CLIFFORD
CHANCE

ON THE (CYBER) ATTACK: HOW ARE THE FCA AND PRA REGULATING CYBER RISK?

There is no doubt that cyber security breaches can present significant operational, financial, data and reputational threats for companies in the UK. In particular, where cyber incidents have, or may have, resulted in personal data breaches, companies are answerable to the Information Commissioner's Office (the "**ICO**"), which has issued fines as high as £20 million (to British Airways in 2020) for failing to protect personal data.

For firms regulated by the UK financial services regulators, weaknesses in cyber security may also present regulatory risks. In recent years, the Financial Conduct Authority (the "**FCA**") and the Prudential Regulation Authority (the "**PRA**", together the "**Regulators**") have made it clear that they expect regulated financial services firms to have effective cyber security controls and to report material cyber incidents. Failure to comply with the Regulators' expectations in relation to cyber risk may result in firms facing enforcement action and sanctions.

This risk has been highlighted by the recent FCA decision to fine Equifax Ltd ("**Equifax**") £11.2m for failing to manage and monitor the security of UK consumer data in relation to a cyber breach which allowed hackers to access the personal data of millions of people in the UK. In this case, the affected data had been outsourced to Equifax's US parent company, Equifax Inc, for processing. As such, the FCA's decision reminds firms that where functions are outsourced, whether internally or externally, the firm must retain appropriate oversight over those outsourced elements to protect against cyber risks and to ensure operational resilience.

Highlighting the regulator's appetite to take enforcement action in relation to cyber security issues, Jessica Rusu, FCA Chief Data, Information and Intelligence Officer, noted with regards to the Equifax decision:

'Cyber security and data protection are of growing importance to the security and stability of financial services. Firms not only have a technical responsibility to ensure resiliency, but also an ethical responsibility in the processing of consumer information. The Consumer Duty makes it clear that firms must raise their standards.'

This briefing further explores the Regulators' powers in relation to cyber security, and looks at their enforcement decisions, including the Equifax case. It also considers how

firms should seek to manage cyber risk by implementing measures both to reduce the risk of a cyber incident occurring and to minimise the impact should one arise.

The Regulators' remit

Whilst there are no UK regulations or regulators specifically dedicated to cyber security, both Regulators have indicated that cyber security is a matter of regulatory interest, and that they expect financial services firms to have effective cyber security controls and to report cyber incidents. In setting out these expectations, the Regulators rely on a number of existing powers:

General principles

The FCA has indicated that its Principles for Businesses, which provide a general statement of the fundamental obligations of firms, and other related rules, apply to regulated firms in the context of cyber security. Therefore, firms are expected to have in place systems and controls designed to manage cyber risk in order to comply with their regulatory obligations, including to act with due skill care and diligence (Principle 2) and to have an adequate risk management framework (Principle 3). Failure to do so may result in harm to customers, for example the theft of personal data in a cyber attack, in breach of Principle 6 (having due regard to the interests of customers and treat them fairly).

The FCA has also made it clear that it expects firms to report material cyber incidents under Principle 11 and Chapter 15 of the Supervision manual (SUP).[1] These rules provide that a firm must deal with its regulators in an open and cooperative way, and must disclose to the FCA anything relating to the firm that the regulator would reasonably expect notice of.

Likewise, a number of the PRA's Fundamental Rules are deemed to be relevant when considering a regulated firm's management of cyber risk including Fundamental Rule 2 (a firm must conduct its business with due skill, care and diligence), Fundamental Rule 5 (a firm must have effective risk strategies and risk management systems) and Fundamental Rule 7 (a firm must deal with its regulators in an open and co-operative way, and must disclose to the PRA appropriately anything relating to the firm of which the PRA would reasonably expect notice). FCA guidance indicates that if a dual-regulated firm is notifying the FCA of a material cyber incident, it should also notify the PRA.[2]

Consumer Duty

Since 31 July 2023, FCA-regulated firms are required to comply with the new consumer principle (Principle 12) which sets out that firms "must act to deliver good outcomes for retail clients". This "Consumer Duty" is designed to ensure higher and clearer standards of consumer protection across financial services by requiring firms to put their customers' needs first.

As indicated by the comments of Ms Rusu in relation to the Equifax decision, the FCA may see the Consumer Duty as relevant when looking at the harm caused to

1 https://www.fca.org.uk/publication/documents/cyber-security-infographic.pdf
2 https://www.fca.org.uk/publication/documents/cyber-security-infographic.pdf; https://www.fca.org.uk/firms/operational-resilience

customers by cyber incidents, e.g., theft of personal data. Accordingly, firms that fail to take steps to protect retail customer data from cyber threats may been seen to be failing to ensure good outcomes for those customers, in breach of the Consumer Duty.

Operational resilience

In recent years, operational resilience has been a key focus of the Regulators and in 2022 the Regulators, along with the Bank of England, introduced a new operational resilience framework. Under this framework, which is set out in chapter 15A of the FCA's Senior Management Arrangements, Systems and Controls sourcebook (SYSC) and the Operational Resilience parts of the PRA Rulebook, firms must identify and map their important business services, set impact tolerances, and implement strategies for complying with the Regulators' requirements in relation to those important business services.

In introducing these requirements, both Regulators highlighted that there is an inherent link between cyber risk management and operational resilience, and that this is a particular focus for the Regulators. For example, the FCA's 2022-25 strategy set out:

"Operational disruptions are inevitable. Firms must be able to respond to, recover and learn from and prevent future operational disruptions. When firms can't, customers can lose access to essential services and confidence in financial services generally.

The disruption caused by Covid-19 and the increasing threat and impacts of cyber-attacks, show why it is especially important for firms to understand the important business services they provide, and to invest in their resilience to protect themselves, consumers and markets.

We've introduced new rules and guidance to strengthen operational resilience. We'll assess the impact of this by testing firms' operational resilience, business continuity and incident response plans, cyber security and third-party management. We will look at how resilient firms are to disruptions as well as the severity and scale of actual disruptions. We will also assess the resilience of third parties that provide critical services to the financial sector. We are focusing our efforts on those firms who can't meet our new standards."[3]

Similarly, in relation to the new operational resilience rules, the PRA's 2023/24 business plan set out:

"[…] the PRA will continue to monitor and assess firms' ability to manage cyber threats through ongoing use of CBEST and the cyber questionnaire (CQUEST). The PRA will collaborate with the FCA, including in response to known technology and cyber incidents, and will continue to monitor and engage with firms on their execution of large and complex IT change programmes. The FPC's recent cyber stress test has broadened the PRA's understanding of how operational disruptions such as cyberattacks may impact financial stability. Throughout 2023 the PRA will continue to deliver this work through a broad range of industry, sector focussed and international engagement including the Authorities Response Framework, the Cross Market Business Continuity Group, the Cross Market Operational Resilience Group and the G7

3 https://www.fca.org.uk/publication/corporate/our-strategy-2022-25.pdf

Cyber Expert Group. This will focus on strengthening the sector's resilience capabilities and its ability to respond to an operational disruption."[4]

Given the close link between cyber security and operational resilience, it is anticipated that, going forward, the Regulators will seek to rely on this framework when taking regulatory action against firms in relation to cyber incidents.

Senior Managers and Certification Regime

Under the Senior Managers and Certification Regime, certain individuals may hold personal responsibility for cyber security. Specifically, the individual performing the Chief Operations senior management function (SMF24) holds responsibility for cyber security and information technology.[5] Alternatively, where a firm does not have an individual who performs the Chief Operations function, responsibility for cyber security must be allocated to another senior manager (in accordance with SYSC 26.11.4G). Consequently, where a cyber incident or other issue arises, the responsible senior manager may face individual regulatory scrutiny and enforcement action if it transpires that, in relation to cyber security, the individual failed to take reasonable steps to prevent any regulatory breach by the firm, was knowingly concerned in any breach and/or did not comply with the Conduct Rules.

The Regulators' appetite for enforcement

The Regulators have wide powers, including to impose fines or other sanctions when their regulatory requirements are breached, and have made clear that they will take enforcement action when needed to ensure that rules are followed and wrongdoers are held to account.[6] However, not every breach of a rule or requirement will result in enforcement action; the Regulators assess the appropriateness of using enforcement tools, the alternative courses of action available and the proportionality of opening an investigation in view of available resources, level of intrusion and cost to the subject.[7]

Although the Regulators have expressed that they are focused on cyber security, prior to the Equifax decision, there had been only one enforcement decision taken by the FCA relating to cyber security, which concerned the handling of a cyber attack by Tesco Personal Finance plc ("Tesco Bank").

There have, however, also been a couple of enforcement actions regarding operational resilience failings in relation to technical outages. These incidents give rise to similar issues as cyber incidents, such as operational disruption and potential customer harm, and highlight the general appetite of the Regulators to take action in relation to issues which cause avoidable operational disruption.

These cases are considered further below.

Tesco Bank

On 1 October 2018, the FCA published a Final Notice setting out its decision to impose a financial penalty of £16.4 million on Tesco Bank. The FCA found that Tesco

4 https://www.bankofengland.co.uk/prudential-regulation/publication/2023/may/pra-business-plan-2023-24
5 SUP 10C.6B.4G
6 See, for example: https://www.fca.org.uk/publication/corporate/our-approach-enforcement-final-report-feedback-statement.pdf; https://www.bankofengland.co.uk/prudential-regulation/pra-statutory-powers
7 See https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/approach/banking-approach-2023.pdf

Bank breached Principle 2 of the Principles for Businesses[8] by failing to exercise due skill, care and diligence in protecting its personal account holders against a cyber attack which took place in November 2016.[9]

In relation to the case, then Executive Director of Enforcement and Market Oversight at the FCA, Mark Steward highlighted that the FCA took enforcement action as Tesco Bank failed to proactively manage its cyber risk which subsequently caused harm to customers. He said:

"The fine the FCA imposed on Tesco Bank today reflects the fact that the FCA has no tolerance for banks that fail to protect customers from foreseeable risks. In this case, the attack was the subject of a very specific warning that Tesco Bank did not properly address until after the attack started. This was too little, too late. Customers should not have been exposed to the risk at all.

Banks must ensure that their financial crime systems and the individuals who design and operate them work to substantially reduce the risk of such attacks occurring in the first place. The standard is one of resilience, reducing the risk of a successful cyber attack occurring in the first place, not only reacting to an attack. Subsequently, Tesco Bank has strengthened its controls with the object of preventing this type of incident from being repeated."[10]

Equifax

Equifax is a credit reference agency and data, analytics and technology business whose business model is dependent on holding and analysing large volumes of data. In 2017, Equifax's parent company, Equifax Inc, was subject to a significant cyber security incident resulting in unauthorised access to personal data including data belonging to13.8 million customers in the UK. The incident affected UK customers because Equifax had transferred UK consumer data to its parent company for processing two Equifax products.

In its Final Notice, published on 13 October 2023, the FCA reiterated that regulated firms need to have effective cyber security arrangements to protect the personal data they hold, and that where the processing of data is outsourced, it must exercise appropriate oversight over outsourced functions. In this case, Equifax failed to put in place an appropriate framework for monitoring and managing the security of UK customer data where it had been outsourced internally. Notably, prior to the cyber incident, Equifax was aware of serious security patching problems at Equifax Inc but failed to take action in response.

The FCA also found that following the cybersecurity incident Equifax failed to pay due regard to the interest of customers and treat them fairly. Equifax's outsourcing arrangements with its parent resulted in delays in obtaining information needed to notify affected UK customers. In addition, Equifax exposed customers to unfair treatment by ceasing quality assurance checks on its complaints handling processes and by publishing several public statements about the impact of the incident on UK consumers which did not meet the FCA's requirements.

8 A firm must conduct its business with due skill, care and diligence.
9 https://www.fca.org.uk/news/press-releases/fca-fines-tesco-bank-failures-2016-cyber-attack
10 https://www.fca.org.uk/news/press-releases/fca-fines-tesco-bank-failures-2016-cyber-attack

The FCA held that Equifax breached Principle 3 (as it failed to take reasonable care to organise and control its affairs), Principle 6 (as it failed to pay due regard to the interests of its customers and treat them fairly), and Principle 7 (as it failed to pay due regard to the information needs of consumers and communicate information to them in a way which is clear, fair and not misleading).

Operational resilience decisions

In May 2019, R. Raphael & Sons plc ("**Raphaels**") was fined a total of £1.89 million by the FCA and PRA for failing to have processes to understand the business continuity arrangements of outsourced service providers, particularly in the event of a disruptive event. The Regulators' investigations arose after a technology incident occurred at an outsourced processor which led to operational disruption for customers over an eight hour period. On publishing its findings, Sam Woods, Deputy Governor for Prudential Regulation and Chief Executive Officer of the PRA, said:

"Firms' ability to manage outsourcing of any critical activities is a vital part of maintaining their safety and soundness. Such outsourcing is an important part of a firm's operational resilience, and particularly so in the case of Raphaels given the level of reliance on outsourcing in its business model."[11]

Similarly, in December 2022, the FCA and PRA fined TSB Bank plc ("**TSB**") a total of £48.7 million for operational risk management and governance failures, including management of outsourcing risks relating to the bank's IT upgrade programme. In this case, enforcement action was taken after technical failures in TSB's IT system resulted in customers being unable to access banking services.

What should firms do to minimise the regulatory risks relating to a cyber incident?

As highlighted above, to comply with the Regulators' expectations in relation to cyber security, firms must implement robust systems and controls that are designed to manage the cyber security risks they may face.

In particular, they must ensure that they invest sufficient resources in minimising the risk of a cyber incident occurring including through written policies and processes, the implementation of cyber security software, appointing individuals to manage security risk, and by conducting wider employee training on cyber risks and good cyber hygiene.

Where firms outsource certain functions, and therefore hand over customer data to group companies and/or third parties, they must continue to have oversight of these functions and ensure that the outsourced entity, whether internal or external, adequately manages cyber and other risks. As highlighted by the Equifax decision, firms remain responsible for outsourced functions, and may be held accountable by the regulator for failures in their systems and controls which lead to cyber issues.

11 https://www.fca.org.uk/news/press-releases/fca-and-pra-jointly-fine-raphaels-bank-1-89-million-outsourcing-failings

Firms should also formulate a plan of action in the event that a cyber incident occurs. This should include:

- identifying a core incident response team, and also considering the engagement of external cyber security specialists and/or legal counsel;
- setting out what steps may need to be taken in response to an event, including to secure systems, to implement business continuity arrangements and to ensure effective communications with customers and suppliers;
- details of notifications that may need to be made, including to:
  - the ICO;
  - the Regulators and/or other regulators such as those overseas;
  - other bodies such as the National Cyber Security Centre, the National Crime Agency and/or Action Fraud; and
  - affected individuals, in respect of high-risk personal data breaches;
- details of other steps that may need to be taken, for example, to comply with the Listing Rules if it is a listed company, and/or to ensure the Board of the Directors comply with their Directors' Duties under Section 172 of the Companies Act 2006.

In planning for notifications and other actions, the firm must be aware of key deadlines. For example, a notifiable breach must be reported to the ICO without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. In addition, firms should give thought to the coordination of notifications, to enable consistent reporting and to make sure that regulators are kept equally briefed where possible.

Taking proactive steps to manage cyber risk should both reduce the risk of a cyber incident occurring, and minimise the impact, particularly for customers, if an event does occur. In turn, these measures should enable a firm to demonstrate to its regulators that it has implemented appropriate systems and controls to manage risk, in accordance with its regulatory obligations, thereby reducing the risk of enforcement action.

CLIFFORD

CHANCE

AUTHORS

Samantha Ward
Partner
London
T: +44 207006 8546
E: samantha.ward@cliffordchance.com

Eleanor Matthews
Senior Associate
London
T: +44 207006 2740
E: eleanor.matthews@cliffordchance.com

2311-008554