



HERBERT  
SMITH  
FREEHILLS

# THE **DATA** GAME

2019 GLOBAL BANK REVIEW



# Contents

- 05 Welcome

---
- 06 Big data: where are we now?

---
- 10 Regulatory data: arrows for the quiver?

---
- 12 Global regulatory update

---
- 22 Are you prepared? The board's role in crisis management

---
- 28 Virtual banks: the case for clearer regulatory guidance on outsourcing

---
- 34 Data vs "gut instinct": analytics in dispute resolution

---
- 38 Regulatory creep or convergence? Competition law authorities as financial services regulators

---
- 42 Data and cyber perils: personal exposure and inadequate insurance

---
- 46 Away from prying eyes: data security in international dispute resolution

---
- 50 IBOR transition: a data challenge

---
- 54 The emergence of the "super-regulator": the lasting legacy of the Australian Banking Royal Commission

---



# Welcome

Welcome to *The Data Game*, the third edition of our Global Bank Review. This is a publication by our Global Banks Sector Group, which brings together people at Herbert Smith Freehills from around the major financial centres of the world who live and breathe banks.

The rapid growth of data is unquestionably one of the most significant developments in the banking sector. Data has, quite literally, the ability to change lives. The exponential growth in data and its uses are already making their mark. The possibilities opened up by big data analytics, artificial intelligence and other related issues are reshaping the industry. That being the case, we are still only at the beginning of the data journey and its impact in the next decade or two will be even more profound.

The changes that data and technology are driving include the emergence of virtual banks. We examine banks in the cloud and the regulatory issues associated with the protection of customer data.

Within this world of new possibilities also exists a world of new challenges. *The Data Game* also explores the role of the board and the new operational risks associated with data and cyber incidents. Approaches vary in this area, and the work of regulators, as well as what has happened in practice, suggest that in many cases more needs to be done by boards to meet these challenges. The increased risks also raise interesting questions in relation to corporate and personal insurance, another important topic which we have covered.

Boards are not the only ones dealing with the brave new world of big data. Regulators have also had to respond and adapt to the new data environment. Banks have felt the effects of that adaptation in a number of ways. The data requests made by bank regulators have increased significantly and show no signs of abating. This is putting increased operational and compliance burdens on banks which are already feeling the effects of more severe regulation in other areas. Regulators are also becoming more thoughtful about their use of the data supplied by banks, in analysing bank and employee behaviour, again presenting fresh challenges.

The increased volume of requests and different uses to which data is put are the only ways in which regulators are responding. What is also emerging is a revised regulatory landscape addressing the new big data environment. Our global regulatory update covers these changes across the United States, the UK, Greater China, Australia, France, Germany and the UAE.

In this time of unparalleled change, and on behalf of the Global Banks Sector Group, we hope you enjoy reading *The Data Game*.



**Hannah Cassidy**  
Partner, Hong Kong  
T +852 2101 4133  
[hannah.cassidy@hsf.com](mailto:hannah.cassidy@hsf.com)



**Simon Clarke**  
Partner, London  
T +44 20 7466 2508  
[simon.clarke@hsf.com](mailto:simon.clarke@hsf.com)



**Tony Damian**  
Partner, Sydney  
T +61 2 9225 5784  
[tony.damian@hsf.com](mailto:tony.damian@hsf.com)

# Big data: where are we now?

With the rapid growth of big data now unstoppable, financial institutions face an inherent tension between maximising the value of data as an asset and ensuring they remain compliant with growing legal and regulatory obligations.

Over 18 million texts, 188 million emails and 500,000 tweets are currently being sent every minute in 2019.<sup>1</sup> By 2020, it is estimated that 1.7MB of data will be created every second for every person on earth<sup>2</sup> and many industry sectors have begun capitalising on the opportunities that this will bring. The banking sector has long been at the forefront of investing in financial technologies (fintech), and will account for nearly 14% of worldwide big data analytics (BDA) revenue this year.<sup>3</sup> The International Data Corporation (IDC) forecasts worldwide revenue for BDA solutions to reach US\$189 billion this year which will continue to grow to an estimated US\$274 billion by 2022.<sup>4</sup>

Big data can also present operational challenges, with financial institutions often reliant upon legacy IT systems and struggling to implement capabilities to capture and utilise big data effectively. Despite these issues, big data has the potential to enable banks to streamline their businesses, and provide more customer-centric services. Gaining a clearer understanding of the risks and legal framework surrounding big data will aid financial institutions in implementing the appropriate governance structures and strategies to maximise the value of the data they hold.

## What is big data?

In simple terms, big data refers to large and complex datasets. Gartner, a leading IT research and advisory company, defines big data further as data that contains:

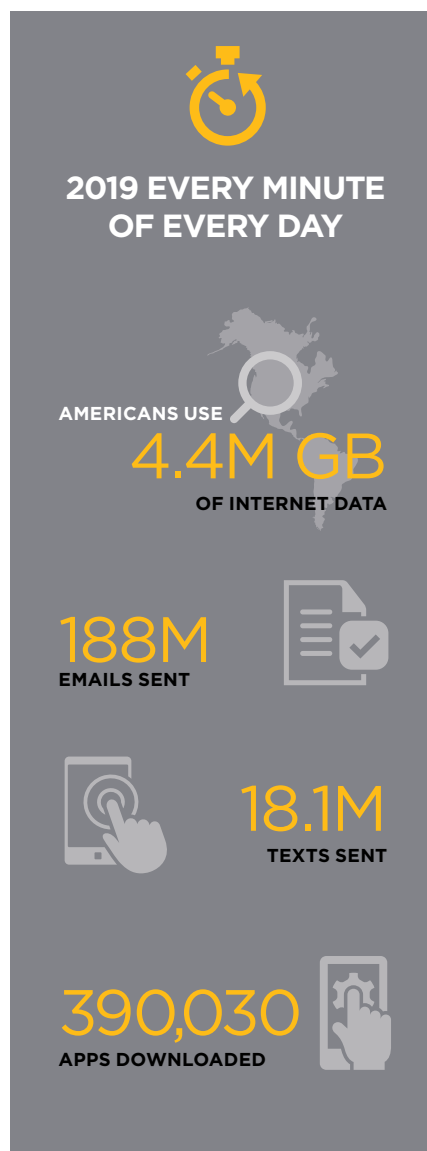
- greater variety (eg text, image, video, sound);
- arriving in increasing volumes; and with
- ever-higher velocity (the fast rate at which the data is received and potentially analysed in real time).

Big data also encompasses the technology by which these aggregated datasets are analysed by software such as machine learning, algorithmic computation and artificial intelligence.

Banks and other financial institutions have access to extensive amounts of data through the use of digital trading platforms. These platforms process millions of trades and transactions daily, and capture customer data through each interaction with the bank (eg products sold, online and mobile transactions and processes used to deliver those products).

## Moving in the right direction

Today, banks employ BDA solutions for a range of business needs, including the detection and prevention of fraud; customer and call centre efficiencies; customer profiling, targeting and optimisation of cross-selling, and risk assessments. In a report carried out in 2016, Central Banking revealed that work in big data could be





considered a mainstream activity for central banks, with over half of their survey respondents working on a big data project.<sup>5</sup>

In 2017, JPMorgan Chase introduced the LOXM equity trading algorithm, an AI program that analyses data from billions of historic trades in order to execute future trades with increased speed and optimal prices. In his annual letter to shareholders this year, Jamie Dimon, the chairman and CEO, also introduced a new AI project, DeepX, which “leverages machine learning to assist [with] equities algorithms globally to execute transactions across 1,300 stocks a day”<sup>6</sup>.

Citibank has also announced that it is investing in big data technologies. Citi’s Treasury and Trade Solutions entered into a strategic partnership with Feedzai, a data science company that uses real-time machine learning and predictive modelling to analyse big data to pinpoint fraudulent behaviour. Citibank will integrate Feedzai’s transaction monitoring platform into its own proprietary services and platform to increase its risk management for payment transactions<sup>7</sup>.

### The legal framework

Despite the myriad of potential benefits that harnessing big data can bring, banks and financial institutions must consider the legal framework for big data to ensure they remain compliant with their obligations. Not only are fines for non-compliance potentially huge (under the General Data Protection Regulation (GDPR), organisations can be fined up to €20 million, or 4% annual global turnover, whichever is greater), reputational damage stemming from a misuse of customer data can be severe.

Ownership of data, from a legal standpoint, is a difficult subject matter. The current legal position in the UK is that there are no ownership rights (ie property rights) in raw data. From an intellectual property (IP) perspective, it is also difficult to ensure comprehensive protection. This perhaps results from the philosophy which underpins IP rights (IPR), which is to create monopolies to reward and incentivise creative effort, and protect against unfair advantage being taken of someone else’s creation. Therefore, as data are simply pieces of information, there is no moral incentive to restrict access or use.

However, whilst there are no ownership rights in data, there are extensive rights and obligations that arise in relation to data. These rights and obligations, which mainly arise through regulation are constantly developing. One interesting development relates to the interaction between data and competition law. The competition authorities are taking an increasing interest in data and its potential to be collected and/or used to anti-competitive effect. For example, regulators are looking at one potential type of abuse of dominance where access to a particular data set is essential to enable competition in a downstream or adjacent market. In addition, data sharing arrangements which foreclose competitors who are not permitted similar access are also at risk of regulatory scrutiny.

### Ongoing regulatory scrutiny

At the forefront of regulatory scrutiny is the Australian Competition and Consumer Commission (ACCC) which is leading in the development and oversight of a new “consumer data right” (CDR) scheme and has recently published a report into digital platforms. Both of these projects have involved collaboration with the Office of the Australian Information Commissioner (OAIC).

The CDR scheme is being launched in the banking sector (where it is also known as “open banking”) and is designed to facilitate competition and product innovation by allowing consumers to access their data held by banks for potential sharing with competitors. The regulatory framework will include legislation, ACCC rules, OAIC guidelines, data standards and an accreditation scheme for fintechs and others wishing to have access to CDR data. An ACCC open banking survey found that of 60 respondents, 56 were interested in becoming accredited.

The ACCC’s digital platforms inquiry proposed various reforms relating to competition and consumer law, alongside significant reforms to take Australian privacy law further in the direction of the EU’s General Data Protection Regulation EU’s GDPR (2016/679/EU), including in relation to consent and penalties. Most of those reforms – if implemented – would not be limited to digital platforms and so the banking sector would also be affected.



## 2019 EVERY MINUTE OF EVERY DAY

NETFLIX STREAMS

694,444



HRS OF VIDEO



INSTAGRAM USERS POST

277,777

STORIES

YOUTUBE STREAMS

4.5M



VIDEOS



TWITTER USERS SEND

511,200

TWEETS

SKYPE USERS MAKE

231,840



CALLS



AIRBNB BOOKS

1,389

RESERVATIONS

UBER USERS TAKE

9,772



RIDES



TINDER USERS SWIPE

1.4M

TIMES

GOOGLE CONDUCTS

4.5M



SEARCHES



Another key focus of regulatory scrutiny for the past couple of years has been privacy, and in particular, the GDPR. By now, financial institutions will be familiar with the GDPR in the EU (and beyond). The UK's Information Commissioner's Office has stressed that big data is one of its key strategic focus areas,<sup>8</sup> and to the extent that the data being processed contains the personal data of an EU individual, banks will have to ensure that their activities comply with their obligations under the GDPR.

Given the recent proliferation of privacy laws around the world, including ever closer steps towards a US federal privacy law, it is clear that privacy is not just a European issue, creating global compliance challenges for multinational organisations.

### Organisational challenges

Of key importance under both privacy and cybersecurity laws are the obligations for organisations to implement appropriate technical and organisational measures to ensure the security of data, which could involve a mix of administrative controls (eg employee training and internal policies), technical controls (eg firewalls and encryption methods) and physical controls (eg appropriate authorisation for access to the data). However, whilst securing data can present a challenge, it is important to note that, for most organisations, there is a real commercial incentive to secure their data.

Another challenge currently facing organisations looking to use BDA to exploit their data commercially is the potential impact on the organisation's brand and reputation. There is a groundswell of movement looking at the ethics behind data processing and organisations should not be afraid to consider whether or not they should do something, just because they can. The recent Federal Trade Commission (FTC) settlement with Facebook included an obligation to create an independent privacy committee, and the concept of having a data ethics committee within organisations is gaining traction. Technology is making the job of BDA easier but the focus is now turning towards the use of technology and BDA as a force for good.

**With the potential to be one of the most valuable assets within an organisation, it is important to have appropriate security in place to protect that asset from a commercial perspective, aside from the regulatory requirements.**

### Looking forward

As well as focusing on complying with legal obligations, banks should continue to invest in upgrading legacy IT frameworks and internal governance systems to ensure data is being stored and employed coherently across the business. Not only will this help banks in assessing security risks and complying with legal obligations, but also in identifying what data a bank holds to help drive decision making at the appropriate levels.

Big data and technological advancements such as machine learning and AI, will only increase the ways in which banks can capitalise on their data, and could create competitive advantage against the influx of new financial services providers. However, with the focus of regulators and legislators across the world being trained on data, and privacy in particular, banks also need to ensure that they have the appropriate controls and legal protections in place to ensure that they can mitigate the risks that the use of big data can bring.



**Miriam Everett**  
Partner, London  
T +44 20 7466 2378  
[miriam.everett@hsf.com](mailto:miriam.everett@hsf.com)



**Kaman Tsoi**  
Special Counsel, Melbourne  
T +61 3 9288 1336  
[kaman.tsoi@hsf.com](mailto:kaman.tsoi@hsf.com)



**Erin Hwang**  
Associate, London  
T +44 20 7466 6404  
[erin.hwang@hsf.com](mailto:erin.hwang@hsf.com)

1. DOMO, Data Never Sleeps 7.0, [www.domo.com/learn/data-never-sleeps-7](http://www.domo.com/learn/data-never-sleeps-7)
2. DOMO, Data Never Sleeps 6.0, [www.domo.com/solution/data-never-sleeps-6](http://www.domo.com/solution/data-never-sleeps-6)
3. IDC, Worldwide Semiannual Big Data and Analytics Spending Guide 2018H1
4. IDC, Worldwide Semiannual Big Data and Analytics Spending Guide 2019
5. Central Banking, Big data in central banking: 2016 survey, November 2016, [www.centralbanking.com/central-banking-journal/feature/2474825/big-data-in-central-banking-2016-survey](http://www.centralbanking.com/central-banking-journal/feature/2474825/big-data-in-central-banking-2016-survey)
6. Security Week, With \$600 million cybersecurity budget, JPMorgan Chief Endorses AI and Cloud, [www.securityweek.com/600-million-cybersecurity-budget-jpmorgan-chief-endorses-ai-and-cloud](http://www.securityweek.com/600-million-cybersecurity-budget-jpmorgan-chief-endorses-ai-and-cloud)
7. Citi Press Room, Citi Partners with Feedzai to Provide Machine Learning Payment Solutions, [www.citibank.com/tts/about/press/2018/2018-1219.html](http://www.citibank.com/tts/about/press/2018/2018-1219.html)
8. Information Commissioner's Office, Technology Strategy 2018-2021, [www.ico.org.uk/media/2258299/ico-technology-strategy-2018-2021.pdf](http://www.ico.org.uk/media/2258299/ico-technology-strategy-2018-2021.pdf)

# Regulatory data: arrows for the quiver?

It is clear that banking regulators globally are becoming increasingly more demanding in relation to the volume and type of data provided to them, more sophisticated in their use of that data and more willing to share that data with other regulators, both inside and outside their national borders.

With over 200 regulators in the global banking sector, the powers, approach and priorities of these regulators vary significantly from country to country. However, one common theme which permeates is their hunger for data about the firms and individuals they regulate. This focus on data has already had a significant impact on certain types of enforcement actions, and is likely to significantly affect regulatory reporting mechanisms in the future. Given this, it is crucial that banks and their employees are cognisant of the ways in which regulators are using their data.

## Demand for data

Unsurprisingly given our era of big data, regulators have in recent years started asking for ever increasing volumes of data. In particular, regulators' demand for data has been steadily increasing not only in the context of potential or ongoing enforcement action, but as part of their ongoing "business as usual" supervisory activities. For example, the UK Financial Conduct Authority (FCA) has recently estimated that it receives over 500,000 regulatory submissions annually through its data collection platform, across 120,000 users and 52,000 firms,<sup>1</sup> while both the Dodd-Frank Act in the US and MiFID II across the EU have significantly increased reporting obligations for firms.

Importantly, this "business as usual" data increasingly includes data about the actions of individuals, as banks globally have seen regulators demand the disclosure of an increasing volume of information regarding individual employees who might be potential "rolling bad apples". The Australian Government, for example, appears set to implement by mid-2020 the Banking Royal Commission's recommendation that licensed firms be required to report "serious compliance concerns" regarding individual financial advisers to the Australian Securities and Investments Commission (ASIC) on a quarterly basis. This follows the US example, where broker dealers must upload to the US Financial Industry Regulatory Authority's BrokerCheck database (amongst other things) all customer complaints and firm disciplinary events.

Similarly, in Hong Kong, (as discussed further in our Greater China Global Regulatory Outlook), the Securities and Futures Commission (SFC) now requires the disclosure of all internal investigations of licensed individuals where those investigations take place within six

months prior to, or at any time after, an individual's departure from a firm. The SFC has also recently announced the launch of a key risk indicator (KRI) platform to collect and analyse data from 22 global financial institutions which are considered as systemically important. The surveys cover areas such as conduct risk (for example, the number of instances of certain types of non-compliance, client complaints, internal whistleblowing incidents, internal alerts, disciplinary actions and regulatory involvement need to be disclosed). The first submission of data is required by 31 January 2020 for the reporting period ending 31 December 2019.

Regulators' use of their compulsory information gathering powers in the context of possible enforcement action is often shrouded in secrecy, which can complicate efforts to monitor trends in the use of such powers. However, the information which is publicly reported suggests not only that there has been a general increase in the use of such powers, but also the volume of data being produced in response to their use. The SFC, for example, has in 2019 reported a nearly 20% increase year on year in the number of compulsory requests for information issued to intermediaries regarding their clients' transactions<sup>2</sup>. Further, ASIC Commissioner Cathie Armour has commented publicly that one ASIC investigation of market misconduct involved the review of over 75 million documents and 2.7 million hours of voice recordings.

## Use of data

Banking regulators' increasing demands for reams of data regarding the activities of regulated firms raises two key questions. First, is this data actually useful to regulators? And if so – how do they actually make use of it? The answers to these questions vary significantly across jurisdictions and the contexts in which regulators are seeking to put data to use.

In the context of enforcement, for example, it is clear that taking a data-driven approach has transformed the prosecution of insider dealing offences. Historically, it has been easy to predict the catalysts for insider trading investigations – namely, unusual spikes in the prices of securities shortly prior to the disclosure of material non-public information. However, these sorts of "security based" investigations are generally reactive, in that they rely on (for example) large movements in a market being observed.



In recent years, the US Securities and Exchange Commission's Market Abuse Unit has pioneered a "trader based" approach, under which regulators instead start by analysing market data gathered through surveillance to identify potentially suspicious traders, and patterns of similar trades between groups of traders over a period of time. Once relationships between groups of traders have been identified, regulators will then seek to identify potentially shared sources of inside information which may link the traders. This change in approach, which has been emulated by the SFC and ASIC, has allowed for the identification of insider trading cases which may otherwise have gone undetected due to their comparatively small size.

The jury is still out in relation to the use of data in a number of other areas, with regulators such as the European Securities and Markets Authority (ESMA) noting that efforts to grapple efficiently with data through the use of data analytics is often thwarted by poorly designed report formats and non-machine-readable data. Given this, a number of regulators globally have begun to explore "regtech" and "suptech" solutions, including machine learning and natural language processing, to improve data analysis, while others such as the FCA and Bank of England are exploring ways to automate regulatory reporting processes and streamline the accessibility of data.

### Data sharing

Finally, it is worth noting that while demands for, and the use of, data by regulators is often conceptualised within national borders, regulators are increasingly interconnected through memoranda of understanding and cooperation arrangements which allow for information sharing. During 2018/19, for example, the FCA received approximately 1000 requests for information from overseas counterparts in relation to active investigations. In recent years,

these requests have come from more than 60 countries<sup>3</sup>. Similarly, in 2017/2018 ASIC made 393 requests to international regulators, and received 495 requests, which represented a 19% increase in outgoing requests and 22% increase in incoming requests compared to just two years earlier<sup>4</sup>.

As such, firms should be conscious that the information disclosed to one regulator may well be disclosed to other regulators around the globe, and ensure that a consistent approach to disclosure is taken where appropriate, particularly in the context of self-reports of misconduct.



**Hannah Cassidy**  
Partner, Hong Kong  
T +852 2101 4133  
[hannah.cassidy@hsf.com](mailto:hannah.cassidy@hsf.com)



**Tania Gray**  
Partner, Sydney  
T +61 2 9322 4733  
[tania.gray@hsf.com](mailto:tania.gray@hsf.com)



**Ruth Overington**  
Partner, Melbourne  
T +61 3 9288 1946  
[ruth.overington@hsf.com](mailto:ruth.overington@hsf.com)



**Emily Rumble**  
Associate, Hong Kong  
T +852 2101 4225  
[emily.rumble@hsf.com](mailto:emily.rumble@hsf.com)

1. FCA Press Release, New platform to replace Gabriel and improve the way we collect data from firms, 16 July 2019, [www.fca.org.uk/news/news-stories/new-platform-replace-gabriel-improve-collect-data](http://www.fca.org.uk/news/news-stories/new-platform-replace-gabriel-improve-collect-data)

2. SFC, Quarterly Report April-June 2019, [www.sfc.hk/web/EN/files/ER/Reports/QR/201904-06/EN/2e.%20Enforcement.pdf](http://www.sfc.hk/web/EN/files/ER/Reports/QR/201904-06/EN/2e.%20Enforcement.pdf)

3. FCA, Enforcement annual performance report 2017/18, [www.fca.org.uk/publication/corporate/annual-report-2017-18-enforcement-performance.pdf](http://www.fca.org.uk/publication/corporate/annual-report-2017-18-enforcement-performance.pdf)

4. ASIC, Annual Report 2017-18, <https://download.asic.gov.au/media/4922570/annual-report-2017-18-published-31-october-2018-full.pdf> and ASIC, Annual Report 2015-2016, <https://download.asic.gov.au/media/4058626/asic-annual-report-2015-2016-complete.pdf>

# Global regulatory update

The collection of data is not new—banks have been collecting data for hundreds of years and it is one of the main tasks of governments. While there has always been data, the future of the financial services industry and the way in which data is perceived and used, has become increasingly multifaceted, facilitated by technology.

In our tour of regulatory developments over the following pages, there are a number of recurring themes: digital disruption and cybersecurity; tackling money laundering; a focus on consumer protection; and culture, conduct and individual accountability, all in relation to data.

Firms and regulators are preoccupied with protecting data as a key digital asset—whether customer data, financial data, data stores—and the use of data. Evidence of this preoccupation is the focus on cybersecurity and anti-money laundering (AML) systems and controls. Under the broader mantle of operational resilience, cybersecurity sits at the top of firms' and regulators' agendas, so it is unsurprising to see this feature significantly in our updates. As the concept of "operational resilience" gains traction in global regulatory forums and as technological development continues, it's likely to continue to feature predominantly over the coming decade.

If cybersecurity and AML can be seen as elements of the "defensive" position, then on the flip side is digital disruption—how the players and products in the market will change and develop through the use of technology. Some traditional market participants may be feeling that they face an existential threat if they don't embrace technology advancements, although BigTech faces its own challenges—not least from public opinion and legislators—in advancing innovations into the marketplace.

Finally, it is easy to feel like big data and technology are moving us further away from the individual, but, if anything, the risks we perceive are seeing some response in the regulators' continued focus on individual accountability, conduct, culture, and consumer protection. For example, with Artificial Intelligence (AI) being more realisable across industries, the ethics of the technology and the individual, human responsibility for the outcomes of AI decision making are a main feature of discussion. Open Banking is opening up a new era of data-driven decision making, but also poses challenges for the industry and regulators from the potential for misuse of data to exploit customers to the temptation which large concentrations of data present to malicious actors.

Looking ahead, we expect to see that balance in the regulatory developments space of the quantitative elements of data and technology on one side, and the qualitative elements of culture and individual accountability on the other, continue.

**"If cybersecurity and AML can be seen as elements of the "defensive" position, then on the flip side is digital disruption"**



## Spotlight on Australia

The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry has had significant effects on the regulation of banking in Australia and these effects will continue into the foreseeable future. The Commissioner's recommendations, and the government's legislative agenda, will mean that depending on their business model, banks will face changes in areas including the regulation of credit and its distribution, financial advice, and superannuation. Additionally, the financial services regulators in Australia — the Australian Securities and Investments Commission (ASIC) and the Australian Prudential Regulation Authority (APRA) — will have additional powers and mandates to act as strong enforcers, as well as themselves undergoing cultural change to reflect their new, toughened, roles.

There will be a number of key changes to the law which will be made in the short-to-medium term, and these will impact the business models of various banks. The Consumer Data Right (CDR) will require the four major banks to start sharing customer, account and transaction data from 1 February 2020, which will create competitive challenges but also opportunities to streamline loan application processes. Credit distribution will see the introduction of a "best interests" duty to require mortgage brokers to act in the best interests of borrowers, and over time the regulatory frameworks for mortgage brokers will be aligned to those of financial advisers, and those advisers will be subject to a new disciplinary body. Grandfathered conflicted remuneration will no longer be available to financial advisers. Industry codes will be able to be enforced using court-based remedies.

Beyond the changes to the law, there will also be substantial changes in the way that banks are regulated. ASIC and APRA are building their data capability and will increasingly incorporate the use of granular data to inform their supervision work. Banks and their executives should assume that there will be a greater level of information flow between ASIC and APRA, and this may change the dynamic in how banks have traditionally seen themselves as being regulated for prudential supervision purposes.

The Royal Commission has seen the start of a series of law reforms which will have profound effects on the banking sector for many years to come.



**Michael Vrisakis**  
Partner, Sydney  
T +61 2 9322 4411  
[michael.vrisakis@hsf.com](mailto:michael.vrisakis@hsf.com)



**Steven Rice**  
Special Counsel, Sydney  
T +61 2 9225 5584  
[steven.rice@hsf.com](mailto:steven.rice@hsf.com)

## Spotlight on Greater China

### Hong Kong's multifaceted approach in mitigating misconduct risk

In the coming year, we expect that Hong Kong regulators will continue their efforts to tackle the causes and consequences of misconduct, as guided by the Financial Stability Board's toolkit published in April 2018.

#### Senior management accountability

Since the implementation of senior management accountability regimes over the past two years, Hong Kong regulators have collected considerably more detailed information about firms'

governance structures and senior management, likely leading to enforcement actions against managers-in-charge (MICs) in the near future. Also on the horizon, we can expect to see the outcomes of the Securities and Futures Commission (SFC)'s thematic reviews on board governance and responsibilities of MICs, as well as specifically on risk governance and risk management MICs.

#### Tackling "rolling bad apples"

Enforcement actions are likely to increase as a result of the implementation of strategic licensing reform by the SFC this year, which aims to tackle the "rolling bad apples" phenomenon, ie, the movement of individuals with a history of misconduct between firms with little or no consequences. Among other

## Spotlight on Greater China, continued

things, the reform requires firms to provide the SFC with significantly more detailed information about any internal investigations conducted against departing licensed employees within six months prior to, or at any time after, their departure.

This has prompted firms to update their internal processes to broaden the scope of reporting and to clarify what should be considered as an “internal investigation” for reporting purposes. Individuals who have committed misconduct will likely find it more difficult to become relicensed with other firms, including those based overseas, given that regulators across jurisdictions are increasingly connected and are sharing information.

It is possible that Hong Kong regulators may introduce further measures to tackle the rolling bad apples phenomenon, such as reference check related requirements which have already been implemented in the UK and are proposed in Singapore and Australia. They may also consider incorporating the human resources function into the senior management accountability regimes, which have been implemented in Australia and proposed in Singapore.

### Culture reform

The Hong Kong Monetary Authority (HKMA) has begun supervisory activities on its bank culture reform which we expect to continue as a key focus in the coming year. Individual banks are required to conduct a self-assessment of progress against the HKMA’s March 2017 guidance, which focuses on governance, incentive systems and assessment and feedback mechanisms. This will be followed by on-site and/or off-site reviews of banks, as well as culture dialogues with senior management, and we are likely to see further guidance issued by the HKMA.

The HKMA will also finalise the revisions to its Supervisory Policy Manual module CG-5, Guideline on a Sound Remuneration System, in the near future. The proposed revisions include a new section on how banks’ remuneration systems should address misconduct risk.

## Enhancement of AML/CTF measures in Hong Kong and Mainland China

This year, both Hong Kong and Mainland China received their report cards from the Financial Action Task Force (FATF) on their anti-money laundering (AML) and counter-terrorist financing (CTF) measures and compliance with the FATF’s 40 recommendations.

### Hong Kong

Hong Kong’s report card, received in September 2019, noted that Hong Kong has a sound legal regime to fight money laundering (ML) and terrorist financing (TF) which is delivering good results. It understands its risks, has effective measures to combat TF and to confiscate the proceeds of crime, and actively cooperates with international partners.

The report, however, highlights that Hong Kong should (among other things) prioritise efforts to prosecute ML involving crimes committed abroad (particularly non-fraud related crimes such as drugs, tax crimes and corruption), and increase risk understanding and AML/CTF implementation by smaller financial institutions (particularly in the money service operators and money lender sectors).

In the coming year, Hong Kong is likely to see further policy changes and enhancements in light of the priority actions identified in the FATF report. We anticipate that financial services regulators will continue to place AML/CTF enforcement high on their agenda and, in particular, include senior management and MICs responsible for AML/CTF in their investigations. The regulators are also boosting their surveillance systems, as seen by the engagement of a consultant by the HKMA in June this year to study the enhancement of the HKMA’s AML/CTF surveillance capabilities.

Additionally, the SFC is exploring whether and how it should regulate virtual asset trading platforms to protect investors against the risks of fraud and ML.

### Mainland China

Mainland China’s FATF report card, received in April 2019, noted that there is a good legal framework with regards to areas such as the criminalisation of ML and TF and the powers and responsibilities of law enforcement authorities, but identified that there was scope for strengthening the framework with respect to a number of preventative measures. There was also an incomplete understanding of risk, and significant weaknesses relating to the transparency of legal persons and legal arrangements and practices related to targeted financial sanctions.

Some of the other areas identified for improvement include increasing the upper limit of financial penalties and addressing gaps in the regulators’ supervision of ML/TF risks.

Going forward, Mainland China is expected to amend its Anti-Money Laundering Law (AML Law) to increase financial penalties, which have a current ceiling of RMB 5 million for financial institutions and RMB 500,000 for individuals. There are

**“The SFC has confirmed that it expects firms to comply with the “spirit” of the requirement when assessing whether an investigation is disclosable. Notifications will therefore be focused on behaviour which calls into question an individual’s fitness and properness, thereby helping to drive misconduct out of the industry – individuals beware.”**

**SAYS PATRICK PANG, MANAGING DIRECTOR – COMPLIANCE AND TAX AT ASIFMA.**

## Spotlight on Greater China, continued

also indications that Mainland China will expand the categories of ML predicate offences covered under the AML Law (which are currently limited to seven) in line with the FATF's recommendation to apply ML to all serious crimes. The AML Law covers predicate offences such as drug-related crimes, organised crimes and financial fraud, but does not cover tax evasion.

To address gaps in regulators' supervision, we can expect to see increased inter-ministerial cooperation involving the sharing of financial intelligence (including information regarding beneficial ownership) between the financial, public security, tax, customs and supervisory ministries. It is also anticipated that Mainland China will increase AML supervision over the rapidly developing internet finance sector, which is ripe for AML risk.

### Foreign investment in Mainland China's financial services market

The enhancement of AML/CTF measures by Mainland China is important in light of the gradual opening of its financial services market, with the granting of national treatment to foreign investors and encouragement of foreign investment. A number of market entry restrictions and ownership caps have been or will be removed. In particular, by 2020, foreign investors will be permitted to own 100% shareholding in securities firms, fund managers, futures companies and certain insurance companies in Mainland China. The government also plans to open up more

areas for foreign investment in the future, such as interbank bond underwriting and pension fund management.

One challenge for foreign investors and financial institutions taking advantage of this opportunity is the need to reconcile their global AML/CTF framework with the regulatory regime of Mainland China. As Mainland China continues to enhance its measures to meet international standards, the regulatory gap with foreign jurisdictions will be reduced.



**Hannah Cassidy**  
Partner, Hong Kong  
T +852 2101 4133  
[hannah.cassidy@hsf.com](mailto:hannah.cassidy@hsf.com)



**Natalie Curtis**  
Partner, Singapore  
T +65 6868 9805  
[natalie.curtis@hsf.com](mailto:natalie.curtis@hsf.com)



**Will Hallatt**  
Partner, Hong Kong  
T +852 2101 4036  
[william.hallatt@hsf.com](mailto:william.hallatt@hsf.com)

## Spotlight on UAE

### The "passporting regime"

On 27 November 2018, the UAE Securities and Commodities Authority (SCA), Dubai Financial Services Authority (DFSA) and Abu Dhabi Global Markets Financial Services Regulatory Authority (FSRA) agreed on a common legislative framework, the "passporting regime", allowing domestic funds to be promoted anywhere in the UAE, pursuant to agreed provisions and licensing regulations.

Each regulator is required to establish a notification and registration facility to enable the marketing of domestic funds set up in the UAE, Dubai International Financial Centre (DIFC) or Abu Dhabi Global Market (ADGM) to potential investors.

The Fund Protocol Rules of the DFSA Rulebook came into effect on 25 February 2019 and set out the DFSA's requirements for registration of domestic funds for passporting. In the ADGM, the recently issued Fund Passporting Rules set out the FSRA's requirements and the SCA has also recently circulated passporting rules.

### Tightening of Anti-Money Laundering regime

The UAE's new Anti-Money Laundering Law (AML Law) (Federal Law No. 20 of 2018) was issued on 30 October 2018 and aims to enhance processes to combat money laundering crimes taking place onshore. The changes include enhanced investigation procedures (including allowing a transaction to proceed in order to trace the funds), increased fines and penalties, and an ability to freeze funds associated with financial crime.

The DFSA and the FSRA have initiated changes to their AML regimes as a result of the upcoming Financial Action Task Force (FATF) Mutual Evaluation of the UAE due to take place in the second half of 2019 to ensure compliance with the 2012 FATF Recommendations.

In October 2018 the DFSA implemented amendments to the Anti-Money Laundering, Counter Terrorist Financing and Sanctions Module of the DFSA Rulebook (AML Rules) and the DIFC Regulatory Law 2004 including, but not limited to,

## Spotlight on UAE, continued

customer due diligence, record keeping, wire transactions, reliance on third parties, internal controls and rules relating to foreign branches and subsidiaries. The DFSA also clarified its AML remit and supervision of Designated Non-Financial Business Professionals. In addition, the DIFC Ultimate Beneficial Ownership Regulations (UBO Regulations) were enacted on 12 November 2018, which require all entities operating in the DIFC to establish a register of ultimate beneficial owners. Failure to comply with the UBO Regulations may result in a fine of up to US\$25,000.

On 11 February 2019, the FSRA issued a consultation paper on its proposed revisions to the AML regime in the ADGM and on 15 April 2019 implemented regulations and rules relating to AML. The amendments enhance the FSRA's powers to prevent money laundering.

### DIFC Companies Law and DFSA's funds regime

The DIFC issued a new Companies Law (DIFC Law No. 5 of 2018) which came into effect on 12 November 2018. The new Companies Law distinguishes between private and public companies, where private companies are subject to less stringent requirements. Other amendments include enhanced directors' duties. Following implementation, the DFSA also introduced enhancements to their funds regime. Some changes include a new distinction between a public and private company as introduced by the Companies Law, introduction of Exchange-Traded Funds as a new specialist class of fund and a new model for internal management of an Investment Company where such company can be internally managed by its licenced sole corporate director, subject to certain requirements.

### Enhancing the role of the Central Bank

A new banking law (Federal Law No. 14 of 28) regarding the Central Bank and Organisation of Financial Institutions and Activities (Banking Law) was introduced in 2018. The Banking Law strengthens the Central Bank's ability to exercise effective regulatory control over the financial sector and aims to ensure consistency with international best practices and standards.

Key developments contained in the Banking Law include:

- Empowering the Central Bank to issue rules and specify exemptions in relation to financial promotions, including cross-border activities.
- Establishing a Financial Activities Committee which will include representatives of the Central Bank, Securities and Commodities Authority and Insurance Authority. This will allow more consistent cooperation and coordination between the main regulators in the UAE, which should strengthen the financial sector as a whole.
- Publishing regulations on the protection of customers. The Banking Law codifies rules on confidentiality of customer information including requiring customer consent before information can be passed to third parties.

- The Central Bank's power to undertake examinations of the activities of Licenced Financial Institutions with branches or entities in the financial free zones (the DIFC and the ADGM) in collaboration and conjunction with relevant regulators.
- Establishing a Higher Shari'ah Authority which will oversee and drive Shari'ah compliance in the UAE. This will support the UAE's goal of becoming a global leader in Islamic finance.

### Netting Law: regulated for the first time

A netting law (Federal Decree Law No. 10 of 2018) came into force on 30 October 2018 (Netting Law) and regulates netting for the first time onshore in the UAE, following the guidelines of the International Swaps and Derivatives Association (ISDA) Model Netting Act 2006.

Previously, netting and set-off were available in accordance with the UAE Civil Code provided no party was insolvent but restricted by the UAE Bankruptcy Law where a party was insolvent. The Netting Law provides certainty by addressing and dealing with the potential conflicts between the UAE Bankruptcy Law and the UAE Civil Code where one party to the transaction is subject to insolvency.

The new Netting Law covers both pre- and post-insolvency situations and applies to transactions entered into by corporate entities or individuals in the UAE (other than the DIFC and the ADGM which are self-legislating jurisdictions).

Its greatest impact is likely to be the benefit it brings for UAE entities contracting with international counterparties.



**Stuart Paterson**  
Partner, Dubai  
T +971 4 428 6308  
[stuart.paterson@hsf.com](mailto:stuart.paterson@hsf.com)



**Chris Skordas**  
Partner, Dubai  
T +971 4 428 6377  
[chris.skordas@hsf.com](mailto:chris.skordas@hsf.com)



## Spotlight on US

Regulators in the United States have been active in a number of areas that demonstrate the ongoing impact of the big data revolution on the law. Recent developments at a number of different agencies are illustrative of this trend, perhaps most prominently the enforcement actions initiated by the US Securities and Exchange Commission (“SEC” or the “Commission”). The number of actions is roughly in line with prior years, with continued focus on securities offerings, investment advisory issues and issuer reporting, and constituting nearly two-thirds of stand-alone cases brought by the Commission.<sup>1</sup>

### A new emphasis on cyber

Among the core principles on which the SEC is currently focused is “keep[ing] pace with technological change”<sup>2</sup> To that end, the SEC is striving to adapt to the myriad ways in which technology interacts with the securities laws.

The SEC’s Cyber Unit became fully operational in FY18. It brought twenty stand-alone cyber-related cases in FY18 and had over 200 ongoing cyber-related investigations at the end of the fiscal year.<sup>3</sup> Notably, the SEC had a number of “firsts” in the cyber sphere during this time, including its first action against a public company for failing to properly inform investors of a data breach, and its first action charging violations of the Identity Theft Flags Rule,<sup>4</sup> which is designed to protect customers against the risks of identity theft.<sup>5</sup>

These actions exemplify the renewed focus of US regulators on cyber-related misconduct and the protection of individuals’ confidential personal data.

### Handling a cyber breach

In April 2018, the SEC announced the results of an investigation into Altiba Inc. (formerly part of Yahoo! Inc.) concerning the circumstances surrounding the 2014 data breach of Yahoo!, which resulted in the theft, unauthorised access, and acquisition of hundreds of millions of its users’ data, including usernames, birthdates, and telephone numbers, at the time the largest known theft of individual user data.<sup>6</sup>

According to the SEC Order, Yahoo! failed to disclose the breach for nearly two years, publicly noting only a risk of future breaches and accompanying litigation and reputational damage, despite the fact that it had internally investigated and determined the extent of the breach by December 2014 at the latest.<sup>7</sup> The SEC also determined that Yahoo! senior management failed to inform its auditors or outside counsel of the breach and ongoing cyber intrusion efforts into 2015 and 2016.<sup>8</sup>

In 2016, Yahoo! was also in talks to sell its operating business to Verizon Communications Inc.<sup>9</sup> Despite being aware of ongoing intrusions and of the likely theft of its entire user database, Yahoo! informed Verizon that it was unaware of any security

breaches which could be expected to have a “Business Material Adverse Effect.”<sup>10</sup> Yahoo! only disclosed the breach to the public in September 2016.<sup>11</sup>

As a result of the SEC’s determination that Yahoo! violated numerous statutory and regulatory provisions, the company agreed to cooperate fully with the SEC, cease and desist from any future violations of the securities laws, and pay a \$35 million civil penalty.

Although simply being the subject of a cybersecurity breach is not per se grounds for finding that an entity has violated the law, as the SEC noted was the case here, “a company’s response to [a cyber incident] could be so lacking that an enforcement action would be warranted.”<sup>12</sup> The SEC also advised that “[p]ublic companies should have controls and procedures in place to properly evaluate cyber incidents and disclose material information to investors.”<sup>13</sup>

### Protecting your customers’ data

In September 2018, the SEC announced the results of an investigation into Voya Financial Advisors Inc. (VFA) concerning a cyber attack that compromised the personal information of thousands of customers, the first enforcement action charging a violation of the Identity Theft Red Flags Rule.<sup>14</sup>

In April 2016, VFA was subjected to an intrusion by persons impersonating VFA contractor representatives telephoning to obtain false resets of passwords.<sup>15</sup> This enabled the intruders to access the personal information of thousands of VFA’s customers, including address, date of birth, email address, last four digits of the Social Security number, and in a smaller but still significant number of cases, full Social Security number.<sup>16</sup> The company’s security staff failed to adequately respond to these intrusions.<sup>17</sup>

The SEC found that VFA violated both the Safeguards and Identity Theft Red Flags Rules because: (i) its cybersecurity policies and procedures were not reasonably designed to protect customer information and respond to cybersecurity incidents; and (ii) despite having implemented a written identity theft policy in 2009, VFA failed to review and update its policy in response to changes in risks to its customers or provide adequate training to its employees, and the policy was not reasonably designed to respond to red flags.<sup>18</sup>

VFA agreed to retain a compliance consultant to conduct a comprehensive review of its policies, provide written certification with documentary evidence to the SEC of its cooperation with the consultant and implementation of his or her recommendations, cease and desist any violations of the securities laws, and pay a US\$1 million civil penalty.<sup>19</sup>

The SEC noted that the “case is a reminder to brokers and investment advisers that cybersecurity procedures must be

## Spotlight on US, continued

reasonably designed to fit their specific business models. They also must review and update the procedures regularly to respond to changes in the risks they face.”<sup>20</sup>

### Conclusion

For entities that handle sensitive personal information, data security is of ever-increasing importance, and with increasing regulatory focus, companies should ensure that they take all appropriate measures to maintain the confidentiality of the information they are entrusted to hold.



**Scott Balber**  
Partner, New York  
T +1 917 542 7810  
scott.balber@hsf.com



**Jonathan Cross**  
Counsel, New York  
T +1 917 542 7824  
jonathan.cross@hsf.com

1 - 3, 5. US Securities and Exchange Commission, Division of Enforcement Annual Report 2018, [www.sec.gov/files/enforcement-annual-report-2018.pdf](http://www.sec.gov/files/enforcement-annual-report-2018.pdf)  
4. Regulation S-ID: Identify Theft Red Flags (248.201 and 248.202), [www.law.cornell.edu/cfr/text/17/part-248/subpart-C](http://www.law.cornell.edu/cfr/text/17/part-248/subpart-C)  
6, 12, 13. SEC Press Release 2018-71, Altaba, formerly known as Yahoo!, charged with failing to disclose massive cybersecurity breach; agrees to pay \$35 million, [www.sec.gov/news/press-release/2018-71](http://www.sec.gov/news/press-release/2018-71)

6 - 11. SEC Order No. 33-10485, [www.sec.gov/litigation/admin/2018/33-10485.pdf](http://www.sec.gov/litigation/admin/2018/33-10485.pdf)  
14, 20. SEC Press Release 2018-213, SEC charges firm with deficient cybersecurity procedures, [www.sec.gov/news/press-release/2018-213](http://www.sec.gov/news/press-release/2018-213)  
14 - 19. SEC Order No. 34-84288, <https://www.sec.gov/litigation/admin/2018/34-84288.pdf>

## Spotlight on Germany

### Adapting to a rapidly changing landscape

Similar to other European countries, Germany's banking sector is in the course of adapting and transforming. The search for a "national champion", as reflected in the recent merger discussions of two large German banks, illustrates how the sector aims to stay competitive. A new German champion would not only compete with other global banks, but also with less traditional competitors who are significantly shaping the future of the financial services industry.

The challenge for Germany's banking sector is to achieve the required balance between innovation and regulation, ie to keep up with the vast variety of competitors and rapid development of disruptive technology, while complying with the equally rapid changing regulatory and legal landscape. The changes in the regulatory regime are fast-paced and are driven by the need to adapt the legal framework to a transforming banking sector. Germany's regulator, The Federal Financial Supervisory Authority (BaFin), has identified major challenges and areas of focus for their regulatory efforts.

### Digital transformation

In light of the ongoing digital transformation, BaFin's focus is on identifying the impact and risks of disruptive technologies to anticipate any need for supervision; and addressing the potential risks arising from digital transformation and the abuse of disruptive technologies:

- **Guidance on Disruptive Technologies:** In February 2018, BaFin issued guidance in connection with Initial Coin Offerings and the classification of Crypto tokens as a regulated financial instrument. In November 2018, BaFin released guidance for outsourcing services to cloud providers, focusing on contractual templates in compliance with applicable supervisory requirements.
- **Identifying future supervisory implications:** In January 2019, the initial results of BaFin's consultation of its report on disruptive technology and its implications for supervision were released. The report "Big Data meets Artificial Intelligence - Challenges and Implications for Supervision and Regulation" aimed to identify strategic trends and developments requiring supervision and consulted with key stakeholders between July and September 2018.
- **Minimum standards IT-Security extended to Asset Managers (KAIT):** In April 2019, BaFin released the minimum standards for IT-Security for asset managers (Kapitalverwaltungsaufsichtliche Anforderungen an die IT). This is the latest development in BaFin's effort to ensure adequate IT security systems in supervised sectors. Similar standards had already been released for the banking sector (BAIT) and for the insurance sector (VAIT).

Further developments are expected and the German banking sector will need to adapt to increased duties in this area. There may also be an increased focus on individual accountability as the IT-security minimum standards unanimously stipulate that compliance is management's responsibility. Furthermore,

## Spotlight on Germany, continued

BaFin has announced it wants to extend its IT-security framework to include sections on crisis management and conduct cyber stress testing.

### Anti-money laundering

Another focus is the prevention of Money Laundering and Terrorist Financing and BaFin's supervisory measures appear to have intensified:

- **Appointment of external monitor:** In September 2018 and for the first time in its supervisory practice, BaFin appointed an external monitor for a German bank. This shows that BaFin is dedicated to ensuring German banks have implemented adequate internal safeguards, and comply with their Customer Due Diligence duties.
- **Issuance of further guidance:** In October 2018, BaFin released its consultation paper containing guidance on which factors should be considered for the risk assessment regarding Cryptocurrencies. In December 2018, BaFin released binding guidelines on the interpretation of the German Money Laundering Act.

Further developments are imminent and will require the German banking sector to adapt. For example, the requirements of the 5th Anti-Money-Laundering Act will have to be transposed into German law by 10 January 2020. BaFin has also announced that it will focus on correspondent banking and examine risk management processes and compliance with applicable laws in this area. This new focus will likely bring about further challenges for the German banking sector.

### Consumer protection

Consumer protection remains an area of focus for BaFin's regulatory efforts and BaFin currently examines the German banking sector's compliance with applicable rules.

- **MiFID II and EU Prospectus Regulation:** In 2018, BaFin conducted an extensive market analysis to determine the status quo of MiFID II's implementation. The overall result was positive but showed that supervised entities still face challenges in implementing the requirements into their processes or lack necessary resources. BaFin plans to enhance EU-wide collaboration in order to find globally consistent and practical solutions. In July 2019, the EU Prospectus Regulation came into force and compliance with it may be a focus of BaFin.
- **Minimum requirements bail-in:** In February 2019, BaFin submitted draft guidance on the minimum requirements for the feasibility of a bail-in for consultation. The draft contains requirements with respect to provision of necessary information and technical standards.

The recent and future developments show that there is not only an ongoing transformation of the German banking sector itself but also a transforming supervisory regime which aims to adapt to the rapid technological developments. The German banking sector will need to tackle both aspects to remain competitive and innovative.



**Kai Liebrich**  
Partner, Germany  
T +49 69 2222 82541  
[kai.liebrich@hsf.com](mailto:kai.liebrich@hsf.com)



**Quenie Hubert**  
Associate, Germany  
T +49 69 2222 82519  
[quenie.hubert@hsf.com](mailto:quenie.hubert@hsf.com)



## Spotlight on France

### ACPR's 2019 priorities: cyber resilience

On 28 May 2019, the French banking regulator, the Autorité de Contrôle Prudentiel et de Résolution (ACPR), presented its activity report for 2018, which includes its priorities for the coming year.

The first priority relates to cybersecurity in the financial sector, which is a key issue for the French Presidency of the G7. In early June 2019, the Banque de France, in partnership with other banking supervisors in G7 countries, simulated a cyber attack, launched simultaneously in all G7 countries. The objective was to evaluate the exchange protocol between financial and banking authorities through the simulation of a major financial system disruption caused by a critical cyber incident. The chairman of the ACPR, François Villeroy de Galhau, announced that he would implement concrete measures once the outcome of this simulation is established.

The ACPR also announced that in 2019, it will focus on the control of business practices, including the protection of vulnerable customers. Since the end of 2018, several inspections were carried out on the measures implemented by banking institutions for financially vulnerable populations, and in particular, on compliance with the right to access basic banking services.

### The fight against money laundering and terrorist financing (AML-CFT)

AML-CFT remains one of the ACPR's main areas of focus this year. In 2018 alone, 23 on-site inspections were carried out in this respect. They revealed, according to the French banking regulator, significant weaknesses in the compliance of regulated organisations in terms of their AML-CFT and asset freeze obligations. In 2018, the ACPR Enforcement Committee issued nine financial penalties, one of which amounted to €50 million.

The ACPR announced that it will continue to monitor asset freezing obligations and will deepen its analysis of the risks raised by new technology and fintechs, including the use of crypto-assets. The ACPR's focus on AML-CFT matters over the past years is all the more a key priority given that FATF (the inter-governmental Financial Action Task Force) will carry out its evaluation of the French AML-CFT system in 2020.

### Asset freeze obligations

The joint ACPR/French Treasury guidelines on the implementation of asset freeze obligations were updated in June 2019. In particular, this update clarified the obligations imposed on French banking institutions' branches operating abroad. French banks must ensure that their branches in third-party countries implement the French and EU restrictive measures.

### Clarified civil penalties in the event of inaccuracy in the overall effective rate

The "taux effectif global" (TEG) is a rate which expresses the total cost of the loan, ie the overall amount of the loan as paid by the borrower.

Until now, the absence of or inaccuracy in the calculation of the TEG was most often sanctioned by the substitution of the legal interest rate to the conventional interest rate, even if the error on the TEG was negligible.

Ordinance No. 2019-740 dated 17 July 2019 clarifies civil penalties in the event of a default or an inaccuracy in the TEG. From now on, absence of or mistake in the calculation of the TEG is sanctioned by the loss of the lender's right to receive the interests on the loan, in a proportion fixed by the court, "in particular with regard to the damage suffered by the borrower".

The judge now has broader discretionary power and, in particular, has to take into account whether or not the borrower has effectively suffered damages as a result of the absence of or inaccuracy in the calculation of the TEG. The ordinance implies, by using the terms "in particular", that criteria other than the damages suffered by the borrower might be taken into consideration by French courts. The ordinance applies to loans granted to consumers, professionals and companies (legal entities).

The publication of this ordinance takes place in a highly sensitive political context. At the end of 2018, a first draft aimed at setting a fixed upper limit in the event of an inaccuracy in the calculation of the TEG. In the midst of the "Yellow Vests" crisis, this measure was heavily criticised and analysed as a "gift to banks". This fixed upper limit has, therefore, not been passed by French authorities.



**Antoine Juaristi**  
Partner, Paris  
T +33 1 53 57 74 04  
[antoine.juartisti@hsf.com](mailto:antoine.juartisti@hsf.com)



**Géraldine Marteau**  
Of Counsel, Paris  
T +33 1 53 57 78 37  
[geraldine.marteau@hsf.com](mailto:geraldine.marteau@hsf.com)

## Spotlight on UK

### Change: risks and opportunities

Whilst it is unsurprising that changes related to the United Kingdom's departure from the European Union have continued to occupy firms and regulators in this past year, and inevitable that they will continue to do so, they are by no means the only significant changes facing the financial services industry in the United Kingdom and those who regulate it.

As acknowledged by Charles Randall, Chair of the FCA in its Business Plan for 2019/20, change brings risks and also opportunities. By way of example, technological change tests firms' operational resilience but also offers opportunities to engage differently with customers.

There is heightened awareness of the importance for firms to be operationally, as well as financially, resilient in the face of threats such as cybercrime.

While it is still early days for Open Banking in the UK, there is regulatory appetite to explore Open Finance ie the extension of Open Banking to insurance, savings and mortgages, using the learnings, both cultural and technical, from the Open Banking journey.

Meanwhile, the expectations on regulators to protect consumers, online and offline, continues: the FCA continues to reflect on the need for a "duty of care" in financial services. It has also published a consultation on proposed guidance for firms on the fair treatment of vulnerable customers and has said that it "would like to see firms using technology to serve vulnerable customers' interests and support them to manage their financial wellbeing."

#### Accountability and cultural change

Of course when things do go wrong, the Regulators take action through enforcement. Both the FCA and the PRA have been ramping up their enforcement activity. For a number of years now, the number of investigations opened by the FCA has increased year on year. In 2015/16, 109 new cases were opened; this has increased to 343 in 2018/2019. Meanwhile, the Prudential Regulation Authority (PRA) has also continued to invest in its enforcement capability. Recent statistics indicate that, as well as 8 ongoing investigations into firms, the PRA has 19 open investigations into individuals, all of whom are senior.

By the end of 2019, the Senior Managers and Certification Regime will be extended to all FCA-authorized firms.

However, as Andrew Bailey, Chief Executive of the FCA has made clear: "...fundamental change in conduct cannot be

delivered solely by rules changes. Those who work in financial services must embrace the principles of responsibility and accountability as well as the process."

Some of this accountability is mandated by the Regulators. For instance, in the context of LIBOR discontinuance, the PRA and FCA required large banks and insurers to identify the Senior Manager(s) within their firms who will oversee the implementation of the firm's LIBOR transition plans.

But the wider issue of cultural change remains at the forefront of the regulatory agenda and a priority for the UK Regulators. The FCA in particular is exploring the role of "purpose" in creating healthy cultures.

#### The approach to data

The FCA is also examining whether its current approach to "Treating Customers Fairly" is adequate to cover data ethics in financial services, or whether there ought to be policy frameworks for how firms collect and use data.

The FCA has said how data and technology have changed and are changing the way it regulates and has set out some ways in which it has reacted to and embraced change, including:

- increasing its data science resource throughout the organisation
- testing and exploiting new tools such as web crawling and scraping, network analytics and natural language processing
- investigating how technology can fundamentally change the interface between the FCA and regulated firms by making parts of the FCA Handbook machine readable and executable, and
- in the longer term, bringing data and analytics capabilities together to deliver near real time monitoring of priority markets, to allow the FCA to identify harm rapidly and deter misconduct.

It no doubt expects firms similarly to assess, and be able to explain how they are responding to, technological and broader changes.

**"Change is here to stay for all of us: for financial markets and firms, consumers of financial services and financial regulators."**

**CHARLES RANDALL, CHAIR OF UK FINANCIAL CONDUCT AUTHORITY, FCA BUSINESS PLAN 2019/20**



**Chris Ninan**  
Partner, London  
T +44 20 7466 2490  
[chris.ninan@hsf.com](mailto:chris.ninan@hsf.com)



**Jenny Stainsby**  
Partner, London  
T +44 20 7466 2995  
[jenny.stainsby@hsf.com](mailto:jenny.stainsby@hsf.com)

# Are you prepared? The board's role in crisis management

With the ever-increasing growth in the number and potential magnitude of cyber, technological and operational risks to financial services entities, boards need to be prepared to respond to these types of crisis and ensure that the entity's critical information assets are appropriately secured.

The role of a board, in particular the non-executive members, changes dramatically in a time of crisis. Customers, the public, regulators, and policymakers expect the board to steer the firm confidently and competently back to safety.

While it is fair to say that a board should consider and plan in advance for how to respond to a crisis, there is a balance to be struck. A board should not be structured solely with crisis management in mind given that crises are likely to be quite rare. However, the prominence that a board is likely to have during a crisis means that it is sensible to consider the collective crisis management skillset. The Chair (and/or in the case of large firms, the Nominations Committee) should regard this aspect of the board's functions when considering potential new appointments and when commissioning a Board Effectiveness Review.

## Regulatory obligations for board members

Boards of financial services entities need to have clear systems and strategies in place to manage the security of data and information assets and respond to incidents, as this is fundamental to the stability of both their business as well as the broader financial markets. The operation and reputation of a financial services entity depends on the security and resilience of its technology systems and regulators around the world are sharpening their focus on technology, operational and non-financial risks.

For example, in Australia, the Australian Prudential Regulatory Authority (APRA) has recently issued Prudential Standard CPS 234 (CPS 234) which makes the board of an APRA-regulated entity ultimately responsible for ensuring the entity maintains its information security. This means that the information security related roles and responsibilities of the board and senior management need to be clearly defined and the board must ensure the entity has controls to protect its information assets and undertakes systematic testing and assurance around the controls effectiveness. APRA's latest Corporate Plan also names improving cyber resilience across the financial system as one of its top four strategic focus areas.

In the United States similar obligations are placed on the board. One example is the "Cybersecurity Requirements for Financial Services Companies" issued by the New York State Department of Financial Services (DFS) in 2017 (Regulations), which has implementation and compliance deadlines throughout 2019. These Regulations require each covered entity to assess its specific risk profile and establish and maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of its information systems. These Regulations apply to any individual or non-governmental entity (unless exempt), operating or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorisation under the New York Banking Law, Insurance Law, or Financial Services Law.

**"The Regulations "require the establishment of governance processes to ensure senior attention to these important protections".**

**"Senior management must take this issue seriously and be responsible for the organisation's cybersecurity program and file an annual certification confirming compliance with these regulations" including "a written policy or policies that are approved by the Board of Directors or a Senior Officer".**

**DFS SUPERINTENDENT MARIA T. VULLO,  
DECEMBER 2018**



In Europe, we find clear expectations for boards or “Management Bodies” in the EU Capital Requirements Directive IV (CRD IV), in addition to the provisions of the Companies Act and the non-binding Financial Reporting Council’s Corporate Governance Code. The legislation sets out the expectation that board members should commit sufficient time to perform their functions and sets restrictions on the number of additional directorships an individual board member may hold. CRD IV and the provisions of the second Markets in Financial Instruments Directive (MiFID II) are further bolstered with guidance from the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA).

The financial crisis of 2007/8 has seen policymakers and regulators become increasingly focused on ensuring that the boards of financial institutions are robust and fit for purpose—including managing a crisis. The focus on time is important as steering a firm through a crisis, from inception to the post-crisis tail, will take a significant time commitment: dealing with a cyber event, such as a large personal data breach impacting upon multiple stakeholders or the unavailability of a critical IT system, can become a full time job in the months following the incident.

**Litigation and personal liability**

Litigation following cyber incidents will often argue that executive directors should be personally liable on the basis of breach of fiduciary duty. Irrespective of the law, executive board members








have frequently stood down from leadership roles following significant data breaches.

In the UK, some in a non-executive capacity might be uneasy about whether they have met their obligations to the firm under the FCA’s Senior Managers and Certification Regime (SMCR) (see Financial Conduct Authority Handbook, Code of Conduct, Annex 1/1, Roles and Responsibilities of NEDS of SMCR firms), such as the role of satisfying themselves that systems of risk management are robust and defensible. However, while there is a temptation to move into a more executive mode, the fact they may have a greater degree of distance from the fray can enable them to take a more measured stance representing the firm externally.

**Preparing the board for a cyber incident**

In 2018 the UK Government’s Cyber Governance Health Check, which looks at the approach the UK’s FTSE 350 take to cyber, concluded that many FTSE 350 boards still do not understand the impact of a cyber incident on their business. Similarly, the UK FCA’s cyber and technology resilience survey (November, 2018) highlighted that firms reported a lack of board understanding of cyber risks, an issue which the FCA has also seen during its supervisory work. In Australia, capabilities across APRA’s regulated entities and their key service providers are variable with a range of cyber exposures and preparedness observed by the regulator.

**Reporting requirements – how long have you got?**

	 Within 1 hour	 Within 72 hours	 Within 10 business days
 UK		Under the General Data Protection Regulation (GDPR), an organisation must report a personal data breach, which is likely to result in a risk to a person’s rights and freedoms, to the relevant Supervisory Authority. <sup>1</sup>  If the breach represents a high risk to a person’s rights and freedoms, the organisation will also have to inform people affected “without undue delay”.	
 Australia		CPS 234 requires an APRA- regulated entity to notify APRA as soon as possible and in any event within no later than 72 hours after becoming aware of an information security incident that affects or could have materially affected the entity or the interests of customers, or has been notified to other regulators (either in Australia or other jurisdictions);	CPS 234 requires an APRA- regulated entity to notify APRA as soon as possible and in any event within no later than 10 business days after it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.
 Singapore	The Monetary Authority of Singapore (MAS) imposes stringent technology risk management and reporting requirements on financial institutions, such as the requirement to notify MAS within one hour of discovering a system malfunction or IT security incident that has severe and widespread impact on the financial institution’s operations or materially impacts on its service to its customers.	Singapore’s Personal Data Protection Commission of Singapore (PDPC) requires organisations to report personal data breaches “as soon as practicable” and in any event no later than 72 hours after establishing that the data breach is likely to result in significant harm to be affected individuals or if the breach is of significant scale.	
 US		Under the Cybersecurity Requirements for Financial Services Companies referenced above, the covered entity must notify the DFS of any breaches as promptly as possible but no later than 72 hours from a determination that any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse an information system or information stored thereon, has occurred, if: (1) notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or (2) the event has a reasonable likelihood of materially harming any material part of the normal operation(s) of the entity.	

1. The clock starts ticking from the time when a controller “becomes aware” of a personal data breach, which means when a controller has a “reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.” The rationale for the notification is so that prompt steps can be taken to mitigate any harm which may be caused.





“CEOs and other decision makers should be held accountable whenever a cybersecurity breach takes place” ... “Organisations need to see cyber attacks as a business risk and leadership at the highest levels have to take accountability”.

**MR DAVID KOH, CHIEF EXECUTIVE OF THE CYBERSECURITY AGENCY OF SINGAPORE, SEPTEMBER 2018**

In order to counteract the lack of cyber understanding prevalent at board level, we are seeing a number of strategies being implemented such as establishing specialist sub-committees and conducting simulation or “Wargaming” activities. In particular, when modelling simulation scenarios for cyber incidents, attention should be given to containment and mitigation strategies.

### Crisis simulations

It is common practice for firms to engage in crisis management simulations—a task which is not to be underestimated given the need for policies, plans, and procedures to be comprehensive and flexible to cover any combination of circumstances. It is important for boards to be fully engaged with the firm’s crisis management simulations and to understand the firm’s activities and main risks. For example, in the EU, CRD IV requires firms to devote adequate resources to induction and training of board members to ensure they possess adequate collective knowledge, skills, and experience.

In the case of a cyber or broader technology incident, adequate simulation training may ensure there is appropriate capability within the board to strategically assess and manage the risks upon briefing from an IT Director or Chief Information Security Officer, allowing for a strategic quick response in a time sensitive situation. Such crisis simulations are also important because they acclimatise boards to the sorts of decisions they will need to make in a real incident.

Such “wargaming” is also useful because it can contribute to meeting the “training” expectations of legislation, in which simulation scenarios are carefully constructed to undertake a test of the board’s role and response in a crisis situation. Such exercises are likely to be most effective when the board sets aside a reasonable amount of time to fully engage with the exercise, review the outcomes and identify any gaps, for example, at a board away-day or offsite. Without wargaming it is unlikely that the board will be able to meet the very tight timetables that are set for reporting by law.

### Preparing a crisis response plan

All organisations should have robust, well-tested incident response plan ready to launch when cybersecurity or technology incidents arise. The key parts of this plan are likely to involve crisis organisation, information and reporting, communications, legal fallout and the aftermath.

### Crisis organisation

There is a balance to be struck between being comprehensive and being flexible to suit any combination of circumstances. If the plan is too rigid, then adhering to it becomes impractical and, in the worst case scenario, serves to exacerbate the crisis. If the plan is too high level, it offers little guidance at a time when that is likely to be needed. The best plans include the detail, but indexed and cross-referenced in a way that is easily navigable for any given type of incident.

In a board context, it is important that – at time of crisis – the respective roles and responsibilities of the various board members are clear and take into account the relevant skill sets.

Typically, the chair of the board will have a leading role in a crisis. However, there may be types of crises where a board member’s profile or skill set is particularly suited for a lead role—for example, if a board member has considerable and relevant reputational capital or technical skills. The plan should allow for the chair to make delegations where appropriate and beneficial for the firm.

The plan should also be clear on the respective roles of the executive versus the non-executive, particularly with regard to representing the firm externally. Given the direct management role which the executive plays in the day-to-day running of the firm, there is potential for those in executive roles to become defensive during a crisis. This is particularly true where external parties—for example, politicians, the media, social media commentators—allude that there may be a degree of personal culpability attached to an individual executive.

## Information and reporting

Many crises require the rapid collation of information from different teams. Cyber crises, for example, require input at speed from many different disciplines, including technical, legal, business continuity and communications—and, given the international nature of many cyber incidents, often across a number of jurisdictions. It is often advisable to appoint a dedicated coordination team to ensure that information is collated sufficiently quickly.

In cyber incidents one of the first steps may be to engage alternative means of communication, given that there may be lack of clarity regarding which systems have been impacted. For example, if corporate e-mail is compromised, it may be necessary to resort to alternatives such as WhatsApp. It is too late to try to set such alternative communications up after the event; it must be done beforehand and be part of the crisis response plan.

While the management information which a board will receive to inform its business-as-usual oversight typically evolves to suit the needs of the board over time, during a crisis there is not time to finesse its formatting and content. An exercise should help to build the board's awareness of and (potentially) familiarity with management information in formats, structures, and volumes which they would be unlikely to use during business-as-usual periods.

During the investigation, care should be taken to log investigative steps and to preserve evidence in case civil or criminal proceedings follow.

## Legal fallout

The role of legal in any incident can be significant. The legal team's input is often required to help contain the incident, to manage regulatory, insurance and other notifications, to manage third parties that may have had a hand in the incident (for example, a third party supplier), to manage any subsequent investigation and to deal with any follow-on claims. Much preparation can be done in advance, and it is common for legal teams to have their own, separate legal incident response plans in order to accelerate their ability to respond in a crisis. As part of this the plan should provide for careful consideration of what documents might attract legal professional privilege and how that privilege can be best preserved throughout the incident and subsequent investigation – bearing in mind that there will often be a trade-off between preserving privilege and stifling efficient and important communications during a crisis.

## External communications

Crises have the potential to throw firms into disarray and it is critical to manage external

messaging, particularly where social media has the ability to proliferate both real accounts and “fake news”. Great care should be taken by board members and it is common practice to provide media training as part of the simulation exercises; such as role playing with specialist media consultants. The challenge is to avoid saying anything that may prove to be a hostage to fortune, while also meeting regulatory expectations to keep stakeholders, including customers, informed.

Where possible, the board should consider what steps a firm might take around communications in the crisis plan, eg heightened monitoring of media and social media, the prioritisation of particular channels and/or the general tone/positioning of external communications, the slightest misstep may be seized upon and spun via mainstream or social media. This could lead to loss of customer trust, with significant reputational and financial consequences.

Responsibility for both approval and delivery of external messaging should also be part of the role allocation process, with consideration given to the audience eg, staff, shareholders, the mainstream media, social media, government and politicians, regulators, peer firms, and the wider industry. Consideration should also be given to the timing and rhythm of communications as the crisis develops, so that key stakeholders are notified simultaneously regarding developments, and that there is consistency to the narrative as the crisis unfolds. In cyber incidents it can take time to determine what has happened; to identify correctly the threat actor and their motivation.

For instance, when an airline operator suffered a large-scale data breach in 2018 with 9.4 million of its passengers impacted, the airline was heavily criticised by the Hong Kong Privacy Commissioner for taking seven months to disclose its breach and not having enough regard for data privacy and governance. Unlike the GDPR's requirement to disclose data breaches within 72 hours, Hong Kong currently has no statutory requirements for data breach notifications. Nevertheless, the privacy watchdog has stated that businesses should adopt “proactive data management” despite Hong Kong not having “a similar principle of accountability” as the EU.

Some of the messages which a firm conveys are subject to regulatory or legal requirements. For example in the UK, firms are expected to disclose anything of which the regulators would reasonably expect notice and for the firm to keep customers appropriately informed. While quite a broad-ranging requirement, a crisis would certainly fall within the disclosure expectations. Similar requirements may emanate from other authorities, for example, those charged with

ONLY **57%**  
TESTED INCIDENT PLANS  
REGULARLY

ALTHOUGH MOST COMPANIES HAD INCIDENT PLANS, ONLY 57% TESTED THEM ON A REGULAR BASIS. BUSINESSES IN FINANCIAL SERVICES WERE AHEAD OF THE PACK, HOWEVER, AS THEY WERE SLIGHTLY MORE LIKELY TO TEST THEIR PLAN REGULARLY, WITH 61% DOING SO, COMPARED TO 49% IN OTHER SECTORS.

THE UK GOVERNMENT'S  
CYBER GOVERNANCE  
HEALTH CHECK



ASIC HAS RECENTLY  
PUBLISHED A LIST  
OF KEY QUESTIONS  
FOR BOARDS ON  
CYBER RESILIENCE

Q. HOW OFTEN IS THE CYBER  
RESPONSE

plan  
reviewed  
AT BOARD LEVEL?

Q. HOW CAN WE MOVE  
FROM REACTING TO

anticipating  
the threats?

Q. CAN WE BE USING MORE

data and  
intelligence

DRIVEN SOLUTIONS TO  
MONITOR & IDENTIFY RISKS?

Q. DOES THE BOARD NEED

more  
expertise

OR SUPPORT TO UNDERSTAND  
THE CYBER AND TECHNOLOGY  
RISKS AND THE IMPACT TO THE  
ENTITY?



upholding data protection standards like the UK's Information Commissioner.

It is crucial to dovetail any external public communications with regulatory, insurance and other notifications, to avoid regulators finding out about incidents via the press rather than from the firm directly.

### Crisis aftermath

Crisis events can, and usually do, have a very long tail – often extending years decades after the event. Plans which are circumscribed to the immediate aftermath of an incident risk validating a short-sighted approach. While a firm cannot, and should not, run in crisis mode for longer than is reasonably needed, the “exit” or “close out” should include a sensible “lessons learned” exercise, including updating the crisis plan, to meet the expectations of customers, the public, regulators and policymakers.

The board should consider any impacts on, for example, the firm's risk appetite and governance arrangements, customers and potential customers, the regulatory relationship, and so on. In a recent enforcement action against a UK bank which related to an IT failure, the UK regulators highlighted that the firm had previously been subject to enforcement action for a similar incident. Commenting on the case, the CEO of the Prudential Regulation Authority noted, “... this was a repeat failing which demonstrates a lack of adequate and timely remediation. This is a significant aggravating factor in this case, leading to an uplift in the penalty.” While not known for sure, it may also be reasonably conjectured that the regulators' supervision of the firm will have become more intensive.

### Conclusion

While it is not possible to plan for every eventuality, boards have a key leadership role in preparing their firms to respond effectively to and recover from a crisis.

As society becomes increasingly digital and data-driven, the harm that can be caused by a cyber incident has become greater. Accordingly, the expectations of board members by regulators, stakeholders and the public are higher than they have ever been. Increasingly, boards will be expected to understand the technologies better that are being widely deployed in business. They will be expected to keep up with the changing threat landscape and oversee the implementation of security controls which are appropriate for the new landscape. The consequences of not meeting those expectations are severe.

Digital transformation and developments in, for example, blockchain-based technologies, machine learning/artificial intelligence and quantum computing will bring further rapid, substantial change. In the future, board members will be assisted by security being built into new products and services by design and default to a greater extent. For now, however, risk-based planning, including a well thought through and robustly tested incident response playbook, that is proportionate to the scale and complexity of a firm's operations will do much to minimise operational damage, reputational harm and legal liability. Preparations do not have to be onerous, and should, in the best cases, provide the board with more insight into the business to improve how they function during business-as-usual.



**Joseph Falcone**  
Partner, New York  
T +1 917 542 7805  
[joseph.falcone@hsf.com](mailto:joseph.falcone@hsf.com)



**Katherine Gregor**  
Partner, Melbourne  
T +61 3 9288 1663  
[katherine.gregor@hsf.com](mailto:katherine.gregor@hsf.com)



**Julian Lincoln**  
Partner, Melbourne  
T +61 3 9288 1694  
[julian.lincoln@hsf.com](mailto:julian.lincoln@hsf.com)



**Andrew Moir**  
Partner, London  
T +44 20 7466 2773  
[andrew.moir@hsf.com](mailto:andrew.moir@hsf.com)



**Andrew Procter**  
Partner, London  
T +44 20 7466 7560  
[andrew.procter@hsf.com](mailto:andrew.procter@hsf.com)



**Mark Robinson**  
Partner, Singapore  
T +65 6868 9808  
[mark.robinson@hsf.com](mailto:mark.robinson@hsf.com)



**Kate Macmillan**  
Consultant, London  
T +44 20 7466 3737  
[kate.macmillan@hsf.com](mailto:kate.macmillan@hsf.com)

# Virtual banks: the case for clearer regulatory guidance on outsourcing

While virtual banks promise a range of exciting new and improved products, they also present financial regulators and market participants with new challenges. One of the key challenges relates to the tension between encouraging virtual banks to engage with innovative fintech companies, and to move their IT infrastructure into the cloud, on the one hand, while simultaneously ensuring that customer data is adequately protected, on the other.

This article: (i) examines whether existing regulatory guidelines on outsourcing in Hong Kong and Singapore provide virtual banks with sufficient guidance when it comes to designing, building and procuring their IT infrastructure; and (ii) compares the Hong Kong and Singapore guidelines with the approach that has been taken in other jurisdictions, such as in the EU by the European Banking Authority, Australia by the Australian Prudential Regulation Authority, and South Africa by the South African Reserve Bank.

The article concludes that while existing guidelines are helpful, financial regulators in Asia could help accelerate the growth of virtual banks by providing more detailed guidance on their expectations for the design, build and procurement of virtual banking IT infrastructure.

## The virtual bank revolution in Asia

The move towards “virtual” or “digital” banks continues to gather momentum in Asia, with the Monetary Authority of Singapore (MAS) announcing in August 2019 that it will accept applications until 31 December 2019 for five digital banking licences (two digital “full bank” licences and three digital “wholesale” bank licences), with the successful applicants expected to be announced in mid-2020 and to commence business by mid-2021. Earlier in 2019, the Hong Kong Monetary Authority (HKMA) granted eight virtual banking licences. Similarly, in Australia, a wave of new digital or neobanks have been granted full Australian banking licences, for example: Volt (stated to be the “first new

retail bank to be granted a banking licence in Australia since the early 2000s”), Judo and 86 400.

It is reported that Malaysia’s central bank, Bank Negara Malaysia, is aiming to join the likes of Singapore, Hong Kong, Australia, China, India, Japan, South Korea and Taiwan by releasing new licensing rules for virtual banks by the end of 2019. Regulators in other Asian countries will monitor these developments with keen interest. The Financial Services Authority in Indonesia, for example, has not announced any plan to issue any virtual bank licence but has recently issued a regulation allowing traditional banks to become more digital.

A key driver behind the new virtual banking licences in Hong Kong, Singapore and beyond is to attract non-traditional players to the banking sector and to provide a greater array of products and, ultimately competition, for the benefit of the consumer.

As noted by HKMA’s chief executive, Norman Chan Tak-lam, “The launch of virtual banks in Hong Kong, a key component of the smart banking initiatives, will certainly facilitate financial innovation, enhance customer experience and financial inclusion”. Similarly, MAS’ senior minister and chairman, Tharman Shanmugaratnam has noted, “the new digital bank licences mark the next chapter in Singapore’s banking liberalisation journey. They will ensure that Singapore’s banking sector continues to be resilient, competitive and vibrant”.

These non-traditional players, some of which are (or are backed by) the world’s



## “Into the cloud”

“A model to enable ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (eg networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

“In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of your computer’s hard drive. The cloud is just a metaphor for the Internet. It goes back to the days of flowcharts and presentations that would represent the gigantic server-farm infrastructure of the Internet as nothing but a puffy, white cumulus cloud, accepting connections and doling out information as it floats.”

ARTICLE, “WHAT IS CLOUD COMPUTING?”

largest technology companies, come armed with: a deep understanding of the technological platforms that underpin modern banking; nimble, agile and solutions-focused working cultures; and platforms of millions, if not hundreds of millions, of loyal and engaged users, many of whom may have had trouble opening traditional bank accounts. It is little wonder that these players are being targeted to drive innovation and customer experience in the banking sector.

Traditional “bricks and mortar” banks in Hong Kong and Singapore do not require virtual banking licences as they have had the right to provide their customers with digital products and services for some time under their existing licences. Furthermore, in the case of Singapore, MAS’s existing policy allows Singapore-incorporated banking groups to establish digital banks (referred to in the policy as internet-only banks) with a joint venture partner where the Singapore-incorporated bank has control over the venture. The new virtual bank licences do, however, present traditional banks with an opportunity to enter into strategic partnerships with non-traditional players where they need not maintain control over the venture.

It is expected that by combining the attributes of technology companies with the banking and regulatory know-how and credibility of a traditional bank, newly formed virtual banks will be able to deliver new and improved products and services. For some traditional banks, such

partnerships are essential for ensuring that they are not left behind in the virtual banking revolution. For others, it can also be a hedge against increased competition from new market entrants.

“Into the cloud”

The move towards “fully virtual” banks is not just about replacing physical branches and ATMs with sophisticated smartphone applications. It involves an end-to-end rethinking of the design and delivery of financial products and services and, in particular, the underlying IT infrastructure. Rather than relying on the in-branch processing of customer paperwork, market participants are now looking to engage emerging IT and cloud service providers to provide a range of cloud-based, digital services, including online customer verification and know-your-customer checks, anti-money laundering and fraud screening, marketing automation services, automated customer contact centres and regulatory reporting services to name a few. The generation of large, structured data sets based on customer activity is giving rise to a new range of products and services, based on data analytics and AI, such as automated and interactive customer helpdesks and loan and financing decision making tools. More generally, the IT infrastructure of virtual banks is moving into the cloud.

Figure 1 sets out at a high level how the cloud infrastructure of a virtual bank may be designed.

Data security risks

Barely a week goes by without a story breaking about a cyber attack or data breach involving a major financial institution.

At the time of writing this article, news was breaking that a hacker had gained access to more than 100 million Capital One customer accounts and credit card applications, and tried to share this information online. In the wake of the data breach, AWS was quick to point out that the breach occurred due to a “firewall misconfiguration”, which was controlled by Capital One, and that no AWS infrastructure or services were compromised.

Historically, traditional banks have managed these sorts of data security risks by managing their IT infrastructure “in-house” and “on-premises”, with limited or constrained involvement from third party vendors. In some jurisdictions, such as Indonesia, traditional banks are even mandated by regulation to store their data in onshore data centres.

In contrast, virtual banks are engaging multiple IT vendors to provide myriad cloud-based solutions. While third party and cloud solutions are not inherently less secure than “in-house” and “on-premises” solutions, they reduce the level of control that a financial institution has over its systems. As demonstrated by the Capital One and Amazon Web Services (AWS) case, additional issues can arise in relation to the apportionment of responsibility and

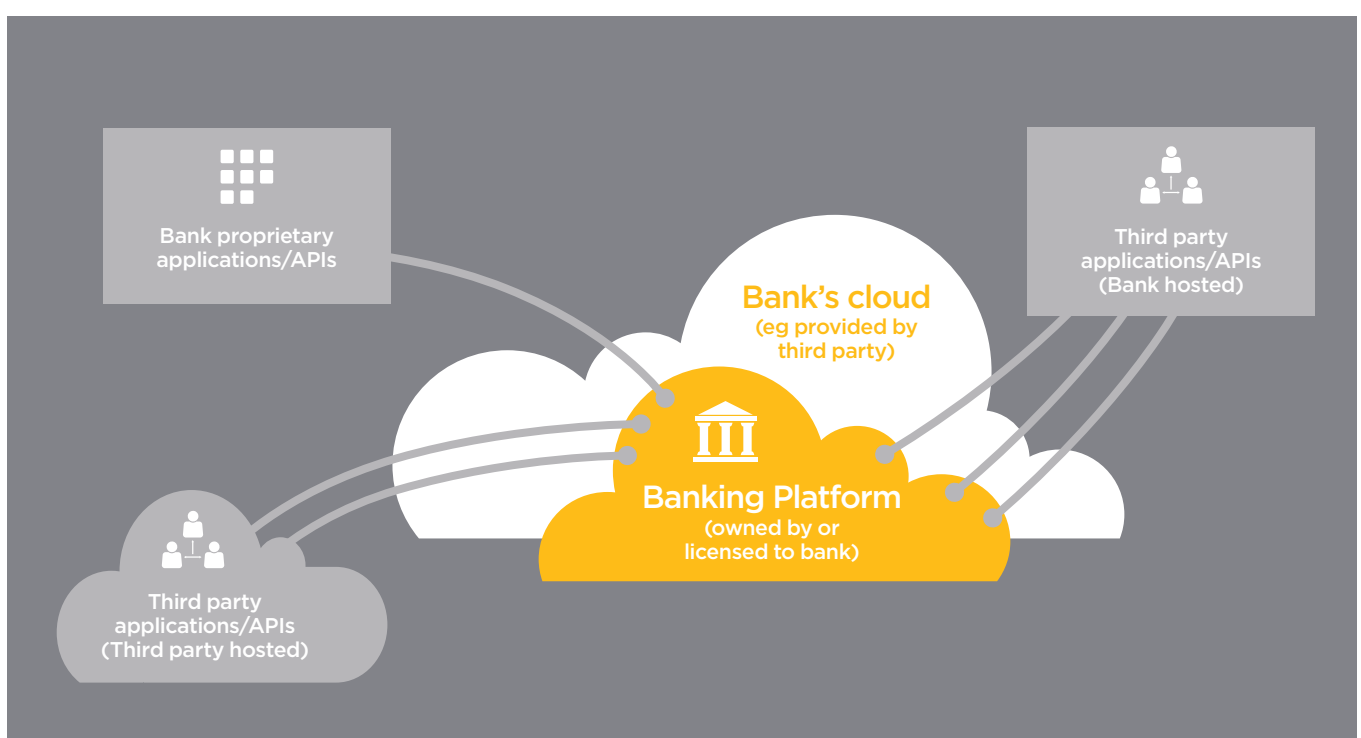


Figure 1: IT infrastructure for Virtual Bank

# The Australian National Blockchain

This century will see the rise of digital infrastructure. Just as the advent of physical infrastructure – such as roads, electricity grids and telecommunications hardware – sparked a new era of economic productivity, the advent of digital infrastructure will give rise to entirely new ways of doing business.

The recently released ACOLA report on the “Effective and ethical development of Artificial Intelligence” made the following key finding:

“AI is enabled by access to data. To support successful implementation of AI, there is a need for effective digital infrastructure, including data centres and structures for data sharing, that makes AI secure, trusted and accessible, ... If such essential infrastructure is not carefully and appropriately developed, the advancement of AI and the immense benefits it offers will be diminished.”

The Australian National Blockchain (ANB) is the coordinated vision of Herbert Smith Freehills, CSIRO's Data61 (the data science arm of Australia's national science agency), King Wood Malesons and IBM to support our clients in their digital journeys and the future use of smart legal contracts.



liability in the event of a data breach. Furthermore, the multiplicity of vendors involved can increase the risk of something going wrong and create additional problems for allocating risk.

Financial regulators have long since provided financial institutions with detailed guidelines on technology and outsourcing procurement. One of the reasons for such guidance is to ensure that customer data is adequately protected. These guidelines apply to both traditional banks and virtual banks, and cover the procurement of cloud-based solutions, which are usually seen as constituting a form of outsourcing.

At a high level, these guidelines require financial institutions to incorporate certain provisions into their contractual arrangements with IT vendors in order to mitigate key risks, including provisions such as audit and inspection rights, restrictions on subcontracting, service level agreements (SLAs), requirements around data sovereignty, the processing of customer data and information security, business continuity and disaster recovery plans, obligations to engage with regulators, incident notification requirements and monitoring rights. While these controls are of central importance to the protection of customer data, traditional views on what may constitute “adequate”, “reasonable” or “practicable” contractual protections are being challenged by the changing IT and cloud services landscape. As a result, it is becoming more difficult for financial institutions to implement existing regulatory guidance strictly.

### The challenges

Parts of the IT and cloud services sector are dominated by a small number of players, including some of the largest and most sophisticated tech companies in the world, such as Microsoft, Oracle, SAP, Google and AWS. With thousands if not millions of customers, these players are often unwilling to depart from their standard terms or grant financial institutions the contractual rights that they require to satisfy regulatory guidance. For example, suppliers often resist broad-reaching audit and inspection rights and controls on sub-contracting and assignment on the basis that such rights would unduly interfere with their business. Further, “off-the-shelf” cloud products may not practically enable financial institutions to comply with the regulatory guidance without specific customisations or configurations made for the financial institution, which may come at significant additional cost to the extent it is possible to do so.

The obligations owed by a financial institution to a national regulator can vary from jurisdiction to jurisdiction. However, many service agreements are negotiated on a regional if not global basis, with multinational suppliers that are often unfamiliar with the idiosyncratic regulatory requirements of a particular jurisdiction and that may be unwilling to comply with the “highest watermark”. This can make agreeing certain provisions particularly difficult. For example, the MAS Notice on Technology Risk Management requires a financial institution to notify MAS as soon as possible, but not later than 1 hour, upon the discovery of a system malfunction or material IT security incident. While this is a legally binding requirement in Singapore, some multinational suppliers will not commit to provide notifications within one hour.

## IT and cloud service providers are reluctant to take on uncapped liability for data breaches (or provide appropriate indemnity protection).

While this may make “business sense”, it places financial institutions in a difficult position. Failure by IT and cloud service providers to comply with obligations regarding the processing of customer data and information security can cause losses that significantly exceed the “contract value”, such as regulatory fines and damage to the reputation and brand of a financial institution, not to mention the financial losses and distress that may be caused to banking customers.

IT and cloud service providers are now seeking broader rights to access and use the data of financial institutions (whether on an anonymised and aggregated basis or not) for the purposes of developing and improving fintech products and services, including the development of AI and sophisticated data analytics tools. While these moves (along with various open banking initiatives) are consistent with the aims of the virtual banking revolution to “facilitate financial innovation, enhance customer experience and financial inclusion”, they require financial institutions to divest further control of their data which may, if sufficient governance and controls are not employed, increase the risk of data breaches.

Regulatory guidelines have been designed to assist regulated financial institutions with negotiating individual cloud agreements, on a case-by-case basis, and are underpinned by the principle that financial institutions must be ultimately responsible for their IT infrastructure. However, for a virtual bank, whose entire business model is focussed on partnerships and outsourcing, compliance with such guidelines can be particularly onerous and time consuming. This is particularly the case for fledgling virtual banks, looking to negotiate with dozens and dozens of IT suppliers, with tight timeframes, for the purposes of a timely a launch. As this model evolves, it will be interesting to see if governments, financial regulators or consumer watchdogs seek to impose obligations on cloud service providers in addition to the obligations that are currently imposed on traditional financial institutions.

Finally, regulatory guidance is not legally binding in many cases and its implementation requires a careful review of the circumstances, which can lead to uncertainty. For example, the MAS Guidelines on Outsourcing (revised 5 October 2018) (MAS Outsourcing Guidelines) provide that, “The extent and degree to which an institution implements the Guidelines should be commensurate with the nature of risks in, and materiality of, the outsourcing arrangement”. Similarly, the HKMA’s General Principles for Technology Risk Management (TM-G-1) (HKMA TRM Guidelines) provides that financial institutions are “expected to implement the relevant technology risk management framework that is “fit for purpose”, ie commensurate with the risks associated with the types of business and operations, the technologies adopted and the overall risk management systems of individual [financial institutions]”. As a result, it can be difficult for financial institutions to assess which of many aspirational requirements set out in the regulatory guidelines are required in particular circumstances.

## Cloud-specific guidelines?

These challenges call into question whether financial regulators should be updating their guidelines for use in a virtual banking world.

The MAS Outsourcing Guidelines, which were last revised on 5 October 2018, contain a section on cloud computing which recognises the advantages and growth of cloud based services, and how “different cloud models provide for distinct operation and security trade-offs”. MAS notes that cloud services constitute a form of outsourcing, and that financial institutions will be ultimately responsible and accountable for maintaining oversight of cloud services and managing the attendant risks of adopting cloud services as in any other form of outsourcing. However, the MAS Outsourcing Guidelines do not go so far as to address the issues set out above in relation to the processing of customer data.

At the time of writing this article, the Association of Banks in Singapore (ABS) released its “ABS Cloud Computing Implementation Guide 2.0” for the financial industry in Singapore. The guide notes the rapid advancement of technology and market practice since 2016, the date of the first version of ABS’ guide. The guide is intended to assist financial institutions with implementing cloud outsourcing arrangements (and cloud service providers with better understanding the requirements of financial institutions). Echoing MAS guidance, it notes, “the guiding principle that controls in the Cloud must be at least as strong as those which the [financial institutions] would have implemented had the operation been performed in-house should apply”.

The HKMA TRM Guidelines, which were last updated in June 2003, and the HKMA Guidelines on Outsourcing SA-2, which were last updated in December 2001, do not expressly engage with the issues presented by cloud services. Helpfully, the Hong Kong Privacy Commissioner for Personal Data (PCPD) released a Cloud Computing Information Leaflet in July 2015 which highlights some of the key concerns, including rapid trans-border data flows, loose outsourcing arrangements, standardised services and contracts, and less control over IT infrastructure. While the PCPD leaflet addresses some of the issues set out above in relation to the processing of customer data, it concludes (like MAS) that financial institutions are ultimately responsible for ensuring that their cloud arrangements meet regulatory requirements, and that any financial

institutions that fail to remedy “gaps” between what is being offered by a service provider, and what is required by the regulator, will bear the risks of data breaches and misuse.

## Europe’s approach to outsourcing

Financial regulators in other jurisdictions have provided more specific guidance on these issues. Earlier this year, the European Banking Authority (EBA) released its Guidelines on outsourcing arrangements. The Guidelines come into force on 30 September 2019, with firms expected to comply with the provisions by no later than 31 December 2021. The Guidelines integrate previously issued EBA Recommendations which aimed at “overcoming the high level of uncertainty regarding supervisory expectations on outsourcing to cloud service providers”. Among other things, the EBA recognises “differences in national regulatory and supervisory frameworks for cloud outsourcing” and encourages financial institutions to adopt “internationally accepted information security standards”.

In relation to sub-processing, the background notes to the Guidelines explain that,

**“With regard to sub-outsourcing, cloud outsourcing is more dynamic in nature than traditional outsourcing. There is a need for greater certainty about the conditions under which subcontracting can take place, in particular in the case of cloud outsourcing.”**

The Guidelines provide that while pre-approval for sub-processing is not required, financial institutions should be provided with ex ante notification in the case of outsourcing of critical or important function, and that financial institutions should always have the right to terminate the contract if planned changes to services would have an adverse effect on the risk assessment of the outsourced services.

The accompanying documents to the Guidelines also set out the EBA’s analysis of a range of issues raised by market participants during the consultation phase. In response to concerns that many cloud services are provided on a multi-tenanted, standard terms basis, by sector monopolists who are unwilling to comply with all relevant regulatory requirements, the EBA notes that financial institutions, “should comply with all regulatory requirements, including with regard to their outsourced functions, independent of the fact that they may be standardised or provided by monopolists”. While this response does not provide financial institutions with the flexibility they are looking for, it nevertheless provides useful guidance to the EBA’s position on this subject.

## Australia’s approach to outsourcing

The Australian Prudential Regulation Authority (APRA) has published a number of prudential standards, including Prudential Standard CPS 231 Outsourcing, detailing the requirements of financial institutions outsourcing a material business activity, and Prudential Standard CPS 234 Information Security, which describes key requirements applicable to the protection of a financial institution’s information assets, including where such assets are managed by a third party. These guidelines include, amongst other things, requirements for outsourcing arrangements to (i) include an indemnity from the service provider in respect of its sub-contracting, (ii) permit APRA to access documentation, information and sites, and (iii) address particular matters in the agreement (including review provisions, service levels and performance requirements, audit and monitoring procedures, and offshoring arrangements).

In response to the “growing usage of cloud computing services by APRA-regulated entities, an increasing appetite for higher inherent risk activities, as well as areas of weakness identified as part of supervisory activities”, in September 2018, APRA published its ‘Information Paper: Outsourcing involving cloud computing services’ (Paper). The Paper outlines prudential considerations and key principles for consideration by financial institutions when adopting the use of cloud computing services.

Recognising that the risks associated with cloud services will depend on the nature of the usage of the services, APRA classifies





risks into three broad categories, with the expectation that all risks will be managed in an appropriately commensurate manner. The Paper provides guidance on APRA's expectations for financial institutions engaging in cloud services arrangements, identifies potential "observed weaknesses" associated with cloud arrangements, has regard to considerations such as "balancing the needs of multiple customers with the practicalities of not overburdening the service provider", and considers APRA's supervisory approach to these arrangements (for example, the need for early engagement with APRA for arrangements with "extreme inherent risk").

While the Paper does not constitute formal regulation, it does support the need for formalised guidance, and contemplates that the principles identified will be reflected in future guidance updates.

This is an area which APRA continues to watch closely.

### South Africa's approach to outsourcing

2019 has been a big year for digital banks in South Africa, with two having already launched and a third set to commence operations soon. These startups have been encouraged by a friendly regulatory environment designed to spur, rather than discourage, this form of innovation.

The banking regulator, the South African Reserve Bank (SARB), established a fintech unit in 2017 which monitors developments in the digital banking arena. The unit sees

itself as an enabler of innovation and has been slow to regulate, instead focusing on providing guidance to industry participants.

For now, the new digital banks are subject to the same highly regulated banking environment as traditional banks operate in. Of specific importance to digital banks is guidance note G5 of 2014 issued by the SARB which regulates the outsourcing of functions within banks.

Similar to other jurisdictions, digital banks which outsource large material functions to cloud and other technology providers need to comply with the guidance note. In addition, when material banking functions are outsourced, the SARB needs to give its permission. This is only given where the relevant bank is able to satisfy the SARB that the risks posed by the outsourcing will be appropriately managed by the bank.

### Conclusion

For the reasons set out in this article, the case is mounting for financial regulators in Asia to revise and update the outsourcing (including the procurement of cloud services) regulatory guidance for virtual banks.

For now, virtual banks remain fully responsible for complying with their regulatory obligations regarding data privacy and information security. They will need to consider all the circumstances when engaging any given IT or cloud service providers to ensure that, on a risk-adjusted basis, they can continue to comply with the existing regulatory obligations.



**Natalie Curtis**  
Partner, Singapore  
T +65 6868 9805  
[natalie.curtis@hsf.com](mailto:natalie.curtis@hsf.com)



**Julian Lincoln**  
Partner, Melbourne  
T +61 3 9288 1694  
[julian.lincoln@hsf.com](mailto:julian.lincoln@hsf.com)



**Nick Pantlin**  
Partner, London  
T +44 20 7466 2570  
[nick.pantlin@hsf.com](mailto:nick.pantlin@hsf.com)



**Mark Robinson**  
Partner, Singapore  
T +65 6868 9808  
[mark.robinson@hsf.com](mailto:mark.robinson@hsf.com)



**Rohan Isaacs**  
Consultant, Johannesburg  
T +27 10 500 2667  
[rohan.isaacs@hsf.com](mailto:rohan.isaacs@hsf.com)



**Harry Evans**  
Senior Associate, Singapore  
T +65 6868 8079  
[harry.evans@hsf.com](mailto:harry.evans@hsf.com)

# Data vs “gut instinct”: analytics in dispute resolution

The landscape for litigation analytics has never been more fast moving. Specialist platforms threaten to disrupt what they see as a fossilised industry with undue power and reward given to senior advisers who do not deign to look at whether the evidence supports their subjective assessments.

## A changing landscape

Litigation has historically been seen as immune to invasion by data analytics, with sceptics arguing that statistical analyses of past cases can never replace the expertise and intuition of seasoned practitioners. Litigators have traditionally been reluctant to undertake a quantified analysis of data in their work, preferring instead to rely on the expert judgement and years of experience that they (rightly) think clients are paying for. Nonetheless, a number of players are exploring what data can tell us about the uncertainties in litigation and arbitration, and the modern disputes adviser (whether in-house or external) needs to be able to use these to the advantage of their commercial client.

In the US, Premonition AI claims to hold the “World’s Largest Litigation Database”, and proudly states that it gives its clients an “unfair advantage in litigation” through its analysis of lawyers’ and judges’ track records. The North American scene is a busy one, with other vendors such as Dispute Resolution Data and Blue J Legal proposing, to a greater or lesser extent, to forecast the outcome of your case by a computerised analysis of past events. Inevitably the sheer volume of US litigation and longevity of serving judges yields a tempting pool of data in which to try out analytical tools.

## Dangers of eliminating the human touch

There are of course many dangers to this approach. The trial process is inherently human, especially in the US where jury trials are the norm. In any jurisdiction, in a factually contentious dispute where credibility of witnesses is key, there may be little to be gained from analysing how past cases have unfolded. Indeed, a party that is too reliant on statistical analysis may be misled into taking the wrong message from it. For instance, recent data

shows that some three-quarters of applications to the English Commercial Court for a freezing injunction are successful, at least in part. But it would be wrong to infer that English judges give them out readily: there is a degree of self-selection before applications are even made to weed out weak and inappropriate applications that the final statistic cannot show. The track record of past cases cannot slavishly be applied to a new case.

Some in the legal sector are also uncomfortable with the notion of being measured in this way. Lawyers who know their win rates will be published will hardly be incentivised to accept instructions on “risky” cases. A new law in France has made it an offence to publish analytics on judicial decision making, punishable by up to five years imprisonment. But on the other hand, others find the data analytics approach compelling and the cost benefits difficult to look past. The Estonian government appears to be considering a pilot scheme to allow computerised models to adjudicate small contract disputes, in an effort to clear court backlogs. Undoubtedly, litigation funders who are keen to identify which investment opportunities present the best risk-reward profile, will look at whatever data may be available.

## Informing the ‘base rate’

In England, a prominent contribution to the litigation analytics space has come from Solomonic, a young start-up co-founded by commercial barrister Gideon Cohen (and which Herbert Smith Freehills has supported through its development). Solomonic provides a platform that is both careful and ambitious in its use of data. At present, it includes a wide range of analytics on the judgments of current and recently retired Commercial Court judges and allows the user to analyse those judgments in various ways.

“Litigation has historically been seen as immune to invasion by data analytics, with sceptics arguing that statistical analyses of past cases can never replace the expertise and intuition of seasoned practitioners.”



For instance, whilst the overall win rate for claimants across the database is currently about 60% (including partial successes), that figure drops to about 37% for actions founded in negligence (and drops further, to about 18%, when one focuses on banking and finance cases). It is also possible to look at whether a particular judge is an outlier—either generally or when faced with particular types of claim. Users can analyse which textbooks appear to be most frequently cited on a given issue, whether a judge has tended to follow precedent or distinguish prior cases, and which expert witnesses have been referred to in judgments (positively or otherwise).

The purpose here is not to say that a negligence claim in a banking litigation matter has only an 18% chance of succeeding: it may be far higher (or lower) than that. Rather, the point is to identify a "base rate", being the rate at which past actions of a similar type have succeeded, so the adviser can orient themselves, study past cases, consider what might make the present case different, and assess its

chances. If this data helps to encourage advisers and their clients to think about litigation risk in probability terms, there is value simply in that, as research has shown that parties facing significant uncertainty often display judgemental overconfidence, and fail to price downside risk properly.

Our Decision Analysis team, a group of numerically driven disputes lawyers, have been supporting clients in their decision making by building bespoke decision tree models to represent the risks inherent in the options under review. A critical component of the task is to attribute probabilities to each separate point of uncertainty in the litigation, rather than adopt an unscientific overall percentage prospects assessment. This rigorous analysis of probability is a task for which the identification of a base rate can be very helpful.

### **Not just about the merits**

Concerns about litigation risk do not stop with the merits: cost is another key issue where clients expect their lawyers to make a well-reasoned prediction about the future.

We have developed a cost prediction tool which uses the actual effort required to execute different phases of past cases, and cross-references these against other data points (value of claim, number of witnesses etc) to identify the relationships between lawyer hours (and therefore cost) and other data points.

Using the cost prediction tool when a new instruction is received, means that costs can be more reliably projected using estimates (or agreed assumptions) about the key variables that appear to be correlated with effort to execute. This can be used to support more reliable fixed or capped fee arrangements, or to enable the firm to cost proposals for contingency fee arrangements (where permitted and sought by the client). Either way, the tool uses the firm's substantial mine of timesheet data from past cases to help clients better manage their legal cost risk. Having been piloted for English litigation cases, a module is now being developed for global arbitration matters.



### The need for (informed) judgement

Litigation of complex commercial and financial disputes is sufficiently bound up in human idiosyncrasies that the role of the astute and experienced practitioner will always be paramount. The ultimate decision maker is going to be a human, and it perhaps stands to reason that (for non-commoditised work where each dispute is at least somewhat unique) clients will rely upon another human to help them assess what might happen in a negotiation/mediation or if the matter goes to trial. But that is not to say that humans cannot get guidance from the data and fine tune their assessments accordingly.

Solomonic co-founder Cohen sees commercial parties increasingly expecting their lawyers to take the data into account when applying their own expert analysis: "We know that businesses want their decisions to be informed by data. Litigation is a final frontier, which had relied solely on litigators' intuition and experience. Now, the growth of litigation analytics has given

lawyers and clients the data with which to inform analysis and guide strategy. That makes a material, incremental difference to the quality of the decision-making over the lifetime of a case." Our experience echoes this sentiment and we are leading the discussion on how to re-shape the delivery of legal advice in a disputes context to reflect the evolving data-informed (but not yet data-driven) paradigm. This poses challenges for in-house lawyers in banks and financial service providers to develop their respective skills and become comfortable handling new sources of information and receiving advice in new ways.



**Alexander Oddy**  
Partner, London  
T +44 20 7466 2407  
[alexander.oddy@hsf.com](mailto:alexander.oddy@hsf.com)



**Donny Surtani**  
Consultant, London  
T +44 20 7466 2216  
[donny.surtani@hsf.com](mailto:donny.surtani@hsf.com)

# Regulatory creep or convergence? Competition law authorities as financial services regulators

The division of regulatory responsibility between competition law authorities and traditional financial services regulators is becoming increasingly blurred. Banks are having to look at their “business as usual” activities through a new lens, knowing that both competition law and financial conduct regulators are watching closely and looking for opportunities to assert their authority.

Over the past year, competition law authorities across the globe have continued to scrutinise the financial services sector. This shows no sign of slowing. New prosecutions and investigations have been announced and competition authorities are actively building their expertise in financial services. At the same time, traditional financial services regulators have been given specific competition powers and mandates.

The increasing prominence of competition law as a regulatory risk has had significant implications for the day-to-day compliance activities and business practices of banks.

## Australia: double (regulatory) trouble for banks

The recent Royal Commission into banking and financial services in Australia was not kind to Australia’s financial conduct regulator, the Australian Securities and Investment Commission (ASIC), which was criticised for failing to take action against wrongdoing. In the wake of this criticism, there were calls from prominent ex-regulators and government advisors to give Australia’s competition authority, the Australian Competition and Consumer Commission (ACCC), a greater role in regulating banks.

The Royal Commissioner ultimately resisted recommending that any of ASIC’s remit be transferred to another regulator. However, this has not deterred the ACCC—its push into financial services has gathered steam over the past year and it clearly sees itself as having an important and ongoing regulatory role to play. Earlier this year it established a dedicated “Financial Services Competition Branch”, aided by AU\$35 million of

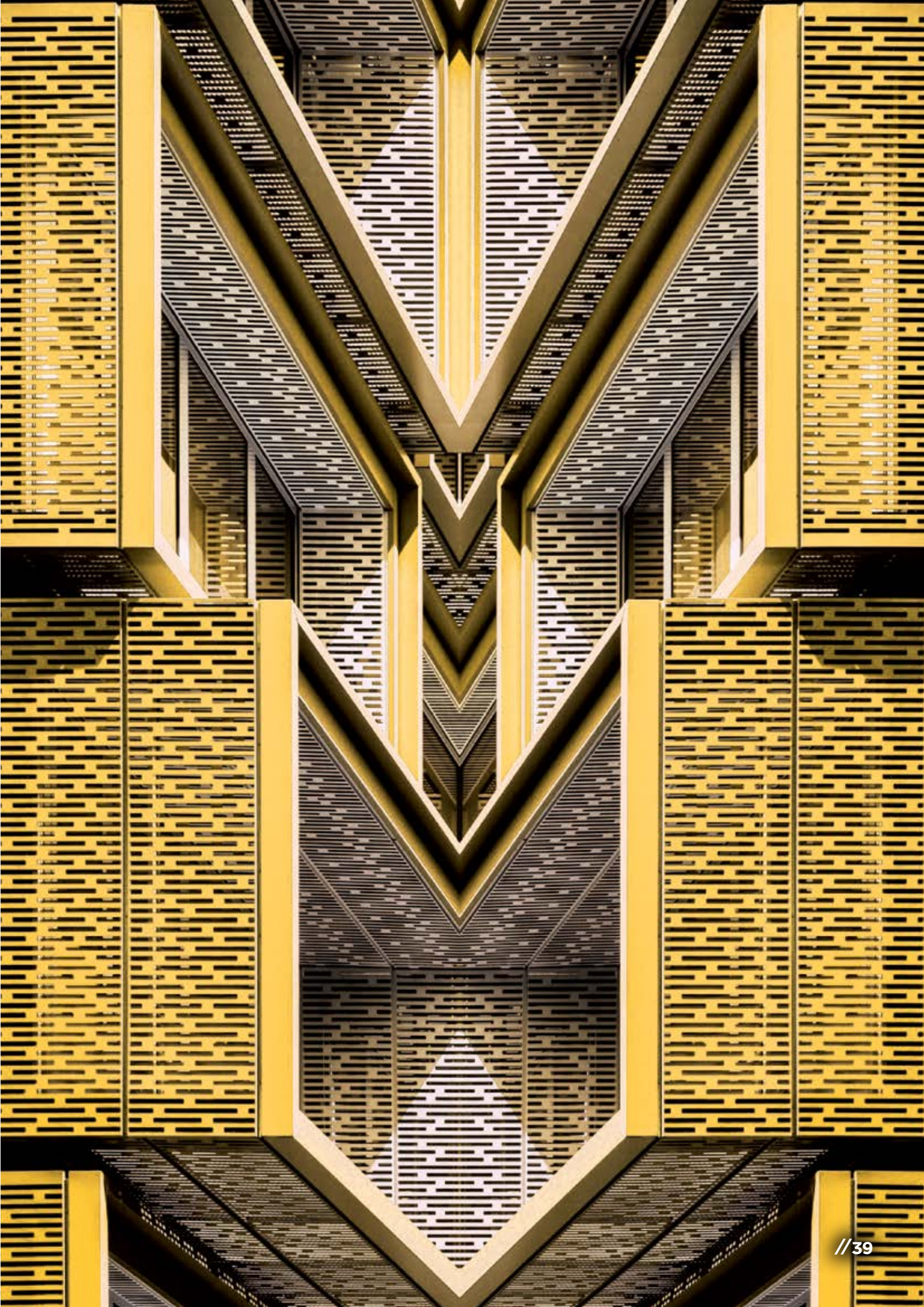
government funding granted in December 2018. This dedicated branch complements the ACCC’s existing Financial Services Unit which focuses on market studies in the financial services sector, such as the ongoing inquiry into foreign currency conversion services.

The ACCC anticipates that the Financial Services Conduct Branch will complete a number of in-depth investigations this year potentially resulting in court proceedings. The ACCC’s Chairman, Rod Sims, has said that two of the cases “go to the heart of competition in banking” and will target the “cosy oligopoly” of the financial services industry in Australia. Some of these cases reportedly stem from the ACCC’s inquiry into residential mortgage products which was finalised late last year.

The ACCC are already pursuing numerous criminal charges in the financial services sector. This includes charges against a business and five individuals for allegedly fixing the Australian Dollar/Vietnamese Dong exchange rates as well as charges against ANZ, Citibank, Deutsche Bank and six senior officers for alleged cartel conduct in relation to an ANZ share placement.

The ACCC’s interest in the financial services sector appears unlikely to wane any time soon. It recently lobbied the Australian Federal Government for a remit to conduct what has been described as a “deep dive” inquiry into competition issues in the financial services sector. The Government has pushed back on this request – so far – on the basis that the sector needs time to implement changes following the Royal Commission.

**“The ACCC are already pursuing numerous criminal charges in the financial services sector.”**





In addition to the threat of ACCC action, banks can expect more vigorous enforcement activity from ASIC, which is looking to reassert its authority. ASIC will now be obliged to consciously consider competition in the financial system, having been given an explicit reference to do so in legislative amendments that took effect late last year.

This convergence of regulatory oversight combined with an emboldened ACCC and an under-pressure ASIC has significantly raised the spectre of enforcement risk for banks operating in Australia.

### **United Kingdom: the FCA sharpens its competition tools**

The trend of competition law authorities pushing into financial services regulation is not unidirectional. Financial service regulators are also building their competition law expertise.

Unlike ASIC, the UK Financial Conduct Authority (FCA) has been granted powers to enforce alleged or suspected infringements of UK competition law occurring in the financial sector.

To date, the FCA has closely cooperated with the UK competition regulator, the Competition and Market's Authority (CMA), in the enforcement of anti-competitive conduct in the financial services sector. The FCA and the CMA reportedly each have an

ongoing investigation into the financial services sector. The CMA investigation is believed to be a probe into collusive conduct in bond trading, which the FCA passed to the CMA (rather than investigating it itself) due to limitations in the FCA's competition-related resources and expertise.

However, over the past 18 months the FCA has substantially ramped up its competition enforcement functions, having issued 11 "advisory" letters on suspected breaches of competition law and its first formal decision under its competition enforcement powers. It has also appointed a new director of competition, Sheldon Mills, in late 2018. Mr Mills was previously a senior director of mergers and state aid at the CMA.

Whilst the FCA has many of the powers generally granted to competition law regulators, it also has some unique advantages in enforcing competition law infringements. In particular, regulated firms have an explicit obligation to report suspected infringements to the FCA. In connection with its first competition enforcement decision earlier this year and fining two of the companies involved, the FCA also fined an individual under the Financial Services and Markets Act 2000 for involvement in relevant conduct, signalling a willingness to draw upon its broader range of enforcement powers in tackling competition law infringements.

### **Asian regulators look to follow suit**

Developments are more varied in Asia, where competition law authorities are relatively young and regulation of financial services remains more firmly with the more established financial sector regulators. However, there have been some notable developments in this space.

In Japan, the competition regulator (the JFTC) has reportedly clashed with the financial services regulator (the FSA) over the review of mergers between regional banks. Whilst the JFTC has been keen to apply general principles and practices to the review of regional banks, this has been at odds with the FSA's encouragement of consolidation amongst regional banks amidst unfavourable market conditions. Following very public remarks made by both regulators on the issue, the Prime Minister Shinzo Abe has reportedly directed his government to review the application of merger control to regional banks.

In China, the State Administration of Market Regulation (SAMR) has reportedly stated that financial services and fintech are potential target sectors for antitrust enforcement. There have been no public reports of enforcement actions to date. However, we understand that a number of financial institutions have received questionnaires from SAMR, indicating further developments may be on the horizon.





In Hong Kong, the Competition Commission recently conducted a series of training sessions for various government officials and regulatory authorities focussed on financial services, including the Securities and Futures Commission (SFC) and the Hong Kong Monetary Authority (HKMA). Whilst these regulators do not have concurrent jurisdiction under the competition law regime, it is expected that they will work closely with the Competition Commission in targeting anti-competitive behaviour. Whilst to date there have been no enforcement cases in the financial sector, the Competition Commission has rejected an application for a decision that the Code of Banking Practice should be exempt from the application of competition law.

### Managing these risks

In this climate of heightened regulatory attention, banks should expect to interact more frequently with competition law authorities. Appropriately managing these interactions can assist both the financial sector and the relevant authorities and beneficially set the tone of the wider relationship.

An effective competition law compliance program is also more important than ever for banks – both in terms of helping to avoid competition law infringements and to mitigate any enforcement action or penalty if an infringement does occur.

The pillars of an effective competition law compliance program for banks include:

- **Compliance policies, procedures and guidelines:** should be appropriately tailored so that the competition law compliance obligations are practically understood within the bank;
- **Training:** competition law training should also be practical and appropriately tailored and carried out on a regular basis;
- **Culture of compliance:** competition law compliance should be prioritised and encouraged from the most senior levels of the bank and clear action taken to address compliance failures;
- **Incentives:** should be consistent with competition law compliance (or at least not conducive to non-compliance);
- **Higher risk areas:** should be identified within the bank to consider whether more targeted and specific training or some form of monitoring is required.



**Sarah Benbow**  
Partner, Melbourne  
T +61 3 9288 1252  
[sarah.benbow@hsf.com](mailto:sarah.benbow@hsf.com)



**Susan Black**  
Partner, London  
T +44 20 7466 2055  
[susan.black@hsf.com](mailto:susan.black@hsf.com)



**Adelaide Luke**  
Partner, Hong Kong  
T +852 2101 4135  
[adelaide.luke@hsf.com](mailto:adelaide.luke@hsf.com)



**Andre Pretorius**  
Partner, London  
T +44 20 7466 2738  
[andre.pretorius@hsf.com](mailto:andre.pretorius@hsf.com)

# Data and cyber perils: personal exposure and inadequate insurance

As data and cyber dangers loom large and breaches and incidents become the new norm, the insurance market is in flux and there is a real risk of inadequate protection if great care is not taken to keep up with the pace of change.

In today's world, data breaches and cyber incidents in one form or another are increasingly common occurrences. The World Economic Forum has identified "data fraud or theft" and "cyber attacks" as the fourth and fifth most likely global risks in its 2019 Global Risks Report. This year has already seen the UK's data protection authority, the ICO, announce that it proposes to levy record-breaking fines for breaches of the General Data Protection Regulation (GDPR) on British Airways (£193 million) and Marriott International (£99 million) as a result of data breaches. However, whilst data and cyber incidents are towards the top of the risk register for many corporates, directors and officers can easily overlook the potentially significant personal exposures they can face as a result of these perils.

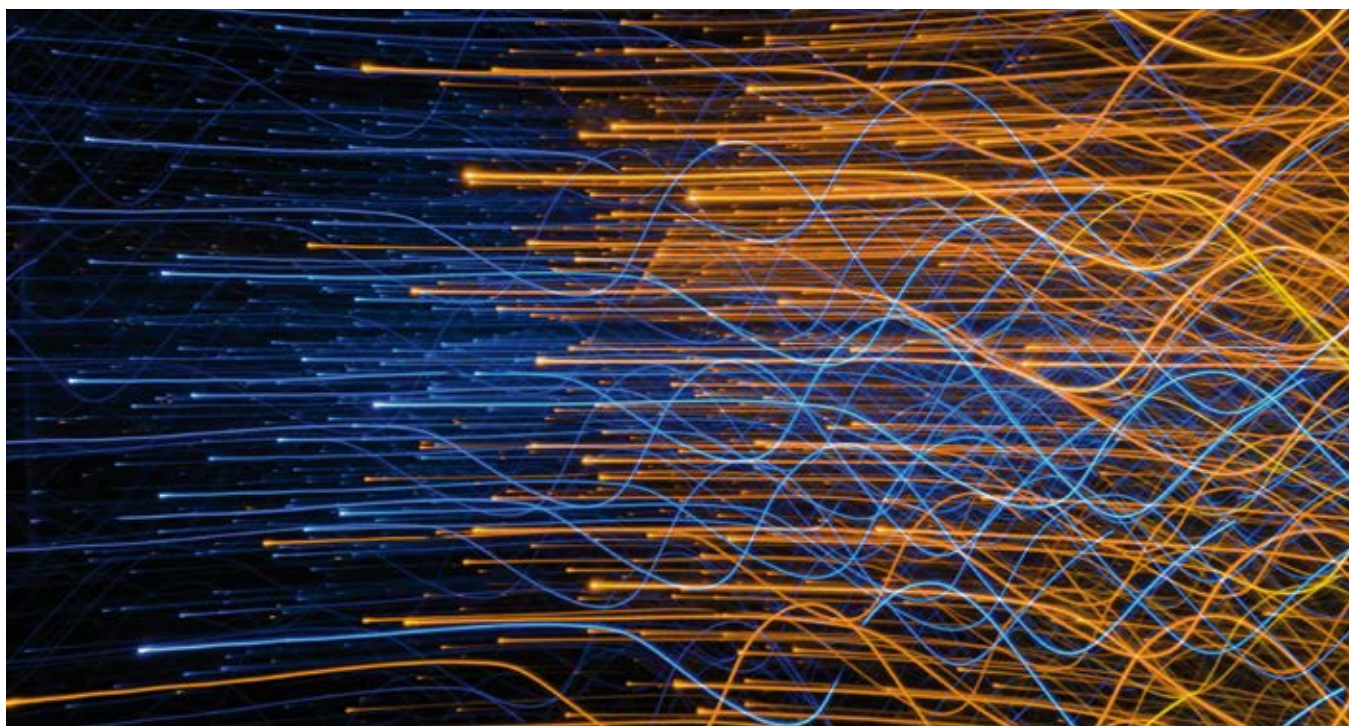
As we detail in this article, directors and officers can face claims, investigations and fines in their personal capacity as a result of data/cyber incidents. In many cases the company will indemnify or fund them against these exposures; but sometimes it may be unable or unwilling to do so. That can leave individuals having to self-fund very large sums unless they have appropriate insurance. Many will assume that their insurance team or broker has arranged adequate cover. That may be so, but the insurance market is evolving quickly; and the more that can be done by individuals to test that the best protections are in place, the better, particularly where personal assets are on the line.



## What risks do individuals face?

Data breaches or cyber incidents expose individuals to a range of possible losses. The initial exposure, irrespective of whether the individual is ultimately exonerated, could be liability for eye-wateringly high legal fees for defending the individual against regulatory investigations or claims. In some cases, such as cross-border investigations or class actions, costs can far exceed what an individual can afford. Fees could potentially be followed by further liabilities and fines. We look at some examples below:

- Regulatory investigations: in various jurisdictions, data protection authorities, financial services regulators and other official bodies have powers to investigate, sanction, or impose fines and penalties on individuals or require them to produce documents or attend interviews. In the UK, for example, the ICO can investigate and impose significant fines on individuals who are data "controllers" and "processors" for breaches of data protection law. The financial services regulators, the PRA and FCA, can likewise do so where prudential or conduct issues are involved. Financial services regulators around the globe, including those in the UK, Spain, Hong Kong and Australia, have in recent years also rolled out senior management accountability or individual accountability regimes, which aim to clarify the responsibilities of senior management and other key responsible individuals (with similar regimes expected



shortly in Singapore and Malaysia). These regimes make it easier to hold individuals to account for breaches of regulatory requirements occurring within their sphere of responsibility.

- Third party claims: directors and officers can face personal liability to third parties. Such claims fall broadly into two categories: (i) claims by persons directly affected by the incident (eg victims of the data breach); and (ii) claims by shareholders and investors for losses in share/investment value resulting from a data breach, for which they hold the management of the company responsible. Both types of claim may manifest as class actions. The first UK data breach class action is currently on appeal to the Supreme Court and in the US shareholder class actions are particularly common. Similar class actions can be anticipated in other jurisdictions. The associated costs and liabilities may reach both bet-the-individual and bet-the-company levels.
- Insolvency events: in a worst case scenario, a significant cyber/data breach could lead to a company's insolvency, and directors and officers may need to respond to third party claims and investigations by insolvency practitioners, regulators or other bodies. In these situations, any funding that the individual might have had from a solvent company would, in most jurisdictions, fall away. Insurance would be the only protection available to the individual.

**“Recently, a securities class action lawsuit was filed against FedEx in which the claimants allege that the company and certain directors did not fully disclose the extent of the disruption at its newly-acquired Netherlands based operation as a result of the NotPetya malware virus in 2017.”**

### The role of insurance

The potential exposures identified above can place a considerable financial burden on individuals. The importance of having adequate insurance cover for investigation and defence costs and other losses cannot be overstated. So where can it be found?

### Cyber insurance

Cyber insurance can be part of the answer. Policies may cover individuals for investigations and claims relating to data breaches and cyber incidents. Significantly, it is widely reported that cyber policy claims are being paid in large numbers despite the relative immaturity of the market in most jurisdictions other than the USA.

However, it would not be safe for individuals to presume they are comprehensively covered by their company's cyber policy. Many companies do not (yet) buy cyber insurance, although the trend is that they are increasingly doing so. Where companies do have such policies, coverage varies considerably. A few notes of caution then:

- Cyber policies do not cover all risks nor do companies necessarily purchase the widest possible cover. There are inconsistencies between whether coverage applies only for data breaches and security failures or also a broader range of perils such as system failures, payments made following non-invasive email scams, or for issues arising in the computer systems of a connected party such as an outsource provider or a contractor. Put simply, just because an incident is cyber related does not mean any particular cyber policy applies. Improvements, however, are being made to the scope and quality of wordings and there is greater market capacity and hence greater limits available in the market.
- The scope and quality of the wordings is not necessarily consistent between policies. For example, in some policies coverage does not apply for individuals (as opposed to the company); and where coverage does apply, it might not be possible to access the cover, particularly if the wording has not been reviewed to check it is written on best terms. On a poor wording, an individual might in principle be deprived of cover for relatively trivial or inadvertent non-compliance with policy terms.
- The amount of cover purchased or available varies and there might not be enough cover as aggregate limits or sub-limits are usually shared with other insureds.

```
PUBLIC INTERFACE IGUIFACTORY {  
    PUBLIC IBUTTON CREATOR;  
}
```

```
PUBLIC CLASS WINFACTORY implements IGUIFACTORY {  
    @Override  
    PUBLIC IBUTTON CREATOR  
    RETURN NEW WINBUTTON;  
}
```

```
PUBLIC CLASS OSXFACTORY implements IGUIFACTORY {  
    @Override  
    PUBLIC IBUTTON CREATOR  
    RETURN NEW OSXBUTTON;  
}
```

```
PUBLIC CLASS WINBUTTON implements IBUTTON {  
    @Override  
    PUBLIC VOID PAINT() {  
        SYSTEM.OUT.PRINTLN("WINBUTTON");  
    }  
}
```

```
PUBLIC CLASS OSXBUTTON implements IBUTTON {  
    @Override  
    PUBLIC VOID PAINT() {  
        SYSTEM.OUT.PRINTLN("OSXBUTTON");  
    }  
}
```

```
PUBLIC CLASS MAIN {  
    PUBLIC STATIC VOID MAIN(String[] args) {  
        IGUIFACTORY FACTORY = new WinFactory();  
        IBUTTON button = FACTORY.CREATOR();  
        button.PAINT();  
    }  
}
```

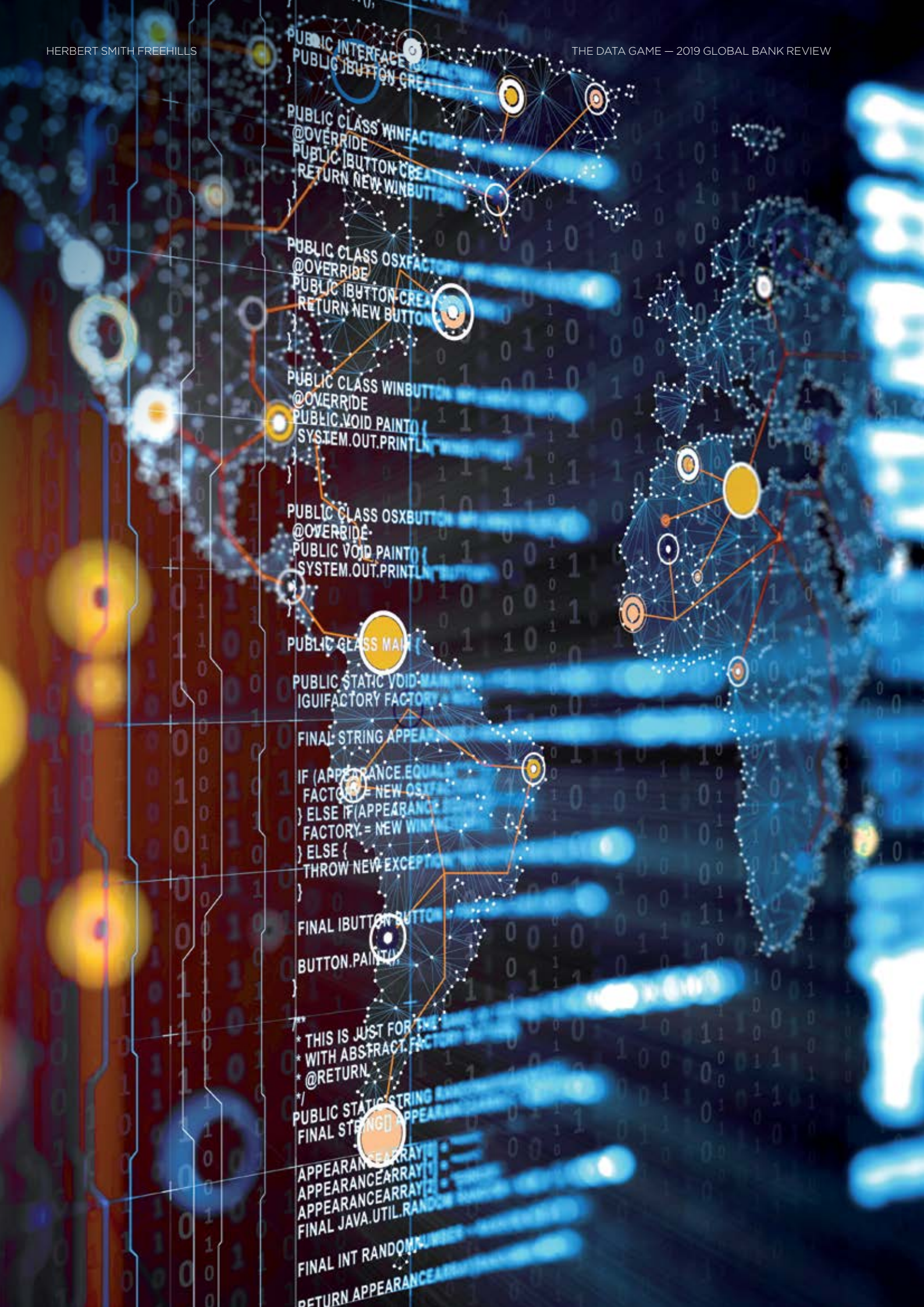
```
FINAL STRING APPEARANCE_ARRAY1[] = {"Apple", "Mac", "iMac", "MacBook", "MacBook Pro", "MacBook Air", "Mac mini", "Mac Pro", "Mac Studio", "Mac SE", "Mac Studio", "Mac SE", "Mac mini", "MacBook Air", "MacBook Pro", "iMac", "Mac", "Apple"};  
FINAL STRING APPEARANCE_ARRAY2[] = {"Apple", "Mac", "iMac", "MacBook", "MacBook Pro", "MacBook Air", "Mac mini", "Mac Pro", "Mac Studio", "Mac SE", "Mac Studio", "Mac SE", "Mac mini", "MacBook Air", "MacBook Pro", "iMac", "Mac", "Apple"};  
FINAL JAVA_UTIL_RANDOM RANDOM = new JAVA_UTIL_RANDOM();  
FINAL INT RANDOM_NUMBER = RANDOM.nextInt(100);  
RETURN APPEARANCE_ARRAY1[RANDOM_NUMBER];
```

```
FINAL IBUTTON BUTTON = FACTORY.CREATOR();  
BUTTON.PAINT();
```

```
*/  
* THIS IS JUST FOR THE PURPOSE OF THE EXAMPLE  
* WITH ABSTRACT.FACTORY.FACTORY  
* @RETURN  
*/
```

```
PUBLIC STATIC STRING RANDOM_NUMBER = String.valueOf(RANDOM_NUMBER);  
FINAL STRING[] APPEARANCE_ARRAY1 = {"Apple", "Mac", "iMac", "MacBook", "MacBook Pro", "MacBook Air", "Mac mini", "Mac Pro", "Mac Studio", "Mac SE", "Mac Studio", "Mac SE", "Mac mini", "MacBook Air", "MacBook Pro", "iMac", "Mac", "Apple"};  
FINAL STRING[] APPEARANCE_ARRAY2 = {"Apple", "Mac", "iMac", "MacBook", "MacBook Pro", "MacBook Air", "Mac mini", "Mac Pro", "Mac Studio", "Mac SE", "Mac Studio", "Mac SE", "Mac mini", "MacBook Air", "MacBook Pro", "iMac", "Mac", "Apple"};
```

```
FINAL JAVA_UTIL_RANDOM RANDOM = new JAVA_UTIL_RANDOM();  
FINAL INT RANDOM_NUMBER = RANDOM.nextInt(100);  
RETURN APPEARANCE_ARRAY1[RANDOM_NUMBER];
```



- Not all losses may be insurable irrespective of what the policy says. In particular, in some jurisdictions, such as England, there is debate over whether some or all data protection fines are insurable; and in other jurisdictions it is clear they are not. Even that might be fixed if the policy were to assess coverage for fines and penalties by reference to laws under which they are insurable.

Despite the issues above, our impression is that it is rare that a director or officer asks not only whether the company has purchased cyber insurance but also whether the policy has sufficiently broad scope, good quality wording and financial limits to provide maximum protection for individuals as well as the company.

#### Directors and officers (D&O) liability insurance

D&O policies typically respond to claims and investigations against individuals in their capacity as directors and officers of the company. They may provide complementary cover to cyber insurance. Currently, D&O insurance will often provide “silent” or “non-affirmative” cover against losses stemming from data or cyber risks, even when not referenced directly in the policy wording. For example, if a director or officer were investigated for regulatory breaches regarding oversight of cybersecurity or systems in the company, or asked to attend an interview with an official body enquiring into the same incident, cover may be available under the D&O policy’s regulatory investigations cover, absent an exclusion for cyber related incidents.

D&O insurance is more of a commoditised product than cyber insurance and best in class wordings have expanded considerably in the soft (buyer friendly) market that has prevailed in recent years. But caution ought to be exercised: change may be afoot for two reasons. First, the D&O market has now started to harden considerably in light of poor loss ratios reportedly driving up prices and causing insurers to scrutinise claims more carefully. Marsh reported a 5.6% global increase in D&O premiums in Q1 2019. This could possibly cause the scope of wordings, including for cyber risk, to contract if the harder market continues to prevail over time. Individuals will therefore need to scrutinise their cover wording more carefully.

Second, there is pressure on insurers in some jurisdictions to deal with coverage for cyber perils expressly and to price it. In

January 2019 the PRA wrote to the major UK insurers urging them again to address the market’s non-affirmative exposure to cyber risks; and in June, the International Underwriting Association published two model clauses intended for use in non-cyber policies which operate to exclude cover for any “Cyber Loss”.

The current position in the London market has been explained by Francis Kean, Executive Director, FINEX at international insurance broker Willis Towers Watson, as follows:

**“Insurers are grappling with their exposure to non-affirmative cyber cover. Wordings are being updated in the D&O market to include affirmative cyber cover and we aren’t (yet) seeing cyber exclusions. However, the devil may be in the detail: if broad cover is the intention, then care must be taken to ensure that affirmative cover clauses do not inadvertently carve out or sub-limit cyber cover that already existed. On the other hand, in other lines, such as crime and professional indemnity, we are already seeing insurers starting to narrow coverage for cyber perils”.**

#### What can be done about insurance gaps and inconsistencies?

The answer is straightforward: as the market moves, it will be essential to review wordings year on year to ensure that, price permitting, best in class cover is purchased at all times. In particular, a close watch should be applied to whether coverage against data and cyber-related claims has been expressly or inadvertently narrowed—and the question asked whether any new covers or extensions are available.

Individuals may be covered on an affirmative or non-affirmative basis against losses arising from data and cyber perils under a wide range of other policies (such as PI insurance in relation to financial and professional services claims and investigations). While a detailed look at those policies is outside the scope of this article, the overall message is

that the company’s insurance programme must be reviewed holistically. Insureds ought to identify:

- the potential data and cyber risks;
- the policies under which such risks are intended to be covered; and
- any gaps in relation to material risk.

This review should be stress tested as part of the company’s wider crisis or risk management strategy, examining what losses would arise that may impact individuals in a given factual scenario and what policy coverage may apply.

#### Conclusion

As the insurance market adjusts to account for looming data and cyber perils, it is crucial that directors and officers ensure that they carefully assess their personal and corporate risk profile and match this risk assessment with an appropriate combination of insurance products. Cyber insurance is a starting point but will not provide adequate protection by itself. As such, insurance arrangements should be examined holistically to ensure that, to the extent it can reasonably be achieved, no areas of exposure are left out of scope under one policy without being addressed under another.



**Greig Anderson**  
Partner, London  
T +44 20 7466 2229  
[greig.anderson@hsf.com](mailto:greig.anderson@hsf.com)



**Alexander Oddy**  
Partner, London  
T +44 20 7466 2407  
[alexander.oddy@hsf.com](mailto:alexander.oddy@hsf.com)



**Antonia Pegden**  
Senior Associate, London  
T +44 20 7466 2530  
[antonia.pegden@hsf.com](mailto:antonia.pegden@hsf.com)

# Away from prying eyes: data security in international dispute resolution

The dispute resolution process is an attractive target for hackers and a key—but frequently underestimated—area of risk. During any formal dispute resolution process, banks create and share large amounts of data. If this data were to become public, it could cause reputational damage, influence share prices or provoke regulatory scrutiny.

International arbitration is an increasingly popular method of dispute resolution in international finance transactions. In 2018, 29% of all cases in the London Court of International Arbitration (LCIA) involved parties in the banking and finance sector, a higher proportion than any other single sector<sup>1</sup>

## Where does your data go?

Arbitration is a private method of dispute resolution where a tribunal, usually of one or three arbitrators, makes a binding decision on a dispute. Arbitration clauses typically provide that the arbitration will be conducted under the rules of, and administered by, a neutral arbitral institution.

A typical arbitration involves various participants ranging from the parties, law firms, and arbitrators, to arbitral institutions and third parties such as experts, witnesses and service providers.

Each of these participants in the arbitration process is likely to hold your data. Clients and their legal advisers will generally share information and discuss drafting points and strategy by email. Pleadings, evidence, expert reports and witness statements are also often exchanged electronically with arbitrators, the other side's legal advisers, experts, witnesses, arbitral institutions and third party service providers. Document review and production regularly takes place on electronic data hosting platforms, usually owned by third party service providers. An award will be drafted, discussed and exchanged between the different members of an arbitral tribunal and may also be sent to the arbitral institution administering the arbitration, before being sent to counsel and the parties.



1. LCIA 2018 Annual Casework Report

“ Each participant represents a fresh target for cyber attackers and a potential point of weakness in relation to the security of arbitration data.”



Once data has been sent electronically in the course of an arbitration, the sender can no longer monitor or ensure its security.

While some arbitrators operate from within law firms or chambers, others are sole traders who may have in place more limited cybersecurity protections. The same could be said of expert witnesses and some fact witnesses who receive and store data on their personal devices. Careful consideration needs to be given by all stakeholders in an arbitration to avoid such participants being a weak link in the chain of custody.

According to the UNCTAD (United Nations Conference on Trade and Development), there have been at least 80 investor-state arbitration proceedings relating to the financial service sector.

### Ensuring your data is secure

In international arbitration, parties can expect to have significant input on procedural matters. It is not yet commonplace for tribunals to make orders on cybersecurity, although this is likely to change, and therefore the onus (and the opportunity) to suggest measures to protect data in the arbitration will be on the parties. Below are some practical steps banks can take working with external counsel in an arbitration.

#### Cybersecurity risk assessment

Before commencing an arbitration (if the bank is the claimant) or immediately once the bank is notified of an arbitration (if it is the respondent), consider carrying out a risk assessment with your legal advisers. This should involve an assessment of whether data likely to be relevant to the arbitration is

- commercially sensitive,
- involves customer, employee or other third party data that the banks may be required to protect (eg under the EU General Data Protection Regulation (GDPR)), or
- confidential data or data that is market sensitive. The risk assessment should inform what approach should be taken to collection, storage and review of that data.

## Increasing use of arbitration in banking and finance

“Agreeing to arbitration allows a party to avoid having to litigate in a jurisdiction in whose courts it does not have confidence, while producing an arbitral award which may have an advantage over a foreign court judgment at the enforcement stage in many jurisdictions.”

2018 ISDA ARBITRATION GUIDE

“Financial institutions tend to favour arbitration when: (i) the transaction is significant or particularly complex;

(ii) confidentiality is a concern; (iii) the counterparty is a state-owned entity; and (iv) the counterparty is in a jurisdiction where the recognition of foreign judgments is problematic or where it is expected that enforcement of an arbitral award under the New York Convention will be easier than enforcement of a court judgment.”

THE INTERNATIONAL CHAMBER OF COMMERCE'S COMMISSION REPORT ON FINANCIAL INSTITUTIONS AND INTERNATIONAL ARBITRATION (MARCH 2018)

How likely is it that international arbitration will increasingly be used to resolve cross-border disputes in banking and finance?

LIKELY 56%

NO VIEW 23%

UNLIKELY 21%

QUEEN MARY UNIVERSITY OF LONDON AND WHITE & CASE, 2018 INTERNATIONAL ARBITRATION SURVEY: THE EVOLUTION OF INTERNATIONAL ARBITRATION

Where cybersecurity is critical, it may be a consideration in nominating an arbitrator. It may be sensible to send a checklist of cybersecurity-related questions to arbitrators before or immediately after nomination or appointment. The answers to such a checklist (or a failure to answer) might lead to concerns that need to be addressed before the arbitrator's appointment is confirmed.

#### Who might want your data?

- Hacktivists seeking to further a social or political cause.
- State Actors pursuing information to advance their own political agenda.
- Cybercriminals perpetrating cyber attacks for monetary gain.
- Unscrupulous opponents in the proceedings.

#### Implementing cybersecurity measures

Following a risk assessment, the next step will be to formalise measures to protect data in the arbitration. This may take the form of a protocol signed by the parties and the tribunal or an order passed by the tribunal covering matters such as:

- Specifying how communications will take place between the parties and the tribunal, between the tribunal members and with other participants; through password protected email or by secure file transfer systems
- Using a secure platform for the transmission of large volumes of documents relating to the case or sensitive documents





- Reducing the use of paper documents (which represent a confidentiality risk) and/or a protocol for their storage
- Redaction of certain categories of data or particularly sensitive information unrelated to the dispute
- Reducing access to certain categories of data
- Reducing unnecessary disclosure
- Breach detection, notification and mitigation
- Allocation of liability and penalties that will apply in the event of a breach (although this may be hard to negotiate in practice)
- Insurance against breach
- Document retention and destruction

**Increasing focus on cybersecurity in international arbitration**

- The International Bar Association and the International Council for Commercial Arbitration have set up a task force to develop practical guidance on data protection in international arbitration.
- The International Chamber of Commerce has published a note to parties emphasising the importance of complying with the GDPR in arbitration proceedings, including in relation to collecting data from witnesses, experts and other individuals.
- The Hong Kong International Arbitration Centre has adopted new rules allowing service of documents via a secure online platform instead of over email.
- Herbert Smith Freehills is spearheading a collaboration with a number of global law firms to look at the development of an arbitration-specific online platform to help protect arbitration data in future.



**Nicholas Peacock**  
Partner, London  
T +44 20 7466 2803  
[nicholas.peacock@hsf.com](mailto:nicholas.peacock@hsf.com)



**May Tai**  
Partner, Hong Kong  
T +852 2101 4031  
[may.tai@hsf.com](mailto:may.tai@hsf.com)



**Brenda Horrigan**  
Partner, Sydney  
T +61 2 9225 5536  
[brenda.horrigan@hsf.com](mailto:brenda.horrigan@hsf.com)

# IBOR transition: a data challenge

It is clear that the transition from London Inter-bank Offered Rate (LIBOR) together with all other significant Inter-bank Offered Rates (IBORs) is “happening” and represents a significant challenge for all financial institutions. Firms will require significant support in the transition and, in respect of the transition involving legacy financial product contracts, at the core of the exercise will be the efficient and effective collection and management of data from hundreds of thousands of existing contracts.

## IBOR transition

IBOR transition teams across the globe are currently grappling with the difficulties posed by transition from IBOR benchmark rates to risk free rate alternatives (RFRs). For most, if not all, this will involve a large due diligence and data collation exercise to assess their exposure, before defining the parameters of a repapering and customer outreach programme. This is happening at a time when the goal posts are still moving and there is a high level of uncertainty across all affected markets. The best prepared are now engaging with suppliers to develop large-scale transition programmes comprising data collation, due diligence, data analysis and client outreach platforms.

In this article, we consider a number of the key issues involved in IBOR transition through a data lens. In particular, we look at the scope of the due diligence and repapering process for financial institutions, the insights shared by the regulators as to what represents good practice in this regard, and potential risks for financial institutions even where they are sufficiently prepared in the eyes of the regulator.

## Preparedness for LIBOR discontinuation

Regulators globally have been dialling up the pressure on financial institutions to make sure they are taking appropriate steps to prepare for life after IBORs cease. For LIBOR, this was the recent message from Andrew Bailey, Chief Executive of the Financial Conduct Authority (FCA), at a LIBOR Transition Briefing in New York on 15 July 2019.<sup>1</sup> The speech marked two years since the FCA first confirmed that it will no longer compel banks to continue to provide quotes for LIBOR after the end of 2021.<sup>2</sup>

Given the significance of LIBOR in London across major currencies and the IBOR manipulation scandals, the FCA and Prudential Regulation Authority (PRA) are generally regarded as leading the pack on IBOR discontinuation. However, because of the widespread reliance on LIBOR and the sheer scale of the repapering task involved, it is perhaps unsurprising the FCA and PRA have reported a real divergence across the UK market in terms of preparedness for LIBOR discontinuation. In particular, this is because of the need to transition not just new business, but also to convert outstanding legacy LIBOR contracts, which has been recognised by the regulators to be harder in some markets than others (eg the bond market, where consent solicitations are required). The same difficulties apply to markets in other jurisdictions, where regulators are pursuing their own means to bring about the required market changes, and in relation to other IBORs. For example, in Hong Kong, the Hong Kong Monetary Authority is actively engaging with market participants to make preparations for IBOR transition.

## Due diligence and repapering exercise

Many firms have commenced their IBOR due diligence as a first step in transitioning legacy contracts (being the focus of this article noting that transition will not only impact contracts, but also pricing and risk models etc), adopting different approaches to outsourcing some or all of the work involved, depending on variables such as the volume of contracts, value and complexity.

For a number of financial institutions, the due diligence phase will involve large scale data collation across multiple jurisdictions

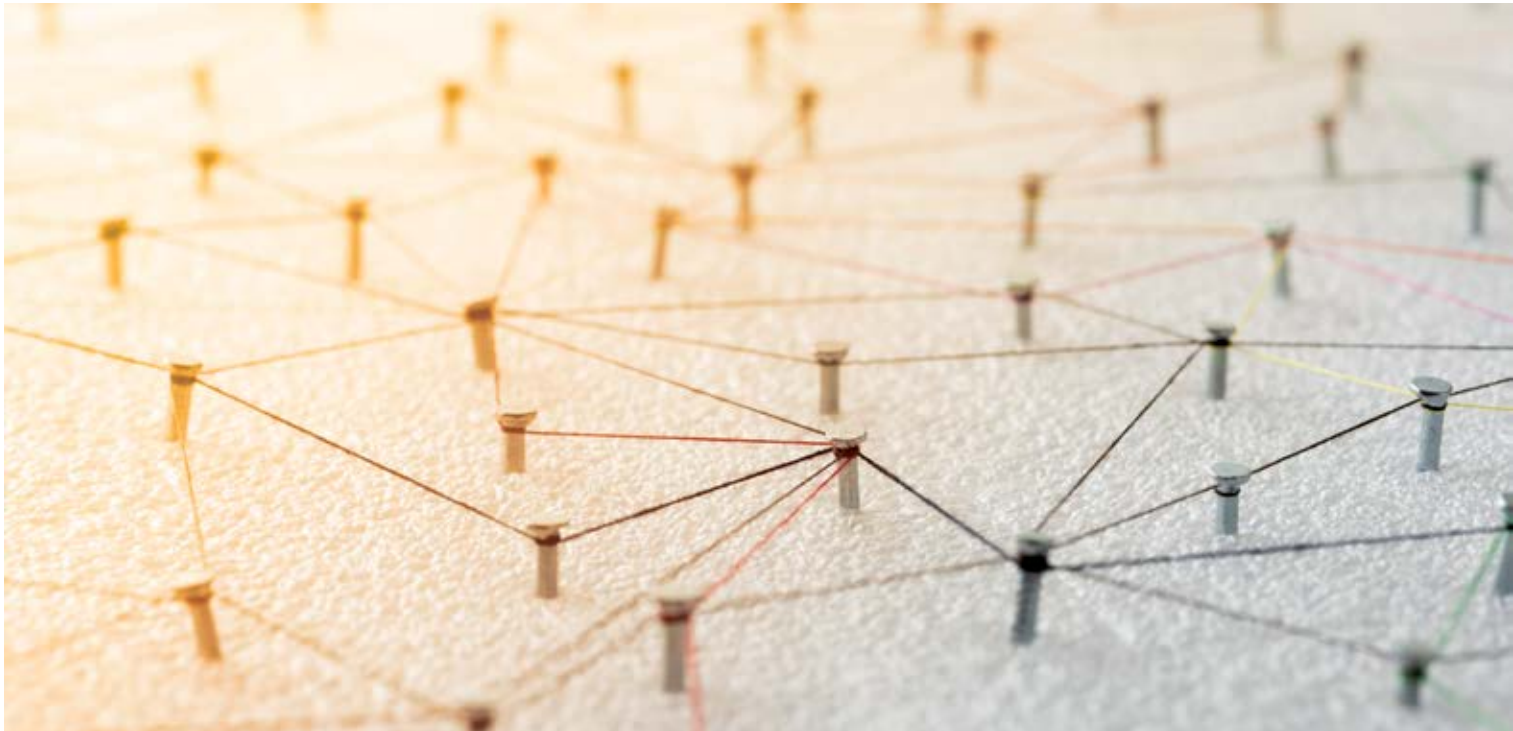
and involving various IT platforms (including legacy systems) and data sources (potentially including hard copy data). Some firms may be able to automate part of this process, but the position may vary across products and many will need to extract the key information needed manually in order to understand the risk of exposure (eg maturity dates, notional values and the existing contractual fallbacks which will operate if there is no amendment). This will require considerable time and effort, and may affect the accuracy of the data collated and therefore the robustness of the firm’s risk assessment of IBOR transition.

The due diligence process will also present specific data protection challenges. Data privacy legislation around the world, including the General Data Protection Regulation (GDPR) in Europe, may restrict the international transfer of personal data without appropriate safeguards being in place. In addition, jurisdictions such as Hong Kong have data localisation laws requiring data or a copy of data to be stored “in-country”. Firms will need specialist advice how to transfer data around the world within their organisations in a compliant manner for their transition programmes.

The documents collated will then need to be sampled to identify defined categories of contract, based on parameters such as product type, fallback wording, maturity date etc. This will enable the total population of contracts to be categorised accordingly. It is possible to use technology to adopt a systematic approach where appropriate, although this is unlikely to remove the need for detailed manual oversight, particularly

“Whilst NatWest has closed a number of SONIA-referenced loans on a bilateral basis and is currently engaged in developing a SONIA-referenced club transaction, we would welcome the intervention of the FCA in facilitating conversations between market participants to establish wider SONIA-referenced lending capability in both the bilateral and syndicated markets, to lead on timing and to work on eradicating blockers. Customer and market awareness of how SONIA works is growing but a wider cascade of SONIA conventions would encourage greater adoption across cash markets.”

JAMIESON THROWER, NATWEST, LIBOR TRANSITION  
BUSINESS LEAD FOR COMMERCIAL BANKING



in the early stages when the scoping parameters are set and as yet there is no one-size-fits-all technology to perform these exercises as each firm will have its own needs and approach.

**“NatWest has commenced its due diligence exercise. The use of technology on this workstream is instrumental in organising the information contained in a large universe of affected contracts so that we can inform our repapering strategy and work with affected customers in the most effective way.”**

**JAMIESON THROWER, NATWEST, LIBOR TRANSITION BUSINESS LEAD FOR COMMERCIAL BANKING**

This could remove some documents from the scope of the repapering exercise, for example if they contain an acceptable fall-back or if they mature before 2021 (or sufficiently soon after that date to be low risk). For those remaining contracts, firms will need to move into the client outreach and repapering phase. This will involve more strategic aspects, such as identifying replacement fallback provisions (based on industry solutions if available); categorising products by sophistication of customer, complexity, value etc; the appropriate manner of client execution/consent; and method of client communication, to name a few.

It is worth considering the scale of the challenge which IBOR transition represent – firms will have thousands (if not tens of thousands) of contracts which contain reference to IBORs across different products and geographies. Unless the regulatory stance softens, all these legacy contracts need to be amended, involving a large scale due diligence and client outreach programme. The financial industry has grappled with similar large scale repapering exercises recently (such as GDPR and Markets in Financial Instruments Directive (MiFID II)) however, the difference with IBOR transition is that the amendments will result in economic changes to existing transactions, which places greater emphasis on the need for firms to conduct careful diligence and customer outreach programmes.

### Insights from the regulators

Globally, regulators are at different stages of engagement with their respective markets. As mentioned, UK regulators have indicated that not all financial institutions are taking appropriate action to prepare for LIBOR discontinuation, identifying areas of varying practice across market participants.

In September 2018, the FCA and PRA issued a “Dear CEO”<sup>3</sup> letter to large banks and insurance companies, asking for details of those firms’ preparations and actions to manage transitioning from LIBOR to alternative interest rate benchmarks (SONIA in the UK).

In a joint statement<sup>4</sup> setting out their key observations from responses received, the

regulators commented that in “stronger responses” firms were identifying reliance on and use of LIBOR beyond a firm’s balance sheet exposure and assessing (for example) whether LIBOR is present in the pricing, valuation, risk management and booking infrastructure firms use. The regulators are looking for transition project plans with sufficient granularity of detail and the nomination of a senior executive responsible for transition (covered by the Senior Manger Regime) whose role is clearly defined.

They expect firms to identify prudential and conduct risks; and to manage those risks on the basis of LIBOR discontinuation at the end of 2021 rather than assuming it will continue in some form thereafter.<sup>5</sup>

In other jurisdictions, similar forms of Dear CEO letters have been issued asking for confirmation of IBOR discontinuation preparedness, most notably in mainland Europe<sup>6</sup>, Hong Kong<sup>7</sup> and Australia<sup>8</sup>. No feedback has yet been published by regulators in these jurisdictions. However, it is not expected that the responses will differ markedly from those in the UK given that many of the financial institutions involved operate globally.

### Litigation risks

The demise of IBORs presents risks which will impact even the most prepared financial institutions. This is because, absent a statutory fix, there will likely be a rump of legacy contracts which is not possible to amend even if efforts are made to do so. This risk is recognised by regulators and has been

referred to as the “tough legacy” question.<sup>9</sup> It is likely to affect different markets to varying degrees. For example, theoretically the risk should be lower in the derivatives market, where the International Swaps and Derivatives Association (ISDA) intends to publish a protocol or set of protocols to amend legacy contracts. However, this will only take effect where both parties to the contract have adhered to the protocol, and there are various reasons why parties may not adhere to that protocol.

A significant source of risk is likely to stem from the fact that converting LIBOR contracts into contracts referencing alternative RFRs is not “present value neutral”, because the alternative RFR may be inherently lower than LIBOR. The potential for value transfer (even allowing the potential for a fixed spread adjustment to mitigate this) means that some counterparties may be reluctant to switch, or see it as an opportunity to renegotiate the commercial deal. This could lead to a stand-off between the parties, reducing the effectiveness of attempts to amend legacy contracts.

Fast forward to a world where LIBOR no longer exists, and the result will be that those legacy contracts then rely upon legacy fallback language which was never intended to operate following a permanent cessation of the reference rate. Whatever the applicable fallback, this presents significant litigation risk for financial institutions because of the clear potential for “winners” and “losers” as a result of the transition from LIBOR.<sup>10</sup> Dependent on the type of fallback, there is also a risk of claims on the basis that the nature of the relevant product is substantially altered.

## Evolving regulatory landscape

Regulators have repeatedly emphasised that market participants should operate on the basis that LIBOR will cease at the end of 2021. However, in Andrew Bailey’s speech on 15 July 2019, he identified the possible option of a legislative fix for legacy contracts, eg redefining LIBOR as the relevant RFR plus fixed spread. Although he emphasised that this option could not be relied upon as being deliverable, he suggested that there would be consultation on this option in 2019.

**“NatWest supports Andrew Bailey’s recent comments in this regard and we will actively participate in the legislative consultation when published. We also see the establishment of a consistent adjustment spread, together with appropriate fallback wording for existing loan products, as key to accelerating the adoption of SONIA-referenced lending and the development of a syndicated market.”**

**JAMIESON THROWER, NATWEST,  
LIBOR TRANSITION BUSINESS LEAD  
FOR COMMERCIAL BANKING**

A number of market-specific consultations are also in progress this year, for example ISDA’s consultation on pre-cessation issues for LIBOR and the precise approach for the spread adjustment to mitigate the value transfer in derivative contracts.

## Conclusion

The uncertainties may not impact the data collection stage, but have the potential to affect both due diligence and data analysis, as well as any client outreach. For example, if primary legislation is an option for legacy contracts, this would of course impact risk assessment, as it would significantly alter the transition risk for legacy contracts entered into prior to a specified date. Market participants are therefore in the unenviable position of carrying out a due diligence and repapering process while simultaneously monitoring the evolving regulatory landscape which will define the parameters of the very client outreach programme they are designing. The transition itself is likely to take years not months, and occupy a significant proportion of the market, as participants adapt to the consequences of an IBOR-free world.



**Hannah Cassidy**  
Partner, Hong Kong  
+852 2101 4133  
[hannah.cassidy@hsf.com](mailto:hannah.cassidy@hsf.com)



**Harry Edwards**  
Partner, London  
+44 20 7466 2221  
[harry.edwards@hsf.com](mailto:harry.edwards@hsf.com)



**Nick May**  
Partner, London  
+44 20 7466 2617  
[nick.may@hsf.com](mailto:nick.may@hsf.com)



**Jenny Stainsby**  
Partner, London  
+44 20 7466 2995  
[jenny.stainsby@hsf.com](mailto:jenny.stainsby@hsf.com)



**Gabrielle Wong**  
Partner, London  
+44 20 7466 2144  
[gabrielle.wong@hsf.com](mailto:gabrielle.wong@hsf.com)



**Ceri Morgan**  
Professional Support  
Lawyer, London  
+44 20 7466 2948  
[ceri.morgan@hsf.com](mailto:ceri.morgan@hsf.com)

1. Andrew Bailey, speech on 15 July 2019: LIBOR: preparing for the end, [www.fca.org.uk/print/news/speeches/libor-preparing-end](http://www.fca.org.uk/print/news/speeches/libor-preparing-end)
2. Andrew Bailey, speech on 27 July 2017: The future of LIBOR, [www.fca.org.uk/news/speeches/the-future-of-libor](http://www.fca.org.uk/news/speeches/the-future-of-libor)
3. PRA & FCA, Dear CEO Letter, [www.fca.org.uk/publication/correspondence/dear-ceo-letter-transition-from-libor-banks.pdf](http://www.fca.org.uk/publication/correspondence/dear-ceo-letter-transition-from-libor-banks.pdf)
4. PRA & FCA Joint Statement, Firms’ preparations for transition from London InterBank Offered Rate (LIBOR) to risk-free rates (RFRs), [www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2019/firms-preparations-for-transition-from-libor-to-risk-free-rates.pdf?la=en&hash=EA87BD3B8435B7EDF25A56C932C362C65D516577](http://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2019/firms-preparations-for-transition-from-libor-to-risk-free-rates.pdf?la=en&hash=EA87BD3B8435B7EDF25A56C932C362C65D516577)
5. See our banking litigation blog post for a more detailed analysis of this feedback: [www.hsfnotes.com/bankinglitigation/2019/06/06/libor-discontinuation-fca-thematic-feedback-on-responses-to-dear-ceo-letter/](http://www.hsfnotes.com/bankinglitigation/2019/06/06/libor-discontinuation-fca-thematic-feedback-on-responses-to-dear-ceo-letter/)
6. European Central Bank Letter, Banks’ preparation with regard to interest rate benchmark reforms and the use of risk-free rates, [www.bankingsupervision.europa.eu/press/letterstobanks/shared/pdf/2019/ssm.benchmark\\_rate\\_reforms\\_201907.en.pdf?8f331a1bb36298a22adcb65e5c41bc8b](http://www.bankingsupervision.europa.eu/press/letterstobanks/shared/pdf/2019/ssm.benchmark_rate_reforms_201907.en.pdf?8f331a1bb36298a22adcb65e5c41bc8b)
7. Hong Kong Monetary Authority Letter, Reform of Interest Rate Benchmarks, [www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190305e1.pdf](http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190305e1.pdf)
8. Reserve Bank of Australia, Regulators Urge Financial Institutions to Plan for LIBOR Transition, [www.rba.gov.au/media-releases/2019/mr-19-12.html](http://www.rba.gov.au/media-releases/2019/mr-19-12.html)
9. Andrew Bailey, speech on 5 June 2019: Last Orders: Calling Time on LIBOR, [www.bankofengland.co.uk/events/2019/june/last-orders-calling-time-on-libor](http://www.bankofengland.co.uk/events/2019/june/last-orders-calling-time-on-libor)
10. Discussed further in our article: [www.herbertsmithfreehills.com/latest-thinking/libor-is-being-overtaken-will-it-be-a-car-crash](http://www.herbertsmithfreehills.com/latest-thinking/libor-is-being-overtaken-will-it-be-a-car-crash)

# The emergence of the “super-regulator”: the lasting legacy of the Australian Banking Royal Commission

Although the Australian Government has announced its intention to take action on all 76 recommendations set out in the Royal Commission’s final report, none of these are set to cause the same tectonic shift in the sector than that caused by the changing approach of regulators, particularly the Australian Securities and Investments Commission (ASIC).

The Royal Commission’s final report, for all of the publicity and commentary it generated, contained themes and recommendations that were not unexpected or new in the global landscape. It is a sign of changing times that, even in jest, the new chair of Australia’s corporate regulator, ASIC, could be likened to a fictional superhero by Senator Hume, Chair of the Senate Economics Legislation Committee.

Previously, ASIC has been described as a “timid and hesitant”<sup>1</sup> regulator with an “ineffective enforcement culture”<sup>2</sup>, “that rarely went to court to seek public denunciation of and punishment for misconduct.”<sup>3</sup> However, under intense scrutiny, ASIC now has increased resources (including AU\$400 million in additional funding); has hired more staff; and adopted a “why not litigate?” approach. It has set about sharpening its enforcement culture and is planning the functional separation of its enforcement activities by setting up an Office of Enforcement (a separation that the US Securities and Exchange Commission (SEC) has had in place since 1972). These, and other initiatives, may bring aspects of ASIC’s work more in line with regulatory approaches adopted by its larger international counterparts.

The Australian Prudential Regulation Authority (APRA), criticised in the Royal Commission for never having taken court action, has also expressed an increased willingness to use its enforcement tools. Based on the intent shown to date (outcomes yet to be seen), stronger regulator enforcement has the potential to be the real lasting legacy of the Australian Banking Royal Commission.

## The shift towards stronger regulator enforcement

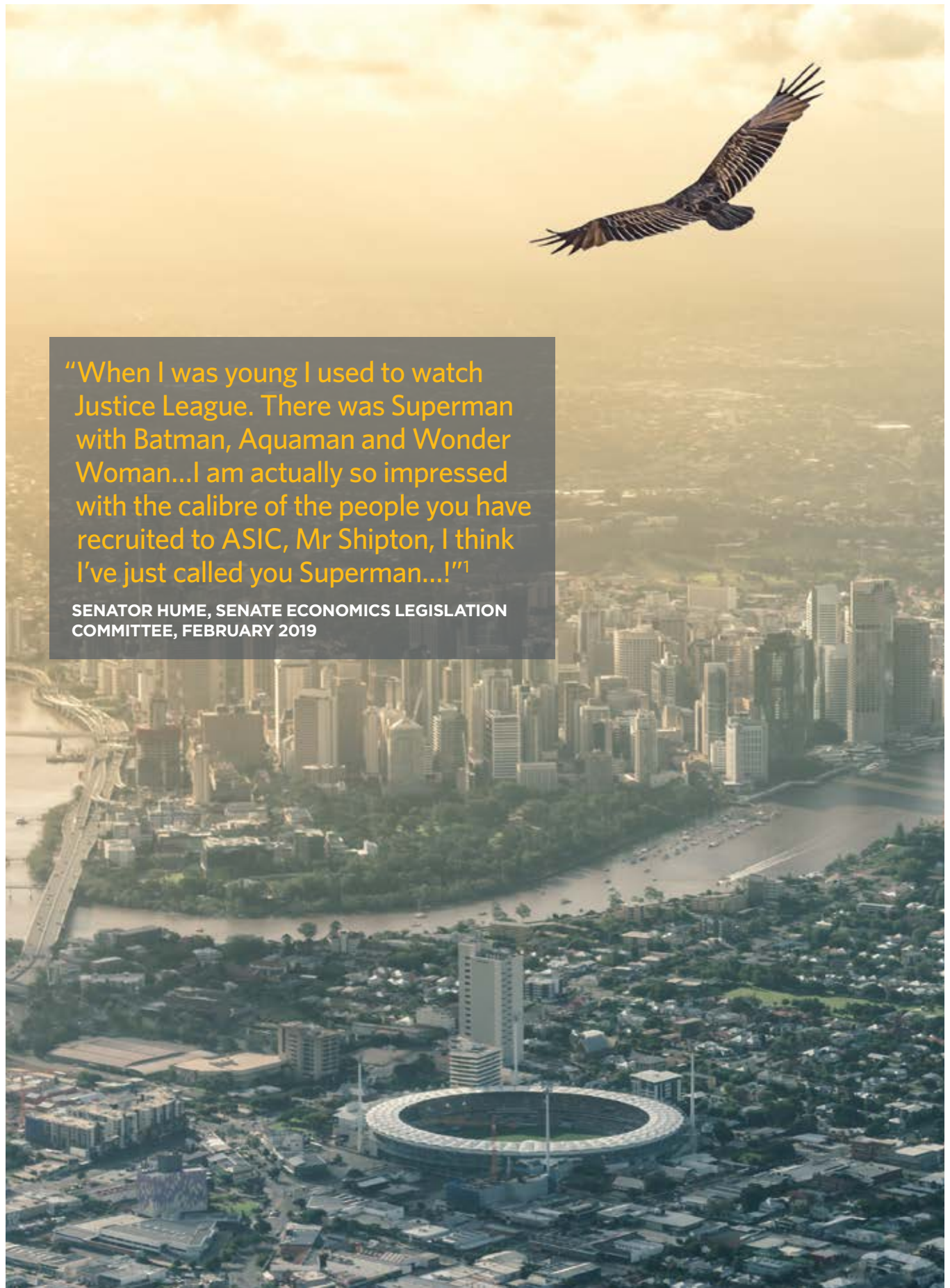
While ASIC did not wait until the release of the Royal Commission’s final report on 4 February 2019 to ramp up its investigations, the shift has been a noticeable one. We are seeing a sustained increase in the number of investigations and monitoring initiatives targeted at financial institutions, as well as innovation in the approach.

As the number of ASIC investigations increases, more criminal and civil proceedings are expected. The fallout from the Royal Commission is, largely, yet to be played out in the courts, but there is little doubt, it will come. Aside from the sheer volume of matters, there has also been a shift in approach. The banks are facing increased and more significant demands for production of documents—in less time—than ever before.

In a world of “big data”, and having invested significantly in data analytics, ASIC seems unafraid of the large volume of materials it is receiving in response to regulatory notices.

This new environment allows little scope for banks to negotiate with the regulator. Previously, it was common for investigations to resolve in either an enforceable undertaking; or if proceedings were commenced, in a settlement involving some limited admissions and an agreed penalty, generally subsequently endorsed by the courts. The Royal Commission, however, was highly critical of ASIC’s use of negotiated outcomes.





“When I was young I used to watch Justice League. There was Superman with Batman, Aquaman and Wonder Woman...I am actually so impressed with the calibre of the people you have recruited to ASIC, Mr Shipton, I think I’ve just called you Superman...!”<sup>1</sup>

**SENATOR HUME, SENATE ECONOMICS LEGISLATION COMMITTEE, FEBRUARY 2019**



As at June 2019 ASIC staff had **been onsite** in one or more financial institutions for a total of **164 days**.

Since ASIC's Close and Continuous Monitoring Program launched in October 2018, ASIC had held **meetings with more than 550 banking staff** at all levels.



As part of ASIC's Corporate Governance Taskforce, as at June 2019, across **21 entities**;

ASIC received and reviewed over **43,000 documents**; and

completed **97 interviews** with CEOs, chairs, board risk committee chairs, and other senior risk, audit and governance executives.



**“Negotiation and persuasion, without enforcement, all too readily leads to the perception that compliance is voluntary.”**

**COMMISSIONER HAYNE,  
ROYAL COMMISSION FINAL REPORT**

### “Super-regulators” in action

ASIC’s public rhetoric has been clear: negotiated outcomes will now only be available for a limited range of enforcement matters. In addition, once in court, ASIC may adopt a new strategy of either going to trial, or taking admissions from the banks on liability, before allowing the court to decide the penalty. This approach of taking matters to trial may lead to some significant public losses for ASIC. The early signs are that ASIC is ready after responding to a recent major court failure by describing it as a “test case”. Whether ASIC can maintain that position over the medium to long term remains to be seen.

In parallel, ASIC’s Close and Continuous Monitoring Program has seen financial institutions required to open their doors to an intensive supervisory approach which places ASIC staff onsite within the bank.

ASIC’s Corporate Governance Taskforce (set up during the Royal Commission) has also been hard at work to detect cultural failings that lead to misconduct. In a novel approach, the taskforce asked directors and officers to participate in a survey designed by psychologists and requested that psychologists attend board meetings to observe cultural dynamics.

### How to respond?

Despite the intense burden that this shift in enforcement approach has placed on financial institutions, there has—so far—been little appetite to challenge or seek to limit the scope of the demands (perhaps, other than in seeking to maintain claims for legal professional privilege). As the heightened investigatory and enforcement activity continues, the general response has been to resource and respond, being flexible to new types of supervision initiatives. These are usually compulsory processes after all, and cooperation can help shrink the size of the stick faced at the end of it all, particularly given recent changes to the law on civil penalty, with penalties for companies increasing to AU\$525 million for any new misconduct.

It is early days in this changing landscape, and we are yet to see whether this less compromising approach will pay dividends for ASIC. Cultural change is difficult and takes time, whether for a regulator or a financial institution. Banks in other countries have had to weather a similar storm, and have found ways to survive the initial onslaught and resettle into a new normal with the regulator, including one that leaves room for negotiation.



**Andrew Eastwood**  
Partner, Sydney  
T +61 2 9225 5442  
[andrew.eastwood@hsf.com](mailto:andrew.eastwood@hsf.com)



**Damian Grave**  
Partner, Melbourne  
T +61 3 9288 1725  
[damian.grave@hsf.com](mailto:damian.grave@hsf.com)



**Tania Gray**  
Partner, Sydney  
T +61 2 9322 4733  
[tania.gray@hsf.com](mailto:tania.gray@hsf.com)



**Jacqueline Wootton**  
Partner, Brisbane  
T +61 7 3258 6569  
[jacqueline.wootton@hsf.com](mailto:jacqueline.wootton@hsf.com)



**Leah Watterson**  
Senior Associate, Melbourne  
T +61 3 9288 1849  
[leah.watterson@hsf.com](mailto:leah.watterson@hsf.com)

1. Senate Economics References Committee Performance of the Australian Securities and Investments Commission, June 2014 at xviii and Hansard, Parliamentary Joint Committee on Corporations and Financial Services, Friday 19 October 2018 at p 4.
2. Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, Final Report 4 February 2019 at p 428.
3. Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, Interim Report, Executive Summary at xix.





## HERBERTSMITHFREEHILLS.COM

---

### **BANGKOK**

Herbert Smith Freehills (Thailand) Ltd

### **BEIJING**

Herbert Smith Freehills LLP  
Beijing Representative Office (UK)

### **BELFAST**

Herbert Smith Freehills LLP

### **BERLIN**

Herbert Smith Freehills Germany LLP

### **BRISBANE**

Herbert Smith Freehills

### **BRUSSELS**

Herbert Smith Freehills LLP

### **DUBAI**

Herbert Smith Freehills LLP

### **DÜSSELDORF**

Herbert Smith Freehills Germany LLP

### **FRANKFURT**

Herbert Smith Freehills Germany LLP

### **HONG KONG**

Herbert Smith Freehills

### **JAKARTA**

Hiswara Bunjamin and Tandjung  
Herbert Smith Freehills LLP associated firm

### **JOHANNESBURG**

Herbert Smith Freehills South Africa LLP

### **KUALA LUMPUR**

Herbert Smith Freehills LLP  
LLP0010119-FGN

### **LONDON**

Herbert Smith Freehills LLP

### **MADRID**

Herbert Smith Freehills Spain LLP

### **MELBOURNE**

Herbert Smith Freehills

### **MILAN**

Herbert Smith Freehills Studio Legale

### **MOSCOW**

Herbert Smith Freehills CIS LLP

### **NEW YORK**

Herbert Smith Freehills New York LLP

### **PARIS**

Herbert Smith Freehills Paris LLP

### **PERTH**

Herbert Smith Freehills

### **RIYADH**

The Law Office of Mohammed Altammami  
Herbert Smith Freehills LLP associated firm

### **SEOUL**

Herbert Smith Freehills  
Foreign Legal Consultant Office

### **SHANGHAI**

Herbert Smith Freehills LLP  
Shanghai Representative Office (UK)

### **SINGAPORE**

Herbert Smith Freehills LLP

### **SYDNEY**

Herbert Smith Freehills

### **TOKYO**

Herbert Smith Freehills