KIRKLAND ALERT | SEPTEMBER 2019

UK Financial Services Regulatory Team Summer Bulletin

In our Winter Bulletin, we summarised some of the key developments relevant to our clients doing business in Europe. In this edition, we revisit some of those developments that either have attracted renewed regulatory attention or that are at a key stage in their implementation. We also review certain other important developments with a market-wide impact.

There are a few areas, which are not discussed in this note, but we anticipate will be at the forefront of regulators' priorities in the coming months. These include firms dealing with systems and controls in relation to money laundering, financial crime and suspicious transactions, market abuse, and issues around supervisory convergence and oversight.

In the US, a significant development will be the introduction of the California Consumer Privacy Act ("CCPA") from 1 January 2020. The CCPA will apply to private fund managers doing business (which is defined broadly) in California that have gross annual revenue in excess of $25 million, and collect, process, use or share "personal information" from consumers. See our recent *KirklandAIM*, which examines the impact of the CCPA to fund managers.

^ TOP

Brexit

There have been significant political changes in the past few weeks in the UK but as things stand, unless a deal or an extension is agreed to by the leaders of the European Union ("EU") and the UK's new Prime Minister, Boris Johnson, there is a possibility that the UK will leave the EU on 31 October 2019 without a deal (a "hard" or no-deal Brexit) and without a transitional period. In such a scenario, UK-regulated firms currently benefitting from a passport will lose their ability to provide cross-border services into EU countries on a passported basis with immediate effect. This will include any services or activities currently carried out by the firm in one or more EU countries that are licensable under the Alternative Investment Fund Managers Directive ("AIFMD") and the revised Markets in Financial Instruments Directive ("MiFID II").

Regulators in the EU and the UK have signed memoranda of understanding in an effort to mitigate the effect of a hard Brexit on the financial services industry. Various EU regulators have also issued guidance on any temporary relief that may be available to UK firms in the event of a hard Brexit.

LUXEMBOURG TRANSITIONAL REGIME

Recently, the Luxembourg regulatory authority, *Commission de Surveillance du Secteur Financier* ("CSSF"), issued further guidance for UK firms providing cross-border services into Luxembourg in a hard Brexit scenario. It notes that UK alternative investment fund managers ("AIFMs") currently providing services in Luxembourg under an AIFMD or MiFID II passport (as well as under passports introduced by certain other EU directives) will first need to notify (through a dedicated portal) the CSSF no later than 15 September 2019 of their 'intentions and way forward' to address any consequences of a hard Brexit. As a second step, UK managers will need to submit an application for authorisation, notification and/or submit

Regulators in the EU and the UK have signed memoranda of understanding in an effort to mitigate the effect of a hard Brexit on the financial services industry.

other required information (depending on the nature of activities they wish to pursue in Luxembourg) before 31 October 2019 to benefit from the 12-month transitional regime following the date of a hard Brexit.

The difficulty arises with the post-Brexit options the CSSF presents for UK AIFMs making the notification. These are:

a. another legal entity will apply for authorisation/an additional license under the AIFMD in Luxembourg and will be appointed as the AIFM;

b. another legal entity will apply for/already has an authorisation under the AIFMD in another EU country and will be appointed as the AIFM; and

c. the Alternative Investment Fund ("AIF") will be liquidated before the end of the transitional period.

The current market practice in Luxembourg is that non-EU AIFMs may manage unregulated Luxembourg funds (not including Reserved Alternative Investment Funds) without needing authorisation under the AIFMD. We understand that the CSSF has distinguished the Brexit scenario on the basis that investors who had invested in the fund pre-Brexit had invested with the full protections of the AIFMD. For funds managed by other third country managers, investors had never enjoyed those protections. In particular, the key question is if UK AIFMs make the notification by 15 September 2019 to benefit from the transitional regime, then would it imply that after a hard Brexit, a UK AIFM may not manage the Luxembourg fund as a non-EU AIFM?

^ TOP

WHAT'S NEXT?

The political situation is uncertain and unpredictable. The current government appears set on leaving the EU on 31 October, deal or no deal, but there is significant domestic opposition to such an outcome both in Parliament and in the wider electorate. The Parliament passed a bill on 9 September requiring the Prime Minister to seek a three-month Brexit extension if a deal cannot be agreed with the EU by 19 October.

For UK AIFMs managing Luxembourg funds, it remains to be seen whether the CSSF will expand the options available for funds managed by UK AIFMs at the end of the transitional period. In any event, firms affected should be finalising their plans for a hard Brexit and keep a close eye on developments.

AIFMD Review

WHO NEEDS TO THINK ABOUT THE AIFMD REVIEW?

Any EU AIFM or non-EU AIFM that manages an AIF in the EU or markets an AIF to EU investors.

WHAT IS CHANGING?

Article 69 of the AIFMD requires the European Commission to review the functioning of the AIFMD, in particular, its impact on investors within the EU and in third countries, and the degree to which its objectives have been met. KPMG conducted a general survey addressed to the stakeholders that are most affected by the AIFMD and produced a report earlier this year. The report is lengthy and provides an indication of the topics that are likely to be considered by the European Commission in its review. These include:

- **Lack of harmonisation across member states:** A large number of respondents found that the AIFMD is not applied consistently across member states (such as marketing requirements).
- **Reporting requirements concerns:** AIFMs submit large volumes of data to national competent authorities ("NCAs") under the AIFMD reporting requirements, but some of the data may be insufficient, duplicative or not essential. Respondents also noted that there are differences between NCAs in the methods of data delivery. Requests from some NCAs for additional information on a periodic or ad hoc basis increases the costs of compliance.
- **Inconsistent leverage calculation methodologies:** Some respondents noted that it would be helpful to harmonise the calculation methodologies for leverage across the AIFMD, the Undertakings for Collective Investment in Transferable Securities ("UCITS") Directive and other relevant legislation. Industry respondents suggested that changes to the requirements should be made taking into consideration the recent recommendations of the International Organization of Securities Commissions.
- **Onerous requirements for investments in non-listed companies:** Respondents reported that the level of detail in the notifications to NCAs under the rules for investments in non-listed companies was not useful or essential, and was overly burdensome (especially given that many private equity/venture capital AIFMs are smaller companies, for whom the administrative burdens may be proportionately greater).
- **Confusion about passport regimes:** Respondents noted that although the EU management passport is working well, the EU marketing passport has not been as effective and suffers from a divergence in approaches taken by NCAs. Developments vary from one member state to another and appear to be heavily dependent on national measures. Some respondents noted the helpfulness of national private placement regimes ("NPPRs") and examined whether the third country passport should be introduced, as market participants have now become familiar with NPPRs.

WHAT'S NEXT?

The European Commission will continue its review of the AIFMD, taking into consideration the report's information and conclusions alongside other sources of data and further analysis. More information will be available in 2020 when the European Commission issues its reports to the European Council and the European Parliament.

Omnibus Proposals on Cross-Border Marketing

WHO NEEDS TO THINK ABOUT THE PROPOSALS ON CROSS-BORDER MARKETING?

All EU AIFMs managing and marketing an EU AIF. Non-EU AIFMs must also consider these proposals, as there is likely to be an indirect impact.

WHAT IS CHANGING?

The European Council adopted a cross-border directive on distribution of collective investment undertakings ("CBDF Directive") and a related regulation ("CBDF Regulation") (collectively, the "Omnibus Proposals") on 14 June 2019. The Omnibus Proposals are designed to create a harmonised EU framework for cross-border fund distribution, and propose to do so by amending the AIFMD and the UCITS Directive.

- Pre-marketing is now a formally recognised concept under the Omnibus Proposals.
- EU AIFMs have an obligation to notify the regulator about pre-marketing activities (i.e., soft marketing) through a letter.
- Soft marketing must be conducted through an EU-authorised entity (e.g., an AIFM, MIFID investment firm or a bank).
- Although expressed to apply only to EU AIFMs managing EU AIFs, it is likely that certain provisions will be applied more broadly.

The Omnibus Proposals are designed to create a harmonised EU framework for cross-border fund distribution, and propose to do so by amending the AIFMD and the UCITS Directive.

In addition, the Omnibus Proposals make reliance on reverse solicitation more difficult. The CBDF Directive provides that a subscription within 18 months of the commencement of any pre-marketing activity will be deemed to have resulted from active marketing, triggering the passporting requirement under AIFMD for EU AIFMs.

For a more detailed summary of the changes brought by the Omnibus Proposals, please see our recent *Alert*, "Revised Proposals for Marketing of Funds in Europe."

WHAT'S NEXT?

The Omnibus Proposals have been published in the Official Journal of the European Union. The CBDF Directive came into force 1 August 2019 with an implementation period of two years (2 August 2021). Note that the CBDF Regulation came into force on 1 August 2019 with most of the substantive provisions applying from 2 August 2021.

Revised Rules on Prudential Supervision of Investment Firms

WHO NEEDS TO THINK ABOUT THE REVISED RULES ON PRUDENTIAL SUPERVISION?

All investment firms authorised under MIFID II, including those that are adviser/arranger firms.

WHAT IS CHANGING?

The new regulation on prudential requirements for MiFID investment firms

("IFR") and the accompanying directive ("IFD") were passed by the European Parliament on 16 April 2019. IFR and IFD will introduce a new prudential regime for most MiFID investment firms to replace the one that currently applies under the fourth Capital Requirements Directive ("CRD IV") and the Capital Requirements Regulation ("CRR").

The new framework set out in IFD and IFR results in investment firms being divided into three classes with each class capturing different risk profiles.

Firms that anticipate being affected by the IFR and IFD must perform some preliminary calculations and determine their initial (and on-going) capital requirements. To assist, we set out below the classification of firms and their initial capital requirements under the IFD and IFR.

The new framework set out in IFD and IFR results in investment firms being divided into three classes, each class capturing different risk profiles.

Class 1, "article 1(2) firms" or Systemically Important Firms	
Conditions	Systemically important firms or article 1(2) firms (broadly large investment firms carrying on activities such as market making or underwriting will be reclassified as credit institutions (i.e., banks) for prudential purposes and will therefore be subject to requirements similar to those currently imposed on credit institutions).
Prudential Regime	The existing CRD IV and CRR regime will continue to apply to these firms.
Initial capital requirements	€5 million

Class 2 or Larger Firms Above Threshold	
Conditions	Firms that are neither Class 1 nor Class 3 (see below).
Prudential Regime	These firms will be subject to the full revised prudential regime as set out in IFD and IFR.
Initial capital requirements	€75,000 for adviser/arranger firms that are not permitted to hold client money. The initial capital requirement could be higher for other firms (€ 750,000 depending on if the firm deals on its own account, underwrites financial instruments or operates an MTF/OTF); or €150,000 for all other investment firms).

Class 3 or Small and Non-Interconnected Firms	
Conditions	The draft rules (article 12 of the IFR) provide for how to distinguish between a Class 2 firm and a Class 3 firm. Class 3 firms must meet certain requirements, such as having a "total annual gross revenue from investment services and activities" of less than €30 million and having assets under management of less than €1.2 billion.
Prudential Regime	Reduced IFR requirements will apply.
Initial capital requirements	€75,000

^ TOP

Note that one of the key changes is the requirement for firms to hold general ongoing capital, and this may increase significantly for certain firms. Class 2 firms must hold capital corresponding to the highest of:

- their fixed overheads requirement: at least 25% of the fixed costs of the preceding year (we expect that this requirement would be the primary reason for the increased capital requirements for firms);
- their permanent minimum capital requirement: at least equal to the amount of initial capital (see table above, likely to be EUR 75,000 for most firms); or
- the K-factor requirement: this consists of broadly individual quantitative indicators intended to represent the risks that a firm can pose to clients, to the market and to the firm itself.

The rules divide the K-factors into three groups, which in turn consist of sub-groups related to the respective risk. Of particular interest to Exempt CAD or adviser/arranger firms are the K-factors pertaining to AUM (assets under management, which includes portfolio management and non-discretionary advisory services) and COH (client orders handled).

The IFD and IFR also introduce more onerous remuneration rules based on those applicable to banks (although there is no bonus cap), as well as a number of internal governance and public disclosure and reporting requirements.

WHAT'S NEXT?

To become law, the IFR and IFD must be adopted by the European Council and published in the Official Journal of the European Union, which is expected later this year. The provisions related to new capital and remuneration requirements will apply 18 months thereafter, subject to phase in provisions of up to five years for certain firms.

The provisions of SRD II most relevant to asset managers focus on increasing stewardship or shareholder engagement in listed companies.

Stewardship & the Shareholder Rights Directive II

WHO NEEDS TO THINK ABOUT THE SHAREHOLDER RIGHTS DIRECTIVE?

Any investment firm that provides portfolio management services to investors, a UCITS Directive management company, a UCITS fund without an external management company and an AIFM (excluding a sub-threshold AIFM). It is not clear if the obligations on AIFMs apply to non-EU AIFMs, but the UK rules make it clear that they apply only to UK-authorised AIFMs.

WHAT IS CHANGING?

The rules implementing the revised Shareholder Rights Directive ("SRD II") have applied since 10 June 2019.

SRD II amends the first Shareholder Rights Directive ("SRD I") and includes requirements relating to shareholder identification, directors' remuneration policies and reports, as well as related party transactions that will impact traded companies (i.e., listed companies). There are also requirements relating to intermediaries, asset managers, institutional investors and proxy advisers.

The provisions of SRD II most relevant to asset managers focus on increasing stewardship or shareholder engagement in listed companies. Specifically, there is a requirement to produce an engagement policy regarding company stewardship and report annually on the implementation of that engagement policy, as well as to provide a general description of voting behaviour and an explanation of the most significant votes.

^ TOP

These provisions apply on a "comply or explain" basis, so there is an opportunity to instead provide a reasoned explanation as to why such a policy has not been produced.

To the extent an asset manager has any investors that are life insurers or pension funds, it will need to explain to such investors how its investment strategy and the implementation thereof complies with arrangements with the investors and contributes to the medium- to long-term performance of the assets of the investors/the funds in which those investors hold interests.

Our recent *Alert*, "What Asset Managers Need to Know About the Shareholder Rights Directive II," discusses SRD II in further detail.

In January 2019, the UK Financial Conduct Authority ("FCA") and the Financial Reporting Counsel ("FRC") issued proposals to revise the existing UK Stewardship Code (published in 2010 and updated in 2012) relating to stewardship in the institutional investment community ("Stewardship Code"). These proposals must be read in the context of the final rules on SRD II published by the FCA, as the revised proposals on the Stewardship Code build on SRD II and could be extended further.

WHAT'S NEXT?

The FRC consulted on such changes earlier in 2019, and finalisation of the revised Stewardship Code is expected in Q3 of 2019.

Senior Managers & Certification Regime

WHO NEEDS TO THINK ABOUT THE SENIOR MANAGERS AND CERTIFICATION REGIME?

All FCA-regulated firms. Banks, PRA-designated investment firms and dual-regulated insurers are already subject to the Senior Managers and Certification Regime ("SMCR"). The SMCR will be extended to cover all FCA-authorised firms.

WHAT IS CHANGING?

Under the SMCR extension, the regime applies differently to firms depending on whether they are categorised as (a) Limited Scope Firms, (b) Core Firms or (c) Enhanced Firms. These firms are subject to SMCR requirements to varying extents to reflect the type and size of firm.

SMCR has a three-tiered approach and consists of:

- **Senior Managers Regime:** This regime replaces the current Approved Persons regime and will apply to all Senior Managers, generally being the most senior persons responsible for a particular area of the business. Similar to the current Approved Persons regime, Senior Managers will be subject to pre-approval by the FCA and heightened supervision by the regulator.
- **Certification Regime:** This regime will apply to persons who are not Senior Managers, but whose role means that it is possible for them to cause significant harm to the firm or its clients. In contrast to Senior Managers, Certified Persons will not need to be pre-approved by the FCA.
- **Conduct Rules:** The Conduct Rules will replace the current Statements of Principle for Approved Persons and apply to all employees apart from 'ancillary staff' (secretarial, security, cleaners, etc.).

WHAT'S NEXT?

The SMCR will be extended to apply to all solo-regulated firms on 9 December 2019. Firms must identify individual staff performing Certification Functions by 9 December, but there is a 12-month implementation period to allow firms to complete their fitness and propriety assessments and get the certification paperwork in place by 9 December 2020.

The FCA's interest in sexual harassment allegations and findings is part of the broader focus on **culture within the UK financial services industry.**

^ TOP

FCA's Focus on Conduct & Culture — #MeToo

WHO NEEDS TO THINK ABOUT THE FCA'S FOCUS ON CONDUCT AND CULTURE?

All FCA-regulated firms.

WHAT IS CHANGING?

Banks and building societies that are already subject to the SMCR have been taking a more holistic view of conduct for the past few years. There is recognition in the market that non-financial misconduct (including sexual harassment) can have regulatory implications for market participants. The FCA has identified the culture of financial services as one of the 'root causes' of why things go wrong or cause harm to the market. The FCA's interest in sexual harassment allegations and findings is part of its broader focus on culture within the UK financial services industry. This has garnered more attention as a result of the letter written by Megan Butler, the executive director of supervision at the FCA, to the Women and Equalities Committee recently. The FCA is clear that it expects firms to foster healthy cultures that create an environment of psychological safety, and that tolerance of this type of misconduct is an obstacle to retaining talent and making the best business and risk decisions.

The FCA has outlined its priorities in this area in its business plan for 2019–2020 and has built a new webpage about psychological safety within the Culture and Governance section of its website earlier this year. This new emphasis is not merely about having proper systems and controls in place for would-be whistleblowers (which the FCA expects firms already have in place), but also about creating a firm culture in which conduct does not exist that would cause employees to feel like they need to blow the whistle.

WHAT'S NEXT?

The FCA has announced on several occasions that firms' handling of poor personal misconduct, including allegations of sexual misconduct, is a topic that the FCA is increasingly discussing with firms. The FCA will continue to give it serious consideration, including through the continued roll-out of the SMCR.

Sustainable Finance Action Plan

WHO NEEDS TO THINK ABOUT THE SUSTAINABLE FINANCE ACTION PLAN?

As currently drafted, the draft proposals apply to (amongst others) asset managers and firms that provide portfolio management, fund management and investment advisory services.

WHAT IS CHANGING?

This is a broad initiative focusing on the provision of finance to investments taking into account environmental, social and governance ("ESG") considerations. The European Commission in 2018 produced an Action Plan on Sustainable Finance ("Action Plan"), which includes a number of proposals for new regulations.

The Action Plan establishes a framework to facilitate sustainable investment (amending AIFMD, UCITS Directive and MiFID II). To further this aim, the European Parliament adopted a Disclosure Regulation at first reading on 18 April 2019.

The Disclosure Regulation contains a number of transparency and disclosure obligations. AIFMs and MiFID firms must:

- Publish sustainability information on their websites, including an explanation of their policies on the integration of sustainability risks in their processes, and of how their remuneration policies are consistent with the firm's integration of sustainability risks. Firms will be required to keep this information up-to-date and, if the information changes, to include a clear explanation of the reason for the change.

^ TOP

- Publish information on whether the firm considers the principal adverse impacts of investment decisions (or investment advice) on ESG matters, respect for human rights, anti-corruption and bribery. This applies on a comply-or-explain basis and proportionately, i.e., the requirement is subject to individual firms' size, nature, scale of activities and the types of financial products they deal with. The option to explain (rather than comply) will cease 18 months after the Disclosure Regulation comes into force for firms (or firms within groups) that have 500 or more employees.
- Include sustainability-related risks in pre-contractual disclosures (e.g. AIFMD disclosures in private placement memoranda) and ongoing reporting to investors, including pre-contractual disclosure of how the firm integrates sustainability risks into its management or advisory processes, and the likely impact of sustainability risks on financial returns. Again, this is on a comply-or-explain basis (with the exception of sustainability-focussed products, as discussed below).
- Disclose further information in relation to sustainability-focused financial products, including: (a) publicly disclosing a description of the sustainability objective of the product and methodologies used to assess it (which raises financial promotion issues); and (b) disclosing the sustainability impact of the product in periodic reports. These disclosure obligations will be subject to detailed requirements and methodologies (to be developed in future regulatory technical standards).

To this end, the European Securities and Markets Authority ("ESMA") has consulted on amendments to the AIFMD relating to: (a) general organisational requirements, (b) resources, (c) senior management responsibilities, (d) conflicts of interest, (e) due diligence requirements and (f) risk management. Similar proposals are in consideration for amendments to MiFID II.

WHAT'S NEXT?

Much of the detail regarding the content, methodology and presentation of the new sustainability disclosure requirements will be set out in future technical standards after the Disclosure Regulation comes into force.
The regulation itself should apply from 15 months after its publication in the Official Journal of the European Union, which is expected to occur later this year.

EMIR Refit Regulation

WHO NEEDS TO THINK ABOUT THE EMIR REFIT REGULATION?

Anyone who participates in the EU derivative markets.

WHAT IS CHANGING?

Regulations regarding the clearing obligation, the suspension of the clearing obligation, the reporting requirements, the risk mitigation techniques for OTC derivative contracts not cleared by a central counterparty, the registration and supervision of trade repositories and the requirements for trade repositories (Regulation 2019/834) ("EMIR Refit") came into force on 17 June 2019 and introduced a number of amendments to existing requirements under the Regulation on OTC derivative transactions, central counterparties and trade repositories (Regulation 648/2012) ("EMIR").

An important change relevant to asset managers is that all EU AIFs (regardless of the AIFM's location) will be categorised as a Financial Counterparty ("FC") unless the vehicle is a securitisation special purpose vehicle or is established solely for an employee share purchase plan. Further, while EMIR does not directly apply to such vehicles, AIFs established outside the EU will be treated as third country FCs in their dealings with EU banks because they would be FCs if established in the EU.

In practice, this means that the following entities will be considered to be FCs:

- EU AIF with an EU AIFM; and
- EU AIFs with a non-EU AIFM.

Non-EU AIFs with non-EU AIFMs are classified as third country FCs and so are indirectly subject to EMIR obligation when trading with directly in-scope entities.

An AIF that is an FC must clear OTC derivatives subject to the clearing obligation if it exceeds certain clearing thresholds and becomes a "large" FC.

Even if such an AIF does not exceed the clearing thresholds, it must comply with the margin requirements for uncleared trades and with the operational risk mitigation techniques for uncleared trades and the reporting requirements as they apply to FCs, each as required under EMIR.

Under EMIR Refit, the AIFM, rather than the AIF itself, will become solely responsible and legally liable for reporting each OTC derivative trade.

Other changes include the introduction of a category of 'small financial counterparties' (which will not be subject to the EMIR clearing obligation) and changes to certain reporting obligations.

WHAT'S NEXT?

After notification of their status to ESMA, FCs (above clearing threshold) and Non-Financial Counterparties (above clearing threshold) will have four months (until 17 October 2019) to establish the clearing arrangements necessary to allow them to clear applicable transactions going forward, and to put in place collateral documentation providing for the mandatory exchange of margin.

Market participants should note that aspects dealt with in EMIR Refit are subject to the development of further technical standards and/or periodic review by ESMA, and that further developments in this area are likely.

Cybersecurity & Operational Resilience

WHO NEEDS TO THINK ABOUT THIS?

Cybersecurity incidents are increasing in number, scale and sophistication. For example, since 2014, there has been a 1,700% increase in cyber attacks reported to the FCA. For this reason, all organisations that process confidential information (and in particular personal data) need to be aware of the regulatory framework in the UK and associated risks.

In the event of a cybersecurity breach, organisations can suffer reputational damage that, in some cases, can affect share price, claims from individuals/companies whose information has been compromised, and/or face significant enforcement action from various regulators (including monetary penalties levied by the FCA, the Prudential Regulatory Authority ("PRA") and the UK Information Commissioner's Office ("ICO"). In addition, under the UK Companies Act 2006, a company director could face personal liability for a breach of their fiduciary duties, should a company fail to have adequate cybersecurity measures in place.

A NEW FINANCIAL SERVICES REGULATORY PRIORITY?

In its business plan for 2019–2020, the FCA chairman warned that cyber resilience was a key risk area for the financial services industry, and that the cybersecurity practices of financial services firms operating in the UK will increasingly be under the regulatory microscope as the cyber threat continues to grow. The FCA intends to undertake a number of further activities in this area this year, such as:

- review its expectations of firms' practices for change management as part of their wider resilience agenda;
- use regulatory tools to test the cyber capabilities of high-impact firms;
- undertake multi-firm supervisory work to better understand the protection measures that firms take against cyber attacks; and

^ TOP

TOP

- respond to major operational incidents, working with other authorities to ensure there is a coordinated response.

WHAT IS THE LAW IN THIS AREA?

The UK has a substantial body of law governing cybersecurity, comprised of laws enacting EU directives and regulations, together with standalone specific UK laws and regulations. A summary of the key cybersecurity laws and regulations that relate to the financial industry is outlined in the following tables.

UK Companies Act 2006	
Applies to:	Directors of companies
Relevant Cybersecurity Obligations	Directors should be aware that they can potentially be held personally liable where they fail to appropriately manage cybersecurity risks. The UK Companies Act imposes a duty on directors to exercise reasonable care, skill and diligence
Notification Obligations	N/A
Penalties	Where shareholders suspect that a director has breached their fiduciary duties, they can commence a derivative action against the company's directors, seeking damages. Although proceedings brought on these grounds in the UK have been rare to date, attempts to hold directors liable are likely to become more common as the frequency of cybersecurity incidents (and corresponding regulatory enforcement) continues to increase.

FCA Handbook	
Applies to:	Financial services firms
Relevant Cybersecurity Obligations	Principle 3 - Firms must take reasonable care to organise and control their affairs responsibly and effectively, with adequate risk management systems.
Notification Obligations	Principle 11 - Firms must report material cyber events to the FCA immediately. Firms may consider an incident material if it: • results in significant loss of data, or the availability or control of its IT systems; • impacts a large number of victims; or • results in unauthorised access to, or malicious software present on, its information and communication systems
Penalties	The FCA has the power to issue monetary penalties for breaches of the FCA Handbook. Notable fines include: £3 million issued by the then-Financial Services Authority ("FSA") against three HSBC firms for various data security failings £1.26 million issued by the then-FSA against Norwich Union Life for failing to implement effective systems and controls to protect customer data Approximately £2.3 million issued by the then- FSA against Zurich Insurance Plc after a subcontractor, who was not adequately supervised, lost an unencrypted back-up tape with data relating to 46,000 customers

Cyber incidents are inevitable and organisations can expect regulatory activity in this area to continue to increase, and notably the FCA is pursuing enforcement investigations more frequently than it has in the past.

General Data Protection Regulation ("GDPR")	
Applies to:	Data controllers and data processors of personal data
Relevant Cybersecurity Obligations	Data controllers and data processors must implement "appropriate technical or organisation measures" taking into account the nature, scope, context and purposes of processing
Notification Obligations	Data controllers must notify: the applicable supervisory authority, within 72 hours of a personal data breach (unless the breach is unlikely to result in a risk to the rights and freedoms of individuals); and affected individuals without undue delay, where the personal data breach is likely to result in a **high** risk to their rights and freedoms.
Penalties	Fines may be issued by the ICO of up to €20 million or 4% of annual worldwide turnover (whichever is higher), as well as the possibility of other enforcement actions (such as suspension of processing activities and audits), liabilities from third-party claims and reputational damage

Network and Information Security Directive ("NIS Directive")	
Applies to:	Operators of essential services (i.e. entities that provide critical infrastructure across sectors including healthcare, transport, energy and banking) ("OES")
Relevant Cybersecurity Obligations	OESs must implement proportionate technical and organisational measures to manage risks posed to the security of their services
Notification Obligations	OESs must notify a supervisory authority without undue delay in the event of a breach that affects the security of their systems
Penalties	The UK NIS Regulations 2018 provide the ICO with the power to issue penalties of up to £17 million

Electronic Identification and Trust Services for Electronic Transactions Regulation ("eIDAS Regulation")	
Applies to:	Trust service providers (i.e. companies that provide services that help verify the identity of individuals or businesses online)
Relevant Cybersecurity Obligations	Trust service providers must take appropriate technical and organisational measures to manage the risks posed to the security of their services
Notification Obligations	Providers must notify a supervisory authority without undue delay in the event of any breach of security that impacts their service
Penalties	Providers are liable for damages caused to any individual due to a failure to comply with their obligations

WHAT'S NEXT?

Cyber incidents are inevitable and organisations can expect regulatory activity in this area to continue to increase. For example, the FCA issued a Final Notice in respect of Tesco Bank in October 2018 (imposing a financial penalty of £16.4 million) and in respect of the Royal Bank of Scotland (RBS) in November 2014 (where the FCA imposed a financial penalty of £42 million and the PRA imposed an additional penalty of £14 million). The RBS case focused on IT resilience and operations, while the Tesco Bank case concerned a cybersecurity failure.

The FCA and PRA's enforcement powers run parallel with the enforcement powers

TOP

of the ICO, which has the power to investigate and impose sanctions on businesses that fail to put appropriate safeguards in place to protect personal data, as well as those that fail to meet their obligations to report cybersecurity incidents to the ICO.

In light of the above, firms and organisations should continue to heed the following advice from the FCA and other regulators to mitigate cybersecurity risk:

- cybersecurity should be a board level issue and appropriate cybersecurity practices and processes should be implemented "from the ground up";
- consider recruiting cybersecurity "champions" in the business who understand cyber and can help to bridge any gaps between the business and its technology and security functions;
- review whether the cybersecurity measures they have taken are proportionate to the nature and scale of their business and consider engaging with cybersecurity operational experts to test such measures;
- actively monitor critical systems and network behaviour;
- conduct a data audit to identify what data you process, in relation to whom, where it is stored and its sensitivity;
- keep systems, software and apps up to date and conduct regular IT penetration testing to identify system vulnerabilities;
- back up all critical systems and data;
- obtain recognised cybersecurity industry accreditation (e.g., ISO, Cyber Essentials, CISM etc.);
- vet third-party vendors' safe data handling practices and processes;
- provide regular cybersecurity training to employees that contains a practical and efficient data breach response plan; and
- obtain cybersecurity insurance that provides an appropriate level of cover to the associated risks.

Authors

LISA CAWLEY

ROMIN DABIR

EMMA FLETT

PHILIP MCEACHEN

PREM MOHAN

REVA RAGHAVAN

COLIN SHARPSMITH

ADAM SKINNER

SARAH THOMPSON

JOANNA THOMSON

Kirkland & Ellis International LLP | 30 St Mary Axe, London, EC3A 8AF, UK | +44 20 7469 2000

TOP