The UK Bribery Act and the Economic Crime and Corporate Transparency Act (ECCTA)

What is the Bribery Act?

The Bribery Act 2010 establishes the following general bribery offenses:

- Makes it illegal to offer, promise, or give a "financial or other advantage" to another person that's intended to induce or reward the person to perform a relevant function or activity (section 1).
- Makes it illegal to request, agree to receive, or accept a "financial or other advantage" in exchange for the performance of a relevant function or activity (section 2);
- Makes it illegal to bribe a foreign public official "to obtain or retain business, or an advantage in the conduct of business" (section 6).

The Bribery Act does not exempt facilitation payments, which the Ministry of Justice defines in "The Bribery Act guidance" as "small bribes paid to facilitate routine government action."

Hospitality, promotional, or other business expenditures that aren't "reasonable and proportionate" may also be considered bribes. The Ministry of Justice cites examples of potential scenarios in the Bribery Act guidance.

Whether prosecutors can make a case for bribery pertaining to hospitality, promotional, or other business expenditures will depend on the "totality of the evidence," weighing such factors as "the type and level of advantage offered, the manner and form in which the advantage is provided, and the level of influence the particular foreign public official has over awarding the business," the guidance states.

The Bribery Act does not address non-bribery offenses, such as fraud, theft, books-and-record offenses, Companies Act offenses, money-laundering offenses, or offenses relating to competition law.

What is the scope of the Bribery Act?

The Bribery Act applies to individuals and relevant commercial organizations. It covers acts of bribery in both the private and public sectors.

The Bribery Act applies to any bribery offense committed in whole or in part in the UK: England, Wales, Scotland, or Northern Ireland. According to the Bribery Act guidance, as long as the organization is incorporated or formed in the UK, or "carries on a business or part of a business" in the UK (no matter where in the world it is incorporated or formed), UK courts have jurisdiction. This gives the Bribery Act extra-territorial reach.

The extra-territorial reach of the Bribery Act applies to bribery offenses that take place outside the UK if the person who committed the offense has a "close connection with the UK," meaning that the person, at the time of the offense, was a British citizen; a British national (overseas); an individual ordinarily resident in the UK; a body incorporated under the law or any part of the UK; or a Scottish partnership.

What is the ECCTA?

While the Bribery Act covers only bribery offenses, the Economic Crime and Corporate Transparency Act (ECCTA) is designed to strengthen the UK government's fight against economic crime more broadly. The ECCTA further introduces provisions designed to improve information-sharing between certain businesses for the purposes of preventing, detecting, and investigating economic crime.

What are economic crimes under the ECCTA?

Schedule 12 of the ECCTA establishes criminal liability for a wide range of "relevant offenses" as they are defined in a wide range of laws, including the Bribery Act, the Financial Services and Markets Act (FISMA), the Fraud Act, the Proceeds of Crime Act (POCA) 2002, the Terrorism Act 2000, the Customs and Excise Management Act 1979, the Theft Act 1968, and others.

Examples of "relevant offenses" under the ECCTA could include fraud, embezzlement, false accounting, false statements by company directors, false customs declarations, offenses relating to the exportation of prohibited or restricted goods, and many more.

What is the scope of the ECCTA?

For an organization to be held liable under the ECCTA, at least part of the underlying fraud offense must have taken place in the UK, or the gain or loss occurred in the UK. "Where no act or omission forming part of the relevant offense took place in the UK, the organization is not guilty of an offense… unless it would be guilty of the relevant offense had it carried out the acts that constituted that offense (in the location where the acts took place)," the ECCTA states.

However, if a UK-based employee or senior manager commits a fraud offense, the organization will be liable, no matter where it is incorporated.

Failure to prevent offense under the Bribery Act and ECCTA

Among the most significant provisions shared by the Bribery Act and the ECCTA is the "failure to prevent" offense. This provision broadly establishes that organizations can be held criminally liable for failure to prevent offenses committed by persons "associated" with the organization.

However, the "failure to prevent bribery" offense under the Bribery Act and "failure to prevent fraud" offense under the ECCTA diverge in a few significant ways that require a closer review. Most significant is the ECCTA's introduction of a new "senior manager's regime" under the scope of the "failure to prevent fraud" offense that is the real gamechanger for organizations with a UK presence.

Failure to prevent bribery offense

Under the Bribery Act, a commercial organization is liable if a person "associated" with it bribes another person with the intent to obtain or retain business or an advantage in the conduct of business for the organization. An associated person could include employees, agents, subsidiaries, contractors, or suppliers.

Senior manager's regime

Under the ECCTA, "if a senior manager of a body corporate or partnership … acting within the actual or apparent scope of their authority commits a relevant offense … the organization is also guilty of the offense."

The ECCTA defines "senior manager" as an individual who plays a "significant" role in the decision-making about the "whole or a substantial part" of the corporate body or partnership's activities to be "managed or organized;" or the actual managing or organizing of the whole or a substantial part of those activities. A broad range of individuals potentially could satisfy this definition, such as the head of a business unit, or an individual who oversees a team or parts of the business, for example.

Failure to prevent fraud offense

Effective from September 1, 2025, the ECCTA introduces a new "failure to prevent fraud" offense, in which large organizations, or an entity whose parent is a large organization, will be guilty of fraud offenses committed by an "associated" person with the intent of benefitting the organization; and where the organization does not have "reasonable" fraud prevention procedures in place. Associated persons could include employees, agents, or others who provide services on behalf of the organization.

The ECCTA's "failure to prevent fraud" offense is significant for large UK organizations because it dramatically increases their risk of liability. Before the ECCTA, UK common law abided by the "identification principle," a legal test used for attributing criminal liability to an organization through the acts of their employees. The identification principle, established in the 1971 case *Tesco Supermarkets v. Nattrass*, held that a company can only be held criminally liable where prosecutors can prove that a natural person acting as the "directing mind or will" of the company committed the offense. Historically, this has been a very difficult test for prosecutors to satisfy.

Who needs to care?

The "failure to prevent fraud" offense applies to all large incorporated bodies, subsidiaries, and partnerships across all sectors. This includes large, incorporated not-for-profit organizations, such as charities, and incorporated public bodies.

Only large organizations are in the ECCTA's scope, as defined by the Companies Act 2006. Thus, organizations that meet two out of the following three criteria are in scope of the size threshold:

- Organizations with more than 250 employees
- More than £36 million in turnover
- More with than £18 million in total assets

Where a parent company and its subsidiaries cumulatively meet the size threshold, that group of companies is in scope of the failure to prevent fraud offense. Liability will be attached to whichever entity within the group was directly responsible for failing to prevent the fraud.

Liability may also be attached to a parent where a subsidiary employee commits a fraud offense for the benefit of the parent company, and "reasonable" fraud prevention procedures were not in place.

Enforcement and penalties

Enforcement and penalties for bribery offenses under the Bribery Act or fraud offenses under the ECCTA are significant.

Bribery Act fines and penalties

Under the Bribery Act, individuals could face a maximum penalty of up to 10 years in prison, an unlimited fine, or both. Organizations could also face an unlimited fine.

The Ministry of Justice clarifies in a Bribery Act "Quick Start Guide" that, to be prosecuted in England and Wales under the Bribery Act, either the Director of Public Prosecutions or the Director of the Serious Fraud Office must be satisfied that a conviction is "more likely than not" and is "in the public interest."

ECCTA fines and penalties

A failure to prevent fraud offense under the ECCTA similarly carries an "unlimited fine" for organizations where the organization cannot show that it took reasonable steps to prevent fraud.

Guidance issued in November 2024 by the Home Office provides further clarity. That guidance states that, to be held criminally liable, there does not need to be a showing that senior managers "ordered or knew about the fraud."

Six core compliance principles

Both the Bribery Act and the ECCTA establish a defense for organizations to avoid liability where it can show that it had compliance procedures in place that were designed to prevent associated persons from committing a bribery or fraud offense.

The Bribery Act refers to these principles as the "adequate procedures" defense as it concerns a failure to prevent bribery offense, while the ECCTA refers to this as the "reasonable procedures" defense as it concerns a failure to prevent fraud offense.

Both the "adequate procedures" defense and the "reasonable procedures" defense are built upon six core compliance principles that companies of all sizes and across all sectors should have in place for preventing bribery and fraud offenses. They are referred to as principles because they are not meant to be prescriptive.

Guidance provided by the Ministry of Justice describes several case studies based on hypothetical scenarios that are designed to illustrate the application of the following six compliance principles for small, medium and large organizations.

Top-level commitment

Both the Bribery Act and the ECCTA stress the importance of top-level commitment. Whether messaging comes from the board of directors, senior management, or both, what's important is that a culture of compliance trickles down from those responsible for the governance of the organization.

Guidance documents that have been issued by the UK government on the Bribery Act and the ECCTA offer a list of measures senior management can take to demonstrate their commitment to a culture of compliance, including:

- Communicating and endorsing the organization's stance on preventing fraud, including mission statements
- Setting bribery prevention policies, or delegating the task to the chief ethics and compliance officer, or equivalent role
- Tasking management to design, operate and monitor bribery prevention procedures, and keeping these policies and procedures under regular review
- Committing to anti-corruption training and resourcing
- Leading by example, fostering a culture where staff are empowered to speak up

Risk assessments

The Bribery Act and ECCTA encourage organizations to assess the nature and extent of their risk exposure. UK organizations operating overseas, for example, should consider such factors as the risk of bribery or fraud posed by the countries they operate in; the sector they are operating in; and the monetary value of the project. Other considerations include risks posed by certain employees, agents and other associated persons.

Risk assessments should evolve as the organization's risks evolve. They should also be documented and regularly reviewed.

ECCTA guidance issued by the Home Office suggests that companies develop risk typologies by considering the following three elements of the "fraud triangle":

- **Opportunity:** Companies should consider where there may be opportunities to commit fraud, such as departments or individuals with weak controls or inadequate oversight. Potential weak spots may include finance, procurement, investor sales, or marketing.
- **Motive:** Financial targets or other operating pressures may cause motivations to commit fraud. Thus, companies may wish to consider whether the company's reward and recognition system, including commissions or bonuses, incentivizes fraud, or whether the culture disincentivizes whistleblowing.
- **Rationalization:** The guidance suggests that companies consider whether the culture is "quietly tolerant of fraud," particularly if it's to secure a contract for the company; whether fraud is prevalent in that particular industry; or whether staff face adverse consequences for reporting concerns.

The Home Office guidance additionally lists several questions to consider for each element of the fraud triangle, which UK organizations may want to refer to as they are reevaluating their compliance programs.

Proportionate risk-based prevention procedures

A key principle of a fraud prevention plan is that prevention procedures be proportionate to the risks identified in the risk assessment, as well as to the "nature, scale, and complexity of the organization's activities," according to the Home Office's ECCTA guidance. Fraud prevention procedures also should be "clear, practical, accessible, effectively implemented and enforced," the guidance states.

The guidance offers several risk factors in the form of questions for organizations to consider for mitigating opportunities and motives for fraud risk, as well as proper consequences to consider when fraud is committed.

Due diligence

Due diligence procedures should be proportionate to risks identified by a risk assessment. Examples of best practices could include:

- Utilizing technology, such as third-party risk management tools, screening tools, online searches, checking trading history or professional or regulated status, if relevant, or vetting checks if appropriate
- Reviewing vendor contracts, requiring compliance, and the ability to terminate contracts in the event of a breach, where appropriate
- Identifying and monitoring staff and agents who pose a high fraud risk because of stress, targets or workload

The Home Office recommends in the ECCTA guidance that organizations conduct due diligence during mergers and acquisitions as well. Examples of best practices during an M&A transaction include assessing relevant criminal or regulatory charges, tax documentation, the firm's risk exposure, and fraud detection and prevention measures.

Communication and training

Organizations should ensure fraud prevention policies and procedures are communicated, embedded, and understood throughout the organization. Such messaging should further be integrated into existing policies and procedures.

"For instance, policies related to sales targets or customer interactions could include a brief statement addressing fraud rationalization and the potential consequences of committing fraud," ECCTA guidance states. Organizations may also choose to publicize investigation outcomes, such as sanctions imposed, the guidance suggests.

Additional examples of what may be addressed in a policy are covered in the Bribery Act guidance. Examples include "hospitality and promotional expenditures, facilitation payments, training, charitable and political donations and penalties for breach of rules, and the articulation of management roles at different levels."

A "secure, confidential, and accessible" reporting mechanism is another essential component of a robust internal communication strategy, especially within organizations with operations abroad, according to the Bribery Act guidance. For example, a hotline or online reporting tool serves as a means for internal or external parties to raise concerns about potential bribery or fraud, to offer suggestions on how to improve prevention procedures, and for requesting advice about specific concerns.

Training is a key part of communication and should cover, for example, the nature of offenses and the procedures for addressing them. "Some relevant bodies may wish to incorporate training into their existing financial crime prevention training, while other organizations may wish to introduce bespoke training to address specific fraud risks," the ECCTA guidance states. It further recommends that training cover whistleblower processes, and that managers be trained on how to respond when whistleblower reports are made.

Monitoring and review

Organizations should continuously monitor for the detection of fraud or attempted fraud. As cited in the ECCTA guidance, practical measures for monitoring fraud could include the following:

- Monitoring financial controls
- collecting data on how many staff have attended fraud prevention training courses and any test results, if applicable
- Monitoring updates to due diligence procedures, or contractual clauses for associated persons

The ECCTA guidance additionally provides several questions organizations should consider when looking for fraud, or when investigating suspected fraud.

When reviewing fraud detection and prevention procedures, some recommended measures include:

- Seeking internal feedback from staff members
- Reviewing fraud detection analyses
- Examining relevant settlement agreements, and subsequent actions taken
- Examining other financial crime prevention procedures
- Conducting formalized periodic reviews with documented findings
- Following advice from subject-matter experts, including legal counsel

The review process should adapt to new and rising developments. "For example, an organization may need to take a more formalized and detailed approach to reviewing its fraud detection and prevention procedures following criminal activity by persons associated with it," the guidance states.

New information-sharing provisions under ECCTA

One provision unique to the ECCTA is its voluntary information-sharing provisions, which came into force on January 15, 2024. This provision allows anti-money-laundering (AML)-regulated businesses under Schedule 9 of the Proceeds of Crime Act 2002 (POCA) to share customer information with each other. The UK government says the intent is to make it easier to prevent, detect, and investigate economic crime.

The ECCTA also allows for the indirect sharing of customer information through third-party intermediaries between businesses in the financial sector (deposit-taking bodies, electronic money institutions, and payment institutions); crypto-asset exchanges and custodian wallet providers; and "large" or "very large" law firms, accountancy firms, insolvency practitioners, auditors, and tax advisers. What constitutes a "large" or "very large" firm is defined under Section 55 of the Finance Act 2002.

A hypothetical example for sharing customer information could apply in a situation where a bank terminates a relationship with a customer who has engaged in an economic crime, as it is defined in the ECCTA, and wants to alert other account providers about this customer.

Companies House transition plan

Another notable aspect of the ECCTA for UK organizations is that it authorizes Companies House to play a greater role in tackling economic crime. In a policy paper, Companies House says the ECCTA "introduces the biggest changes to Companies House since corporate registrations were established in 1844."

Approximately 50 statutory instruments will be introduced in phases over the coming months and years, with the aim of completing them all by the end of 2027. The UK government says the intent is "improved transparency and more accurate and trusted information" on Companies House registers.

Three UK Registrars of Companies

The UK has three registrars of companies:

- The Registrar of Companies for England and Wales, based at Companies House, Cardiff, is responsible for the registration of companies in England and Wales.
- The Registrar of Companies for Scotland, based at Companies House, Edinburgh, is responsible for the registration of companies in Scotland.
- The Registrar of Companies for Northern Ireland, based at Companies House, Belfast, is responsible for the registration of companies in Northern Ireland.

Four core objectives

In its policy paper, the Companies House describes four core objectives underpinning the new framework for the three registrars:

- **Objective 1:** To ensure any person who is required to deliver a document to the registrar does so (and that the requirements for proper delivery are complied with)
- **Objective 2:** To ensure information contained in the register is accurate and that the register contains everything it ought to contain. This reference to 'the register' includes any records kept by the registrar under any enactment
- **Objective 3:** To ensure records kept by the registrar do not create a false or misleading impression to members of the public
- **Objective 4:** To prevent companies and others from carrying out unlawful activities, or facilitating the carrying out by others of unlawful activities

Implementation plans

Companies House says it has improved the quality of information on the register since March 2024 through the following key measures:

- Querying and rejecting new information received in customer filings suspected to be "wrong or fraudulent"
- Removing "inaccurate" information, including citizens' names and addresses used without consent
- Querying and rejecting company names that "mislead customers, facilitate fraud, or give the false impression that the company is connected to a foreign government"
- Improving the accuracy and reliability of registered office addresses by introducing a new definition for "appropriate address" (i.e., not using a Royal Mail PO Box or equivalent service offered by other parties)

Companies House says it also has improved information-sharing with law enforcement agencies and regulatory bodies in a greater effort to tackle economic crime. It also has undertaken greater analysis of the information it holds, including comparing data sets against the data it obtains externally.

According to its policy paper, the Companies House has been able to better prevent disqualified directors from acting by rejecting documents notifying appointments of new directors to existing companies when these individuals are disqualified directors.

Identity verification

The UK government highlights identity verification as a major component of the reforms that will be taking place. As of February 25, 2025, certain service providers, including accountants and solicitors, will be allowed to register to become an Authorized Corporate Service Provider (ACSP), who will then be allowed to carry out verification services for their clients and provide these details to the registrars.

By autumn 2025, identity verification will be required for all directors and "persons with significant control" (PSCs) for new incorporations. Existing companies will have a 12-month transition period to provide identity verification credentials for their directors and PSCs when their confirmation statement is due.

Reforms to make the information of limited liability partnerships "more accessible and transparent" will occur "no sooner than spring 2026." As a final reform, "following an extensive formal notice period," the Companies House will mandate software-only filing for all accounts.

Companies House guidance

On February 19, 2025, the Companies House published guidance on how ACSPs can meet the identity verification standard for verifying identities, such as:

- Asking for information on persons (e.g., full name and any former names, date of birth, home address, address history for the last 12 months, and email address)
- Obtaining identity verification documents
- Checking the authenticity of the identity verification documents
- Ensuring persons are trained by a specialist training provider in detecting false documents if the identity verification documents are being checked manually

Additional guidance published by the Companies House includes how to register as a Companies House authorized agent; and the role and responsibilities of being an authorized agent.