Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

UK Financial Orgs Could Face Cyber Enforcement On 2 Fronts

By **Rob Dedman and Kim Roberts** (July 29, 2019, 4:46 PM EDT)


Rob Dedman


Kim Roberts

The Financial Conduct Authority recently revealed the number of cyberincidents reported to it had soared by 1086% in 2018. Last year, 819 cyberincidents were reported compared to 68 in 2017, according to a freedom of information request from RSM International.

The increase of reports may seem hefty but the implementation of EU General Data Protection Regulation regime in May 2018 overhauled the entire landscape for reporting cyber-related incidents. There has been a general uptick in reporting of data breaches last year. The Information Commissioner's Office said there had been a significant increase in reporting both in the period before and after the implementation of GDPR.

In June 2018, 1,792 personal data breaches were notified to the ICO, a 173% rise on the 657 reports received in May 2018, which is an almost five-fold increase to the April figures, when there were just 367 notifications. However, the four-figure increase in reports to the FCA illustrates the ever-increasing importance that financial services organizations are now putting on data issues as well as the particularities and challenges they face in the sector.

The Findings

The RSM-obtained figures make for interesting reading. Retail banking contributed the bulk of reports (59%) with wholesale financial markets (16%) taking second spot. Technology infrastructure in retail banks, which hold the data of millions of individual consumers, has historically been an area of significant interest for the regulators. They have regularly expressed concern about the potential detriment to consumers and potential risks to financial stability posed by a combination of legacy IT estates and the increase in sophistication of cyberattacks.

The other sectors (retail investments, retail lending, general insurance and protection, pensions and retirement income and investment management) contributed between 4% and 6% each.

The most common "root cause" of the report was third-party failure, accounting for more than a fifth (21%) of reports. This finding highlights one of the trickiest aspects of cyberrisk and data management:

the supply chain and the impact of the use of external providers which receive personal data in connection with the provision of services.

Many financial institutions have been focused on implementing, as best they can, watertight internal processes and procedures as well as putting robust contractual mechanisms in place with such third parties, as the GDPR requires. However, it is considerably harder to ensure that third parties always follow such standards, and to manage the consequential risk if the data management practices of external providers are substandard.

From an enforcement perspective, regulators are clear that the regulated institution must take responsibility for its outsource providers, and will normally regard any failure of outsourcing to be a failure by the regulated firm concerned. Likewise, they have been clear that senior managers cannot outsource their own personal responsibility for failings in the areas they are responsible for.

The next most common "root causes" were hardware/software issues (19%) and change management (18%), with 11%, or 93 reports resulting from a cyberattack. Within the category of cyberattacks, phishing/credential compromise accounted for 52% of cases, ransomware (20%), malicious code (17%) and DDOS (denial of service) (11%).

While this will be an encouraging statistic for IT departments, it is a pertinent reminder that not all cyberincidents or breaches are a result of sinister activity or can be mitigated against by improving internal processes. Financial institutions need to have appropriate governance and processes in place to minimize issues ranging from human error to internal foul play, and capacity management to personnel changes.

A Costly Experience

The increased reporting of data breaches to the FCA also puts an intensified regulatory spotlight on financial institutions.

The U.K.'s data protection authority, the ICO, has been regarded as the responsible regulator for privacy and data breach issues. The ICO has, until very recently, been relatively reserved in its enforcement, and up until this month has been enforcing under the predecessor data protection legislation.

However, it gave notice of its intention to fine British Airways on July 8 a record-breaking sum of £183 million for the data breach to BA's booking website and app, its first fine levied under the GDPR. Soon after, on July 10, it notified of its intention to fine Marriott International £99 million for its data breach. In the financial services sector, the prospect of an ICO fine would be bad enough, but financial institutions can face the double whammy of enforcement by the ICO and the FCA for data breaches.

The two regulators established a memorandum of understanding in 2014, and updated it in February 2019. The memorandum sets out how they will coordinate their activities. The ICO and FCA have publicity stated that, while the ICO will focus on the GDPR, the FCA will consider obligations under GDPR under their rules, specifically the senior management arrangements, systems and controls module on maintaining and improving technology and cyberresilience systems and controls.

While the FCA has not pursued many cases, last year saw the headline-grabbing case of Tesco Personal Finance being hit with a £16.4 million fine for "failing to exercise due skill, care and diligence" in

protecting its customer against a cyberbreach in November 2016 that saw £2.26 million (€2.59 million) swiped from current accounts.

An increase in reports could well mean an increase in investigations in the financial services sector, with firms potentially having to fight on two fronts. And as a result, the risk of simultaneous enforcement action by the ICO and the FCA remains high. Senior managers are bound to come under increased scrutiny for their role in any failings identified by the FCA. While the regulators recognize that this is not a zero-failure regime, the prospect of long investigations and heavy fines means that cyberrisk has rightfully taken its place among the most significant operational and regulatory risks for financial services firms.

Rob Dedman is a partner and Kim Roberts is counsel at King & Spalding LLP.