

Technical factsheet

The Economic Crime and Corporate Transparency Act 2023

Contents

	Page
Introduction	2
Companies House reforms	2
New identity procedures	3
Corporate directors	4
Failure to prevent fraud	4
Cryptoassets	6
Anti-money laundering powers	6
Filing requirements	7
Register of Overseas Entities	7
Other notable changes	8
Conclusion	10

This factsheet has been produced in partnership with Steve Collings FCCA, director of Leavitt Walmsley Associates Ltd Chartered Certified Accountants, lecturer and author of financial reporting publications. You can find the latest publications at stevecollings.co.uk.

Introduction

On 26 October 2023, the Economic Crime and Corporate Transparency Act 2023 received Royal Assent and became law. The act introduces several wide-ranging reforms with the objective of tackling economic crime and improving transparency over corporate entities. However, it should be emphasised that at the time of preparing this factsheet, secondary legislation was needed to implement many of the measures contained in the act, and the timing of this secondary legislation is unclear. Changes to computer systems at Companies House will also be needed to implement some of the measures contained in the act.

The act builds on the Economic Crime (Transparency and Enforcement) Act 2022, which was introduced in light of Russia's invasion of Ukraine. The 2022 act:

- allowed the government to move faster when imposing sanctions
- created a Register of Overseas Entities (see below) to target foreign criminals using UK property to launder money
- reformed the UK's unexplained wealth order regime.

Together, these acts provide additional powers to tackle money laundering and other unorthodox behaviour. The long-awaited Companies House reforms also form part of the act.

As a high-level overview, the new measures include:

- reforms that prevent the abuse of limited partnerships
- new powers to enable the seizure and recovery of suspected cryptoassets
- reforms to provide businesses with more confidence to share information and tackle economic crime
- a new 'Failure to Prevent Fraud' offence (although this will only apply to large corporates)
- new identity verification for registered company directors, persons with significant control (PSCs) and those who file on behalf of companies
- improvements to the information filed on the public record (ie financial information) so that it is more accurate
- providing the registrar with more effective investigation and enforcement powers
- introducing better cross-checking of data with other governmental bodies
- enhancing the protection of personal information, which is sent to Companies House
- new filing requirements for small companies

Companies House reforms

It is not uncommon to see concerns over the integrity of the information placed on the public record. Over the years, there have been many sets of accounts filed that are clearly incorrect and do not comply with accounting standards or company law requirements. Fictitious names of directors have also been used inappropriately.

The act reforms the role of Companies House, with the aim of improving transparency over UK companies and other legal entities to strengthen the business environment, in addition to national security, and to enable economic crime to be tackled. The benefit of this is that the register will be more reliable.

The reforms to Companies House include the following:

- introducing a more rigorous identification regime for all new and existing registered company directors, PSCs and those delivering documents to Companies House (see below)
- broadening the power of the registrar such that they become a more active 'gatekeeper' over company creation and a custodian of reliable data, including new powers to check, remove or decline information submitted to, or already on, the register
- improving the financial information on the companies register so that it is more reliable, complete and accurate. In addition, it will also reflect the latest advancements in digital technology to help users' decision-making processes
- providing Companies House with more effective investigation and enforcement powers, as well as introducing better cross-checking of data with other public and private sector bodies. It should be noted that the act enables Companies House to proactively share information with law-enforcement bodies where they have evidence of anomalous filings or suspicious behaviour
- enhancing the protection of personal information provided to Companies House to protect individuals from fraud and other harm
- wider reforms to clamp down on the misuse of corporate entities.

New identity procedures

The act brings in new identity (ID) procedures for individuals, with the aim of improving information held at Companies House. This will apply to all new and existing directors registered at Companies House, PSC and those who are delivering documents to Companies House. Existing companies will have a transitional period in which to verify these identities.

The verification procedures will be carried out either by Companies House itself (using electronic ID checks) or by an authorised company service provider (eg an accountancy firm using normal anti-money laundering regulations protocol).

Again, secondary legislation will need to be published by the government and an update of the systems at Companies House to enable relevant ID checks to be carried out.

It should be noted that invalid registered office addresses, such as those used fraudulently to create companies, will be removed.

If a person is verifying their identity directly with Companies House, identity verification will link a person with a primary identity document (such as a passport or driving licence). The person undergoing the verification will need to take a photograph or scan their face and the identity document. The two will then be compared, using likeness-matching technology, and the identity will be verified.

For directors of new companies, identity verification must take place before an application for the formation of a company is delivered to the registrar. Post-incorporation, a new director must verify their identity as soon as possible and must do so before their appointment is notified to the registrar (ie within 14 days).

In general, it is expected that identity verification will be a one-off requirement. Once a person is verified, they will obtain a verified status. However, there may be instances where re-verification is

required (eg if a person changes their name). The events that will trigger the requirement to re-verify will be outlined in secondary legislation.

The act provides that an individual will not be able to act as a director unless they have verified their identity. Consequently, until they verify their identity, they should not take any actions on behalf of the company in their capacity as a director. If they fail to verify their identity and continue to act as a director, they will be committing a criminal offence, which is punishable by a fine.

It will also be a new offence for an individual to act as a director unless the company has notified the registrar of the director's appointment within 14 days of their appointment. The notice **must** include a statement that the director's identity has been verified. This is to ensure that all directors are included on the companies' register.

Corporate directors

The act does not make provisions in respect of corporate directors, but the government has issued a factsheet that confirms that it has the powers to restrict the use of corporate directors, and that these powers will be brought into force in parallel with the act. The 'principles-based' exception proposals, which the government consulted on in December 2020, will form the basis of these regulations.

Consequently, only corporate entities with 'legal personality' will be properly appointable as corporate directors. The directors of the corporate entity must be natural persons and must (prior to the corporate director appointment) have been subject to an appropriate identity process. In addition, only UK-registered corporate entities will be permitted.

Existing companies with corporate directors will be given 12 months to comply and, within that time, they must either ensure that their corporate director is compliant with the conditions set out in the act or resign them. New companies, or existing companies appointing a corporate director for the first time, will need to ensure that they satisfy the conditions from the date the measures come into effect.

Failure to prevent fraud

The act introduces a new offence of failure to prevent fraud. This will hold an organisation to account if they profit from fraud committed by their employees.

Potentially, this new offence is very unusual and very significant because it is a strict liability criminal offence. It essentially builds on the existing offence of failure to prevent bribery under the Bribery Act 2010 and a failure to prevent the facilitation of tax evasion under the Criminal Finances Act 2017. Secondary legislation will be needed where this new offence is concerned; in particular, guidance is awaited on the 'reasonable procedures' defence.

As noted earlier, this offence applies only to larger companies and partnerships that meet at least two of the following criteria in the financial year preceding the year of the fraud offence:

- more than 250 employees
- more than £36m turnover
- more than £18m in total assets on the balance sheet.

An organisation that is the parent undertaking of a group will also be within scope of the offence when it meets at least two out of the following criteria in the financial year preceding the year of the fraud offence:

- an aggregate turnover of over £36m net (or £43.2m gross)
- total assets over £18m net (or £21.6m gross)
- more than 250 aggregate employees.

Under the act, such an organisation will be liable if it fails to prevent a specified fraud where:

- an 'associated person'¹ of the organisation commits the fraud
- the fraud is intended to benefit the organisation or a person to whom services are provided on behalf of the organisation.

An important point to emphasise is that it is not confined to just the UK. If an associated person commits fraud under UK law (or targets UK victims), the organisation can be prosecuted even when the organisation and associated person are based overseas.

Schedule 13 contains specific fraud offences, including:

- fraud by false representation
- fraud by abuse of position
- fraud by failing to disclose information.

Secondary legislation can be passed by the government, which can add or remove offences from Schedule 13.

An organisation will have a defence where it can show that it had either 'reasonable procedures' in place to prevent the fraud; or that it was not reasonable for the organisation not to have such procedures in place. As noted above, the government will need to publish guidance on what it considers to be 'reasonable procedures' in this regard; this is expected to be published in early 2024.

There is also an update to the legal principle known as the 'identification doctrine', which will ensure businesses can be held criminally liable for the actions of senior managers who commit economic crimes.

The courts have often found it challenging to bring criminal charges to corporate entities due to the 'directing-mind-and-will' test. Under this test, a company could only be held criminally liable if the offence could be traced to a natural person who could be said to represent its 'directing mind and will' at the time the offence was committed. This represented a very narrow group of individuals, and the threshold was very high. This test has also been the subject of criticism by various authorities, which stated that it was outdated and no longer fit for purpose.

¹ An 'associated person' is defined as an employee, agent or subsidiary of the organisation (as well as any others who perform services for or on its behalf). This is broader than the definition in the Bribery Act 2010, which includes a rebuttable presumption that an employee is an associated person, but in relation to agents and subsidiaries applies a test to determine if the associated person performs services for, or on behalf of, the organisation in the circumstances.

The act replaces the 'directing-mind-and-will' test with a new 'senior manager' test, which has been taken from the Corporate Manslaughter and Corporate Homicide Act 2007. The impact of this is that the new test significantly expands the group of individuals through which liability can be attributed, and hence makes it easier for prosecutors to pursue guilty corporate entities.

A 'senior manager' is an individual who plays a significant role in either managing the company's activities or making decisions about how these are to be managed. A 'relevant offence' covers a broad range of offences, including the substantive money-laundering offences and the ancillary money laundering-related offences of 'failing to disclose' and 'tipping off', fraud, false accounting, tax evasion, bribery and breaches of sanctions regulations.

Organisations caught under the scope of this new offence will need to carry out a risk assessment to re-examine their fraud detection and prevention procedures. It should also be noted that while the new act does not impose additional burdens on senior managers, they will come under greater scrutiny.

This part of the act applies only to large entities, but smaller organisation that fall outside the scope of the Failure to Prevent offence (in particular those that act as counterparties to large organisations) should carefully consider whether they need to revise their policies and procedures in a similar manner.

Cryptoassets

Fraud where cryptoassets is concerned has become more common over the past couple of years. Indeed, some individuals have lost thousands of pounds of their own savings when investing in cryptoassets, only to find that they are one of several people who have also lost money. Indeed, the National Crime Agency's National Assessment Centre estimates that over £1bn of illicit cash was transferred overseas using cryptoassets in 2021.

The act provides additional powers to law enforcement so that they are able to act more swiftly to seize and recover cryptoassets which are the proceeds of crime or associated with illicit activity such as money laundering and ransomware attacks. Specifically, the act has introduced provisions for the Police and National Crime Agency to seize cryptoassets more easily and convert them into money before a forfeiture hearing has taken place. In exceptional circumstances, there will also be a power to destroy seized cryptocurrency.

Essentially, the criminal and confiscation powers of the Proceeds of Crime Act 2002 (POCA), Parts 2, 3 and 4, are amended as well as the civil recovery powers in Part 5 of POCA. These amendments enable law-enforcement agencies to tackle criminal use of cryptoassets more effectively.

Anti-money laundering powers

The act strengthens the anti-money laundering (AML) powers, which should enable better information sharing on suspected money laundering, fraud and other economic crimes. The act will:

- enable businesses in certain situations to share information more easily for the purposes of preventing, investigating or detecting economic crime. This will be achieved by disapplying civil liability for breaches of confidentiality for firms that share information to combat economic crime

- enable proactive intelligence gathering by law enforcement and strengthening the National Crime Agency's Financial Intelligence Unit's ability to obtain information from businesses concerning money laundering and terrorist financing. This is achieved by removing the requirement for a pre-existing suspicious activity report having to be filed before an Information order can be made
- focus private sector and law-enforcement resources on high-value activity. This will reduce the reporting burden on businesses, enabling greater prioritisation of law-enforcement resources by expanding the types of case in which businesses can deal with clients' property without having to first submit a defence against money laundering.

Filing requirements

This is probably the issue of most interest to accountants acting for small and micro-entities.

The first thing to note is that small companies will no longer have the option to prepare and file abridged accounts. The act also removes the option to file 'filleted' accounts. Instead, small companies will be required to file **both** the profit and loss account and directors' report. Micro-entities will be required to file their profit and loss account (although there is no requirement for micro-entities to prepare a directors' report, hence there will be no need to lodge one at Companies House).

In the past, it has been difficult for Companies House to determine whether an exemption taken by the company was valid: for example, whether the entity is a micro-entity or not, because the profit and loss account was not lodged with the registrar, so one of the criteria for taking the exemption was unavailable. The registrar was therefore reliant on the two remaining criteria (being balance sheet total and employee numbers), so provided these were within the limits, the registrar had to accept the exemption was available.

Interestingly, the act includes provisions that allow the registrar to make the profit and loss accounts of small or micro-entities (or parts thereof) unavailable for inspection. This may provide some element of relief for those concerned about trading information could be deemed 'commercially sensitive' becoming publicly available. Hence, filing the profit and loss account with Companies House will enable them to verify that companies are filing the accounts correctly (ie the company is, in fact, a micro-entity or small, hence relevant exemptions taken by the entity are valid). Secondary legislation is needed in this respect and so until this is published, it is currently uncertain as to whether the profit and loss account of small and micro-entities will be unavailable for inspection.

Many small companies and micro-entities are currently entitled to claim audit exemption. Where advantage of this is taken, a statement under s477 of the Companies Act 2006 is required to be made on the balance sheet. The act includes a further requirement where companies (including dormant companies) claim audit exemption. This additional statement must identify the exemption being taken and confirming that the company qualifies for the exemption.

Register of Overseas Entities

The Register of Overseas Entities aims to enhance transparency around aspects of ownership. Where an entity does not declare their beneficial owner, they will face restrictions on selling their property. Where it can be proven that a person has broken the rules, they can face up to five years in prison.

This particular register came into force in August 2022. All companies on the register will need to lodge an updated statement on an annual basis confirming that the information held by Companies House is correct and up to date. This is required even if nothing has changed. Entities on the register should note that it is a criminal offence not to file the updated statement, and the offence is punishable by prosecution or a financial penalty.

Other notable changes

Other key changes brought in by the new act are summarised as follows:

Registered office

Companies are required to ensure that their registered office is, at all times, situated at an appropriate address. An 'appropriate address' is an address where, in the ordinary course of events, a document addressed to the company, and delivered there by hand or by post, would be expected to come to the attention of a person acting on behalf of the company, and the delivery of documents is capable of being recorded by the obtaining of an acknowledgement of delivery. A failure to meet this requirement is punishable by a fine.

The registrar will have the power to change the address of a company's registered office, both on application and on its own motion, if they are not satisfied that it is an appropriate address.

Email address

All companies must have a registered email address. This must be one where, in the ordinary course of events, emails sent to it by the registrar would be expected to come to the attention of a person acting on behalf of the company. A failure to maintain an appropriate email address without reasonable excuse will be an offence and the company's officers will be subject to a criminal penalty.

The purpose of this new requirement is to enable the registrar to communicate with all companies electronically. It should be noted that the registered email address will not be made available for public inspection.

Company names

The circumstances restricting company names have been widened to include those that could facilitate the commissioning of offences involving dishonesty or deception, or which may be misleading (ie those that may suggest a connection with a foreign government or various international bodies).

Company formation

Additional statements will need to be completed to confirm formation for a lawful purpose and that subscribers, directors and PSCs are not disqualified directors.

Company registers

The act abolishes the requirement for companies to maintain their own register of directors, directors' residential addresses, secretaries and PSCs. Instead, the public will rely on filings at Companies House, which will become the single and verified source of information for company registers.

Register of members

There is a requirement for a company to maintain a register of members as it will no longer be able to hold this centrally at Companies House, and certain information must be included. The register must include 'required information' concerning members. This means that the members' forenames and surnames must be entered in the register as well as a service address. For corporate members and firms, the corporate or firm name and a service address is required. The register must also note the date the person was entered as a member.

New members will need to ensure that the company is supplied with the required information within two months of them becoming a member. Any changes to that information must be notified within two months of the change occurring. A criminal offence (punishable by a fine or imprisonment, or both) will be committed where there is a failure to comply with this requirement without a 'reasonable excuse'.

Shortening an accounting period

The act reduces the number of times a company can shorten its accounting reference date to once in every five years. Companies have taken advantage of a loophole in the legislation, which provides an extra three months' filing grace where an accounting period is shortened by one day (as a company could shorten its accounting period as many times as it wished). This new limitation is aligned to the lengthening of an accounting period, which can only be done once every five years.

Disqualification of directors

Disqualification will be possible if there are persistent breaches of company filing obligations and identity verification requirements. In addition, it will not be possible for an individual subject to UK sanctions to act as a director.

Limited partnerships

Part 2 of the act introduces changes to the law on limited partnerships. This was deemed necessary to bring the legislation up to date and to tackle the perceived abuse of limited partnerships. The changes include the following:

- Stricter registration requirements will require more information concerning the partners of a limited partnership. This information must be submitted by authorised corporate service providers, which are supervised for AML purposes.
- Limited partnerships must have a firmer connection to the part of the UK in which they are registered by having to maintain a registered office there.
- All limited partnerships will need to submit statements confirming that the information held about them on the register is correct.
- The registrar will be able to deregister a limited partnership that is dissolved or no longer carries on business.
- Sanctions will be enforced for breaches of the above against the partners of the limited partnership.

The broader reforms to Companies House found in other areas of the act will also impact limited partnerships. This is because the role and power of the registrar is wider, hence there will be mandatory identity verification of general partners, which will then provide enhanced data sharing of information concerning limited partnerships.

Limited liability partnerships (LLPs)

Secondary legislation will be passed in due course to adapt company law, as amended by the act, to the law governing LLPs.

Members of the LLP will be required to verify their identities and a criminal offence will be committed if they fail to do so. The members will also be required to verify the identity of the PSCs. Where a partner is a corporate entity, all of the directors (or equivalents) will be required to verify their identity.

The changes brought about by the act will also apply to all information submitted to Companies House by LLPs. Hence, the registrar will have the power to query information that is held about the entity on the register. The registrar will also be able to exchange information with other bodies.

LLPs that are the general partners of limited partnerships (and which are also corporate entities) will be required to name a managing officer who is an individual for the purposes of communicating with the general partner and the new corporate director reforms as discussed above and will apply to all LLPs acting as corporate director. An LLP will only be able to act as a corporate director if all the members have had their identity verified.

Conclusion

The act has been described as ‘world-leading’ and the reforms have been welcomed across government. However, secondary legislation and guidance is needed to implement many of the measures. Changes to the systems at Companies House will also be needed to deal with the new identity measures, for example.

JANUARY 2024

ACCA LEGAL NOTICE

This technical factsheet is for guidance purposes only. It is not a substitute for obtaining specific legal advice. While every care has been taken with the preparation of the technical factsheet, neither ACCA nor its employees accept any responsibility for any loss occasioned by reliance on the contents.