-understand guidance on the firm's fraud prevention systems and controls, including penalties for breaching the policy
- Must not be a "cookie cutter" document and should instead reflect the company's corporate culture and values
- Should be communicated to all associated persons and incorporated into contracts with third parties, accompanied by relevant audit rights

Anti-fraud procedures

- A company's anti-fraud procedures should reflect and mitigate the risks identified by its risk assessment. Procedures should be clearly documented and frequently revisited to ensure they remain fit-for-purpose. Examples include:
  - Review and sign-off of POs, invoices and payments,
  - Audits of contractual documentation,
  - Whistleblowing systems, and
  - Reviews of technical systems
- Home Office Guidance states that procedures must be "*communicated, embedded and understood throughout the organisation, through external and internal communication*"

Reasonable Prevention Procedures

Top-level Commitment, Communication & Training

Top-level commitment

- A company's top-level commitment is frequently evidenced by a company-wide statement (such as a CEO's statement or note).
- It is unlikely that a prosecutorial body would be satisfied with this alone. A company should also ensure that anti-fraud systems and controls have been discussed and approved at a sufficiently senior level in the company (usually at the board level) and that there are appropriate lines of reporting in place.

Communication and training

- Appropriate training will usually entail new-joiner and cyclical training. A company should keep training logs and copies of training material (the latter is often overlooked when companies use external online providers).
- A company should also be able to demonstrate that their anti-fraud policy has been communicated to its associated persons and other relevant third parties.

Reasonable Prevention Procedures Defence
Policies & Procedures (2 of 2)

Due Diligence

- Most companies will already be undertaking due diligence on their associated persons. These processes may be ongoing or reflect the risks of specific clients or transactions
- The Home Office Guidance notes that existing due diligence procedures may need to be updated to reflect the specific risks of the failure to prevent fraud offence: *"[t]hose with exposure to the greatest risk may choose to clearly articulate their due diligence procedures specifically in relation to the corporate offence"*
- Examples of best practice include:
  - Use of technology, including screening tools and internet searches,
  - The inclusion and use of audit rights in contracts,
  - Review of new contracts and contract variations,
  - Increased monitoring of third-parties that are deemed to present a higher fraud risk, and
  - The use of appropriate due diligence should also be considered in the context of mergers and acquisitions

Reasonable Prevention Procedures Defence Monitoring & Review

Monitoring and review

Monitoring and review must be tailored to the level of risk identified in the fraud risk assessment. At the very basic level a prosecutorial body would be looking for evidence of:

- Detection of attempted fraud and investigation of suspected fraud,
- Fraud risk assessments being periodically refreshed,
- Testing and assessment of existing fraud mitigation measures,
- Audit rights in contracts being utilised if there is a suspicion of fraud,
- Ongoing review of relevant metrics, including whistleblower metrics,
- Regular updates to senior management on the implementation and success of anti-fraud measures,
- Anti-fraud measures being regularly discussed by the audit committee,
- Review of anti-fraud measures by internal audit, prioritising higher risk business unit, and
- In certain situations, an external anti-fraud audit may also be appropriate

FTPF and Reasonable Prevention Procedures Defence
Key Takeaways

Update existing fraud risk assessments and policies to cover FTPF

Fraud risk assessment methodology should be reasonable and documented

ECCTA is broader than the UKBA
A company may be liable for offences committed by a subsidiary
"Benefit" = intended benefit to company, its clients, a subsidiary or subsidiary's clients

Consider industry risk including business unit risk, process risk, third party/intermediary risk, transaction risk and geographical risk

Consider motive, means and opportunity

Demonstrate top-level commitment to anti-fraud measures

FTPF and Comparison with US Law (1 of 2)

There is no comparable failure to prevent fraud offence under US law, nor is there an affirmative defence to exculpate a corporation based on its reasonable prevention procedures

- As noted previously, U.S. *respondeat superior* doctrine broadly imposes corporate criminal liability for the acts of employees, agents, and other representatives

DOJ policy is to consider a company's control environment when deciding whether and in what form to pursue criminal charges, including the adequacy and effectiveness of the company's compliance program at the time of offence and at the time of the charging decision (DOJ, Principles of Federal Prosecution of Business Organizations, 9-28.200 [General Considerations of Corporate Liability])

These factors also may be relevant to mitigate the applicable fine at sentencing. The US Sentencing Guidelines as written (but rarely in application) allow for a reduction in sentence if a company (1) "*exercise*[s] *due diligence to prevent and detect criminal conduct*" and (2) "*otherwise promote*[s] *an organizational culture that encourages ethical conduct and a commitment to compliance with the law*" USSG §§ 8B2.1, 8C2.5(f)

FTPF and Comparison with US Law (2 of 2)

Factors the DOJ considers in evaluating a company's control environment for the purposes of charging and penalty decisions include (but are not limited to):

- Does the company conduct periodic risk assessments and update its compliance program accordingly?
- Is the company's commitment to full compliance with the relevant laws assessable and applicable to all employees through policies and procedures?
- Have employees been trained effectively?
- Is there a trusted mechanism by which employees can anonymously or confidentially report allegations of misconduct?
- Is there high-level commitment by company leadership to implement a culture of compliance?

DOJ Criminal Division, Evaluation of Corporate Compliance Programs, (September 2024)

These factors are not limited to fraud and apply broadly to compliance with laws generally

OTHER KEY PROVISIONS

5

Crypto Asset Regulation

Serious Fraud Office Pre-Investigation Powers

- The SFO has wide-ranging investigatory powers under section 2 Criminal Justice Act 1987 (CJA) which includes the ability to compel individuals and companies to provide information and documents
- Originally these powers could only be used once the SFO had commenced an investigation which made it difficult for the SFO to gather information
- In 2008 "*pre-investigation powers*" were introduced under section 2A CJA 1987 which allowed the SFO to use their investigatory powers before the SFO formally commenced an investigation for cases involving international bribery and corruption
- ECCTA has expanded the section 2A pre-investigation powers to all SFO cases
- This will make it easier for the SFO to gather information at an early stage and may result in more investigations being pursued.

Companies House

- Companies House is the official government register of companies and overseas entities in the UK. It is responsible for incorporating and dissolving limited companies and maintaining the public record of company information
- Broad powers of enforcement (e.g. over 150 offences in the Companies Act 2006), but historically low numbers of charges and low conviction rate
- ECCTA sets out a number of objectives for Companies House: currently hiring and planning to increase employee numbers to meet these objectives
- Companies House will be able to levy fines of up to £10,000 directly
- More significantly, Companies House will be able to share information with other agencies including police and law enforcement, NCA, FCA, HMRC and even overseas authorities
- ECCTA looking to make Companies House a more effective gatekeeper; how Companies House deploys its increased powers and resources in practice remains to be seen

Q&A

6

Upcoming Programs – Fall White Collar Webcast Series

Date and Time	Program	Registration Link
Tuesday, December 10, 2024 12:00 PM – 1:00 PM ET 9:00 AM – 10:00 AM PT	**Anti-Corruption Enforcement and Recent Developments in Latin America** Presenters: Michael Farhang, Patrick Stokes, Pedro Soto	Event Details
Thursday, December 12, 2024 12:00 PM – 1:00 PM ET 9:00 AM – 10:00 AM PT	**Gatekeeper Liability** Presenters: David Ware, Michael Scanlon, Nancy Hart	Event Details

Allan Neil

Partner / London

Telephone House, 2-4 Temple Avenue,
London EC4Y 0HB, UK

+44 20 7071 4296

aneil@gibsondunn.com

Allan Neil is an English qualified partner in the dispute resolution group of Gibson, Dunn & Crutcher's London office.

His recent work involves large-scale multi-jurisdictional disputes and investigations (both regulatory and internal investigations) in the financial institutions sector.

His work covers investment banking, asset management and compliance matters.

Allan Neil was called to the Bar by the Middle Temple in 2001, having been awarded the Queen Mother Scholarship in consecutive years, and named a Blackstone Entrance Exhibitioner.

Allan is recognised by *The Legal 500 UK* 2025 for Commercial Litigation, Banking Litigation: Investment and Retail and Regulatory investigations and corporate crime (advice to corporates), and has been awarded the Client Choice Award 2015 in recognition of his excellence in client service in the area of UK Litigation. He is also recognised in the 2016 *Legal Week* Rising Stars in Litigation list, which profiles the up-and-coming litigation stars at UK top 50 and top international firms in London.

He is fluent in French and German.

EDUCATION

University of Leicester
Postgrad Dip. European Law

University of Aberdeen
Doctor of Philosophy

City University London
Postgraduate Diploma in Law

University of Aberdeen
Master of Arts

John W.F. Chesley

Partner / Washington, D.C.

1700 M Street, N.W.,
Washington, D.C. 20036-4504

+1 202.887.3788

jchesley@gibsondunn.com

John Chesley is a litigation partner in Gibson Dunn's Washington, D.C. Office. He focuses his practice on white collar criminal enforcement and government-related litigation. He represents corporations, board committees, and executives in internal investigations and before government agencies in matters involving the Foreign Corrupt Practices Act, procurement fraud, environmental crimes, securities violations, sanctions enforcement, antitrust violations, and whistleblower claims. He also has significant trial experience before federal and state courts and administrative tribunals nationwide, with a particular focus on government contract disputes.

John served as the Interim Chief Ethics & Compliance Officer of a publicly-traded, multi-national corporation, responsible for managing a global team of compliance personnel. In this role, John conducted and oversaw internal investigations, managed a whistleblower hotline, provided compliance advice, created and updated compliance policies, and administered compliance training for tens of thousands of employees worldwide. This opportunity provided John with first-hand insights into the day-to-day challenges experienced by in-house counsel, which he uses to bring practical solutions to the table for all of his clients.

John has been recognized repeatedly as one of the leading lawyers of his generation. Specifically, he was named one of the "world's leading young investigations specialists" by *Global Investigations Review* "40 Under 40," as well as a "Rising Star" in the Government Contracts and White Collar fields by *Law360* and *The National Law Journal*, respectively. Most recently, John was recognized by Washington, D.C. *Super Lawyers* as a "Top Rated White Collar Attorney." He also has been recognized by *Benchmark Litigation* as a "Future Litigation Star" in Washington, D.C. (2020) and by *Who's Who Legal Investigations* guide as a "Future Leader" in Investigations (2022 - 2024).

EDUCATION

Georgetown University
Juris Doctor

University of Maryland
Bachelor of Arts

Christopher Loudon

Of Counsel / London

Telephone House, 2-4 Temple Avenue,
London EC4Y 0HB, UK

+44 20 7071 4249

cloudon@gibsondunn.com

Christopher Loudon is a Scottish qualified of counsel in the London office of Gibson, Dunn & Crutcher, and practises in the firm's Dispute Resolution Group. He has broad-based commercial litigation and multi-jurisdictional investigations experience, with a particular focus on the financial services sector.

Since joining Gibson, Dunn & Crutcher, Christopher has worked on disputes before the English, French, Swiss, German, Dutch, Italian, US, Australian, BVI and Cayman courts, and in particular on a large number of cases in Luxembourg, including commercial, administrative and criminal matters. He also has considerable investigations experience, both in private practice and while seconded to the in-house Legal function at UBS in London. Most recently, this has included working on two criminal investigations in different jurisdictions arising out of the largest Ponzi scheme ever uncovered, and a high profile cross-border tax investigation. While on secondment at UBS, he was responsible investigator for a multi-jurisdictional fraud investigation.

Christopher is recognised by The Legal 500 UK 2024 for Regulatory Investigations and Corporate Crime.

Prior to joining Gibson Dunn, Christopher trained in the Scottish offices of a leading international law firm and spent time seconded to the in-house Dispute Resolution group at one of the world's largest financial services groups.

Christopher has also worked at the European Parliament in Brussels and Strasbourg. He speaks fluent French.

EDUCATION

University of Glasgow
Diploma in Legal Practice

University of Glasgow
LL.B. (First Class Hons)

EDUCATION

College of Law - London
Bar Vocational Course

College of Law - London
Graduate Diploma in Law

University of Nottingham
Master of Laws (LL.M.)

University of Cambridge
Bachelor of Arts

Marija Bračković

Associate Attorney / London

Telephone House, 2-4 Temple Avenue,
London EC4Y 0HB, UK

+44 20 7071 4143

mbrackovic@gibsondunn.com

Marija Bračković is an associate in the London office of Gibson, Dunn & Crutcher. She is a member of the firm's Litigation, White Collar Defense and Investigations, Global Fintech and Digital Assets and Privacy, Cybersecurity and Data Innovation Practice Groups.

Marija has substantial experience in both domestic and international dispute resolution, including litigation and investigations, and regulatory compliance and counselling across sectors, with a focus on fintech and emerging digital regulations. Her practice has an emphasis on high-profile and politically sensitive matters, such as cases relating to bribery, money laundering and allegations of cross-border and international crimes. Marija regularly advises on complex regulatory and compliance issues, including the scope and implementation of the emerging digital regulatory regime across the UK and EU, including the Digital Services Act, Online Safety Act and EU AI Act.

Marija has acted in matters in the UK, Bangladesh, Sri Lanka, Sierra Leone, Iraq and Cambodia, representing diverse clients including governments, political parties, non-governmental organizations and private individuals. She has particular experience in acting for major technology companies, banks, crypto firms and financial institutions.

Marija is recognised by *The Legal 500 UK* 2024 for Regulatory Investigations and Corporate Crime. She has also been recognised by the 2024 edition of *Best Lawyers* in the United Kingdom as "One to Watch" for International Arbitration and Litigation.

Prior to joining Gibson Dunn, Marija was an associate in the Litigation and Dispute Resolution team of another international law firm. She previously practiced at a leading set of barristers' chambers in London and completed secondments at the Serious Fraud Office and a major retail bank. Called to the bar in 2010, Marija is an experienced advocate and has appeared in all manner of proceedings, including jury trials, court martial and tribunal hearings, as both a sole and junior advocate.

Amy Cooke

Associate Attorney / London

Telephone House, 2-4 Temple Avenue,
London EC4Y 0HB, UK

+44 20 7071 4041

acooke@gibsondunn.com

Amy Cooke is an English qualified barrister and associate in the London office of Gibson, Dunn & Crutcher.

She practices in the firm's Dispute Resolution Group and specializes in white collar investigations. Her recent work includes large-scale multi-jurisdictional disputes and investigations in the financial services sector.

Amy is recognised by *The Legal 500 UK* 2024 for Regulatory Investigations and Corporate Crime.

Prior to joining Gibson Dunn, Amy was a lawyer at the Serious Fraud Office where she gained extensive experience of complex fraud and bribery investigations and prosecutions involving both corporate entities and high net worth individuals. She also dealt with a number of confiscation and restraint matters.

Amy also has a wide range of advocacy experience from her time at the independent bar, during which she handled a variety of criminal and civil cases.

EDUCATION

College of Law
Bar Vocational Course

College of Law
Graduate Diploma in Law

University of Birmingham
Bachelor of Arts

Appendices

7

Appendix A ECCTA Schedule 12 (1 of 2)

Common law offences

- Cheating the public revenue.
- Conspiracy to defraud.
- In Scotland, the following offences at common law—
  - fraud;
  - uttering;
  - embezzlement; and
  - theft.

Statutory offences

- An offence under any of the following provisions of the Theft Act 1968—
  - section 1 (theft);
  - section 17 (false accounting);
  - section 19 (false statements by company directors, etc.);
  - section 20 (suppression, etc., of documents); and
  - section 24A (dishonestly retaining a wrongful credit).
- An offence under any of the following provisions of the Theft Act (Northern Ireland) 1969—
  - section 1 (theft);
  - section 17 (false accounting);
  - section 18 (false statements by company directors, etc.);
  - section 19 (suppression, etc., of documents); and
  - section 23A (dishonestly retaining a wrongful credit).
- An offence under any of the following provisions of the Customs and Excise Management Act 1979—
  - section 68 (offences in relation to exportation of prohibited or restricted goods);
  - section 167 (untrue declarations, etc.); and
  - section 170 (fraudulent evasion of duty).
- An offence under the Forgery and Counterfeiting Act 1981 (forgery, counterfeiting and kindred offences).
- An offence under section 72 of the Value Added Tax Act 1994 (fraudulent evasion of VAT).
- An offence under section 46A of the Criminal Law (Consolidation) (Scotland) Act 1995 (false monetary instruments).
- An offence under any of the following sections of the Financial Services and Markets Act 2000—
  - section 23 (contravention of prohibition on carrying on regulated activity unless authorised or exempt);
  - section 25 (contravention of restrictions on financial promotion);
  - section 85 (prohibition on dealing, etc., in transferable securities without approved prospectus); and
  - section 398 (misleading the FCA or PRA).
- An offence under any of the following sections of the Terrorism Act 2000—
  - section 15 (fund-raising);
  - section 16 (use and possession);
  - section 17 (funding arrangements);
  - section 18 (money laundering); and
  - section 63 (terrorist finance: jurisdiction).

Appendix A ECCTA Schedule 12 (2 of 2)

- An offence under any of the following sections of the Proceeds of Crime Act 2002—
  - section 327 (concealing, etc., criminal property);
  - section 328 (arrangements facilitating acquisition, etc., of criminal property);
  - section 329 (acquisition, use and possession of criminal property);
  - section 330 (failing to disclose knowledge or suspicion of money laundering); and
  - section 333A (tipping off: regulated sector).
- An offence under section 993 of the Companies Act 2006 (fraudulent trading).
- An offence under any of the following sections of the Fraud Act 2006—
  - section 1 (fraud);
  - section 6 (possession, etc., of articles for use in frauds);
  - section 7 (making or supplying articles for use in frauds);
  - section 9 (participating in fraudulent business carried on by sole trader); and
  - section 11 (obtaining services dishonestly).
- An offence under any of the following sections of the Bribery Act 2010—
  - section 1 (bribing another person);
  - section 2 (being bribed); and
  - section 6 (bribery of foreign public officials).
- An offence under section 49 of the Criminal Justice and Licensing (Scotland) Act 2010 (possessing, making or supplying articles for use in frauds).
- An offence under any of the following sections of the Financial Services Act 2012—
  - section 89 (misleading statements);
  - section 90 (misleading impressions); and
  - section 91 (misleading statements, etc., in relation to benchmarks).
- An offence under regulation 86 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.
- An offence under regulations made under section 49 of the Sanctions and Anti-Money Laundering Act 2018 (money laundering and terrorist financing, etc.).
- An offence under an instrument made under section 2(2) of the European Communities Act 1972 for the purpose of implementing, or otherwise in relation to, EU obligations created or arising by or under an EU financial sanctions Regulation.
  - An offence under an Act or under subordinate legislation where the offence was created for the purpose of implementing a UN financial sanctions Resolution.
  - An offence under paragraph 7 of Schedule 3 to the Anti-terrorism, Crime and Security Act 2001 (freezing orders).
  - An offence under paragraph 30 or 30A of Schedule 7 to the Counter-Terrorism Act 2008 where the offence relates to a requirement of the kind mentioned in paragraph 13 of that Schedule.
  - An offence under paragraph 31 of Schedule 7 to the Counter-Terrorism Act 2008.
  - An offence under regulations made under section 1 of the Sanctions and Anti-Money Laundering Act 2018 (sanctions regulations).
  - In this paragraph—
  - “EU financial sanctions Regulation” and “UN financial sanctions Resolution” have the same meanings as in Part 8 of the Policing and Crime Act 2017 (see section 143 of that Act); and
  - “subordinate legislation” has the same meaning as in the Interpretation Act 1978.

Appendix B
ECCTA
Schedule 13

Common law offences

- Cheating the public revenue.
- In Scotland, the following offences at common law—
  - fraud;
  - uttering; and
  - embezzlement.

Statutory offences

- An offence under any of the following provisions of the Theft Act 1968—
  - section 17 (false accounting); and
  - section 19 (false statements by company directors, etc.).
- An offence under any of the following provisions of the Theft Act (Northern Ireland) 1969—
  - section 17 (false accounting); and
  - section 18 (false statements by company directors, etc.).
- An offence under section 993 of the Companies Act 2006 (fraudulent trading).
- An offence under any of the following provisions of the Fraud Act 2006—
  - section 1 (fraud);
  - section 9 (participating in fraudulent business carried on by sole trader); and
  - section 11 (obtaining services dishonestly).

GIBSON DUNN