Feature

KEY POINTS

- As financial institutions experience the increased costs of cyberattacks and data breaches, data protection becomes more important to financial firms and regulators.
- Recent regulatory developments in multiple jurisdictions have underscored the conceptual alignment of the data protection legal framework and financial regulation.
- Practitioners should keep an eye on cross-cutting initiatives that allow financial regulators to work closely with data protection regulators and share information for more effective regulation.

Authors Akira Kumaki, Stuart Levi, Eve-Christie Vermynck and Shannon Togawa Mercer

Regulatory co-operation: data protection and financial regulation

In the financial services industry, the monetary and reputational costs of data breaches can be enormous, both to financial institutions and to the financial system itself. As the rate of breaches or incidents increases over time, financial regulators in some jurisdictions have recognised the need to collaborate with their data protection authorities in order to align capabilities, rationalise enforcement and better prepare for hybrid threats. Additionally, in order to effectively regulate global institutions, financial regulators need to share data across borders without hindrance. This article describes recent developments in this space.

Cybersecurity and data protection are top priorities for the global financial services industry. The number of cyberattacks and data breaches has steadily increased, seeing a sharp rise more recently in certain countries. The financial services sector in the UK reported 145[1] breaches in 2018, more than five times the number in 2017. In the US, the overall number of data breaches seems to have decreased, notwithstanding a reported 126% increase in the number of records that contained sensitive personally identifiable information.[2] In all cases, the potential financial and reputational cost of any one incident is dangerously high. Mark Carney, the governor of the Bank of England, recently stated that the average cost of cybercrime to financial services firms has increased by 40% over the last three years.[3] Financial firms have recognised how critical data and cybersecurity are to their operations and have worked to stay ahead of the threat; major firms have hired chief information security officers (CISOs) and actively work to develop technology to combat constant and increasingly complex attacks from hackers. These threats have not gone unnoticed by regulators and the need for collaboration across borders in order to stymie cybercrime has never been more apparent.

THE NEED FOR INCREASED CO-OPERATION BETWEEN FINANCIAL AND DATA PROTECTION REGULATORS

As financial regulation becomes more focused on data security, and data protection regulation becomes more prominent on the international stage, there are questions about whether data protection regulations and more conventional financial regulations will clash. In other words, will data protection laws such as the General Data Protection Regulation (2016/679) (GDPR) get in the way of the productive and collaborative data sharing required for cross-border financial regulation? Not necessarily.

In fact, recent regulatory developments in Europe, Japan and the US have underscored the conceptual alignment of the data protection legal framework and industry-specific regulations, such as those applied to the financial sector. Strong data management and cybersecurity policies both protect consumers and investors, and have the potential to create long-term efficiency for financial institutions. Both regimes have an interest in treating consumers or data subjects fairly and consider greater consumer control over personal data to be essential. These common themes can be successfully pursued through tighter regulatory requirements placed on companies (acting as controllers over their customers' personal data from a data protection law standpoint and as regulated entities under applicable financial regulations) concerning the use of customer data, increased customer agency and transparency. From the perspective of financial institutions such as banks, effective data management is key in operational strategy to provide efficient and secure service to clients. The efficiency of these institutions' strategy will be tested through the implementation of their data protection and cybersecurity policies and safeguards. Accordingly, co-operation between industry-specific regulatory authorities and supervisory authorities within the GDPR framework is encouraged at both EU and EU member-state levels.

In the US, the Financial Services Information Sharing and Analysis Center (FS-ISAC) was created in response to the 1998 US Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators and was updated in 2003 by Homeland Security Presidential Decision Directive 7 (which establishes a national policy for Federal departments and agencies to identify and prioritise critical infrastructure and to protect them from terrorist attacks). Today, FS-ISAC connects nearly 7,000 member financial institutions in more than 70 jurisdictions, including banks, investment firms, insurance companies and payment processors. Amongst other functions, the group disseminates critical cyber intelligence and allows members to stay updated through alerts, indicators, member insights, threat assessments and analysis. The following examples will demonstrate the importance of co-ordination between financial and data protection regulations in a number of jurisdictions, including the UK, Japan and the US, and showcase concerted efforts in the EU to create a GDPR-compliant structure for a co-operative system of regulations.

CO-OPERATION BETWEEN DATA PROTECTION AUTHORITIES AND FINANCIAL REGULATORS

On 18 February 2019, the Information Commission Officer (ICO) – the national data protection authority in the UK acting as an independent regulatory office – and the Financial Conduct Authority (FCA) – an independent financial regulatory body in the UK – published a Memorandum of Understanding (MoU)[4] establishing a framework for co-operation, co-ordination and information

Biog box

Stuart Levi is a partner/co-head in the Intellectual Property and Technology Group in New York and has a diverse practice that includes outsourcing transactions, technology and intellectual property licensing, fintech and blockchain matters and privacy and cybersecurity advice, among others. Email: stuart.levi@skadden.com

Eve-Christie Vermynck is counsel in London and focuses her practice on intellectual property, technology, cybersecurity and data protection matters. Email: eve-christie.vermynck@skadden.com

sharing between the two regulatory bodies. While the MoU does not create legally binding obligations, it does memorialise several items of mutual understanding: the parties' willingness to alert each other to potential breaches of the law as they pertain to the operations of each other; the mandate to exchange information as necessary, the ability to request information from each other, collaboration in policymaking, an agreed-upon framework for co-operation and responsibility sharing in investigations and enforcement (although no mention is made about rationalising penalties between the regulatory bodies) and measures for the maintenance of confidentiality.

In essence, the ICO remains in charge of implementing the GDPR and the UK Data Protection Act of 2018, and the FCA continues to monitor the conduct of financial services firms. But the FCA also will now consider data protection in its industry-specific requirements, and it will collaborate with the ICO in order to best handle hybrid regulatory cases and necessary information sharing. This model is the product of an acute recognition of its necessity. In a joint publication in February 2018, the FCA and the ICO signalled the FCA's increased focus on cybersecurity and data protection issues.[5] In 2018, the FCA fined Tesco Personal Finance plc £16.4m[6] for breaches related to a cyberattack in 2016, including failure to take appropriate action to prevent foreseeable risk of fraud and failure to respond to the cyberattack with "sufficient rigour, skill and urgency".[7] Further to that focus, on 8 March 2019, the FCA published a collection of practices and experiences – "cyber security industry insights" – collected from 175 firms in different financial sectors comprising one of the FCA's cyber co-ordination groups.[8]

While the MoU is still in its early days, it brings into relief a key area of common interest and necessary collaboration between the ICO and the FCA: consumer protection. Additionally, the MoU's operational success will be worth keeping an eye on; if successful, it could lead to key insights into co-operation in practice, and potentially set trends for other national regulatory authorities both in the EU and outside of the EU.

The FCA also is working across borders to strengthen cybersecurity in the financial sector. On 13 June 2019, the Monetary Authority of Singapore (MAS), the Bank of England and the FCA announced the intention to enter into a MoU increasing collaboration to strengthen cybersecurity in their respective financial sectors. This plan will include developing more effective information sharing channels.[9]

Although not directly applicable to the financial services industry, the US Department of Justice (DOJ) released a white paper in 2015 regarding whether the Stored Communications Act[10] restricts network operators from voluntarily sharing aggregated data with the government that would promote the protection of information systems.[11] Importantly, the DOJ stated that "improved information sharing is a critical component of bolstering public and private network owners' and operators' capacity to protect their networks against evolving and increasingly sophisticated cyberthreats". This is not to say that privacy concerns have no place within information sharing. As the DOJ noted, such sharing "must occur without contravening federal law or the protections afforded individual privacy and civil liberties".

In Japan, the Personal Information Protection Commission (PIPC) was established in 2016 to implement and strengthen co-operation across authorities with respect to personal information protection. The Japanese Personal Information Protection Law (PIPL) was enacted in 2003 for the purpose of protecting the individual's personal information in all industrial areas, however, before the establishment of PIPC, personal information protection under the PIPL was assigned to the relevant authority supervising individual industrial areas. For instance, the Japanese Financial Services Agency was mainly responsible for personal data protection with regard to banks and other financial players. The Japanese government realised that the harmonised and integrated approach would be important, not only for "protection", but also "utilisation" of the personal information, and, therefore, the government could use resources more effectively and efficiently with a clear and shared goal. The Japanese government therefore established PIPC to take responsibility for a cross-industry approach. Under the current regime, PIPC leads the personal data protection regime overall and co-operates with each authority for each industry – recognising that each authority has supervising power over, knowledge of and relationships with companies – to implement and monitor personal data protection effectively. In addition, PIPC is expected to lead discussions about the utilisation of personal information from each industry.

PROMOTING CONTINUED CROSS-BORDER CO-OPERATION WITHIN THE GDPR FRAMEWORK

At the supranational level, the European Data Protection Board (EDPB),[12] the independent advisory body bringing together all EU national data protection authorities and promoting consistent application of data protection rules in the EU through binding guidance, has made a concerted effort to ensure the continued information exchange between financial regulatory bodies within and outside of the European Economic Area (EEA). Converging integrated global markets have created increasingly integrated global financial institutions, requiring data sharing between national authorities in order to better protect consumers, monitor market integrity, monitor prudential risk and, in some cases, promote competition. The EDPB embraced this macro-economic reality by issuing opinion 4/2019, the first of its kind, to create an ad-hoc framework to enable the continued flow of information specific to this industry within the GDPR framework.

Under the GDPR, data cannot be transferred to a non-EEA country that has not been granted an adequacy decision by the EU Commission in light of its applicable data protection legal framework unless appropriate safeguards are in place. Opinion 4/2019 delivered on 12 February 2019, approved a draft Administrative Arrangement (AA) created by the European Securities and Markets Authority (ESMA), the EEA financial supervisory authorities National Competent Authorities (NCAs) and the International Organisation for Securities Commission, to enable the transfer of data between (and co-operation among) EEA and non-EEA financial supervisory authorities on matters of securities regulation.

The AA is designed to be used by all market regulators in the EEA and submitted to any given national data protection authority with a request for authorisation in the case of a necessary data transfer outside of the

Feature

Biog box

Akira Kumaki is a *bengoshi* partner in Tokyo who concentrates on mergers and acquisitions, private equity, securities and other general corporate matters. Email: akira.kumaki@skadden.com

Shannon Togawa Mercer is an associate in London who concentrates on a variety of cross-border corporate transactions, with a particular focus on data protection and cybersecurity matters. Email: shannon.mercer@skadden.com

EEA. The AA itself lays out the basic legal principles and requirements for a transfer with appropriate safeguards in alignment with the GDPR, including the principles of purpose limitation, data minimisation, data quality, proportionality, transparency, data retention, security and confidentiality measures as well as restrictions on onward transfers. Each competent national data protection authority will monitor the implementation of these AAs.

The EDPB's dedication to rationalising the needs of financial regulation and data protection regulations does not stop here. The EDPB has issued guidance on the EU Payment Services Directive 2 (2015/2366) (PSD2) data requirements and the GDPR, particularly the definition of consent for access to data, processing and retention under both regimes.[13] The PSD2 remains a part of the EDPB's 2019-20 work program, signalling the body's continued focus on rationalising regulatory regimes to best meet data protection needs within the GDPR framework.

The demand to co-ordinate and rationalise data protection and cybersecurity governance has manifested across other institutions. On 10 April 2019, the Joint Committee of European Supervisory Authorities – a forum for collaboration between financial system authorities, the European Banking Authority, ESMA, and the European Insurance and Occupational Pensions Authority – published advice[14] in response to the European Commission's 2018 FinTech Action plan, suggesting, among other things, that streamlining breach or incident reporting of cross-sectoral frameworks (such as the Network and Information Systems Directive, the GDPR and general requirements under the Central Securities Depository Regulation) for financial services will promote operational resilience. Recognising that each incident reporting mechanism has independently valuable purposes, the proposal suggests that the European Commission keep each regime in place while also creating clearer guidelines and developing harmonised templates and taxonomies across reporting requirements. This push for further co-ordination and harmonisation is yet another example of work being done at the EU-level to create more comprehensive and co-ordinated regimes.

The potential conflicts between financial regulations and data protection regulations such as the GDPR are not intractable.

CO-OPERATIVE FRAMEWORKS ARE (LIKELY) THE FUTURE OF DATA PROTECTION

The FCA and the ICO perhaps put it best in their 2018 joint GDPR update press release:

> "The requirement to treat customers fairly is also central to both data protection law and the current financial services regulatory framework."[15]

While the potential for conflict exists, the reality is that financial and data protection regulators should recognise, and in many cases already have recognised, the necessary synergy between their operations to promote the development of the financial industry while ensuring that adequate safeguards are in place for the protection of personal data. Financial companies constantly work across borders and with large volumes of customer data. The pressure to safeguard this data is critical in light of the frequency and increased level of complexity of cyberattacks, demonstrating the overlap between data protection and financial security. These models for legal co-operation, built with the GDPR framework in mind, contribute to developing a new framework for handling technological threats to the financial sector and may soon be leveraged by other industries. ■

All of the authors are attorneys at Skadden, Arps, Slate, Meagher and Flom. (*Skadden Arps Law Office, registered associated office of Skadden Arps Foreign Law Office)

1 *Financial Times*, 'Cyber Attacks on Financial Services Sector Rise Fivefold in 2018', https://www.ft.com/content/6a2d9d76-3692-11e9-bd3a-8b2a211d90d5.

2 Identity Theft Resource Center, '2018 End-of-Year Data Breach Report', https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/.

3 Bank of England, 'Monetary Authority of Singapore and UK financial authorities announce collaboration on cyber security', (13 June 2019), https://www.bankofengland.co.uk/-/media/boe/files/news/2019/june/mas-and-uk-financial-authorities-announce-collaboration-on-cyber-security.pdf.

4 Information Commissioners Office, 'Memorandum of Understanding between the Information Commissioner and the Financial Conduct Authority', https://ico.org.uk/media/2614342/financial-conduct-authority-ico-mou.pdf.

5 Financial Conduct Authority, 'FCA and ICO publish joint update on GDPR', (2 August 2018), https://www.fca.org.uk/news/statements/fca-and-ico-publish-joint-update-gdpr.

6 Note that the fine was the result of a settlement qualifying Tesco Bank for a 30% discount under the FCA's settlement procedures. The total fine would have been £23,428,500 without the early settlement.

7 Financial Conduct Authority, 'Final Notice' (1 October 2018), https://www.fca.org.uk/publication/final-notices/tesco-personal-finance-plc-2018.pdf.

8 Financial Conduct Authority, 'Cyber security – industry insights', (March 2019), https://www.fca.org.uk/publication/research/cyber-security-industry-insights.pdf.

9 *Supra* note 3.

10 18 U.S.C. § 2701 et seq.

11 United States Department of Justice, 'White Paper: Sharing Cyberthreat Information Under 18 U.S.C. § 2702(a)(3)', (9 May 2014), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/03/26/guidance-for-ecpa-issue-5-9-2014.pdf.

12 Established by the GDPR but preceded by the Art 29 Working Party, which filled a similar function but with less authority under the EU Data Protection Directive.

13 European Data Protection Board, 'EDPB Letter On Data Protection Issues in PSD2, Including Silent Party Data and Consent' (5 July 2018), https://edpb.europa.eu/sites/edpb/files/files/news/psd2_letter_en.pdf.

14 European Supervisory Committee, 'Joint Committee of European Supervisory Authorities Joint Advice on Information and Communication Technology Risk Management and Cybersecurity', (4 October 2019), https://esas-joint-committee.europa.eu/Pages/News/ESAs-publish-Joint-Advice-on-Information-and-Communication-Technology-risk-management-and-cybersecurity.aspx.

15 *Supra* note 6.