BUDDLE FINDLAY
NEW ZEALAND LAWYERS

CYBER SECURITY AND RISKS IN THE FINANCIAL SECTOR

Allan Yeoman, Partner, Buddle Findlay

BFSLA Annual Conference, Brisbane, 2 September 2017

1. INTRODUCTION

1.1 A number of high-profile incidents involving banking and other financial service organisations in recent months and years have highlighted the risks posed and the damage that can be caused by cyber attacks and vulnerabilities in technology.

1.2 Those incidents are reflective of a general trend across business and society at large: an unfortunate but real side-effect of living and working in a connected economy is that the valuable information stored or accessible online – trade secrets, intellectual property, personal information – will be accessible to others, unless steps are taken to secure it.

1.3 For banking and financial services organisations, the risks are greater again, as unauthorised access to or manipulation of a bank's systems can directly facilitate theft or unauthorised transfer of funds.

1.4 This paper examines:

- the types of cyber attacks and threats to which a financial services provider may be subject;
- the generic laws and regulations that potentially give rise to liability following a cyber attack;
- the causes and details of the Bangladesh Central Bank / New York Federal Reserve 'heist' in February 2016; and
- regulation and requirements specific to the financial services sector in a range of jurisdictions.

2. CATEGORISING CYBER ATTACKS

2.1 Cyber attacks can be categorised in a number of ways (eg, by the methods used, the type(s) of target, or the identity of the actors behind them), but it is useful to consider them in the context of the motivation(s) behind them and what the attackers hope to achieve. In a broad sense, most attacks can be placed into one of the following categories:

- **Theft of personal information for identity fraud purposes**, for example:
  - *LinkedIn* – 167 million account credentials (email addresses and passwords)
  - *Yahoo* – 500 million user accounts compromised
  - *Ashley Madison* – 37 million user accounts compromised
  - *Unicredit Banca* – loan account data of 400,000 customers stolen
- **Theft of credit card data**, for example:
  - *Target* – 40 million credit and debit card details compromised

- *Home Depot* – 56 million credit card numbers and 53 million email addresses stolen

- **Disruption or denial of service for ransom**, for example:
  - *Wannacry* – over 300,000 computers infected and $300 to $600 ransom demanded (in Bitcoin)
  - *TalkTalk* – 156,000 customer accounts (including credit card details) compromised and £200,000 in Bitcoin ransom demanded

- **Political disruption or activism**, for example:
  - *Petya* – primarily on Ukrainian organisations (first thought to be ransomware, but now believed to be attempt to cripple Ukrainian infrastructure and economy)
  - *US Office of Personnel Management* – names, DOB, social security numbers, and criminal background checks of 22.1 million federal employees
  - *Democratic National Committee*

- **Theft of money**, including:
  - Phishing scams
  - *Bangladesh Central Bank and NY Federal Reserve*

2.2 The banking sector is in some ways unique in that it is a prime target for all of these objectives. Banks are in a unique position in that they are the trusted custodians not only of their customers' money, but also of extensive confidential and personal information of a large number of individual and corporate customers, most of which is extremely sensitive with the potential to cause significant harm and distress. Similarly, for those attacks where the objective is disruption or denial of service rather than theft (whether for political or pecuniary gain), the impact on critical banking infrastructure and systems can have severe downstream effects for many other businesses, and an economy in general if it leads to a loss of confidence in the financial services sector.

2.3 Therefore, while much of the focus of this paper is on the Bangladesh Central Bank heist, it would be inaccurate to construe cyber risks as being limited to the theft of money. Banks are as much of a target for other types of target as any other business or government agency, and in most cases, more of a target.

3. BANGLADESH CENTRAL BANK / NEW YORK FEDERAL RESERVE HEIST

Background facts

3.1 The broad facts of this attack are reasonably well-known, but the details and exact chain of events are less frequently discussed. The Appendix to this paper sets out a detailed timeline of how the attack was carried out, allowed to occur and ultimately discovered.

3.2 The key points of the heist, carried out over four days in February 2016, are as follows:

- The Bangladesh Central Bank (**BCB**) held an account with the Federal Reserve Bank of New York (**NY Fed**) in which World Bank aid monies were deposited.

- Hackers installed malware on the SWIFT Access Alliance software used by the BCB to send instructions and messages to the NY Fed, via the SWIFT network. The malware covered up the hackers' tracks by redirecting messages sent by the NY Fed, and disabling print functionality for SWIFT messages.
- The hackers used credentials of legitimate BCB employees to initiate and send fraudulent transfer requests to the NY Fed via the SWIFT network. In total, the hackers sent 35 transfer instructions totalling almost US$1 billion. US$101 million was transferred (US$20 million of which was later successfully reversed) before the attack was detected and the transfers halted. To date, just over $US15 million has been recovered.
- The missing funds were deposited into a Philippines bank account that the attackers had opened some 9 months earlier. From there, they disappeared into the casino industry. The BCB and Bangladesh Government considered proceedings against the NY Fed and various other parties, but ultimately dropped the suits.
- No one has been arrested or charged in connection with the attack, though several individuals have been charged with money laundering offences in the Philippines. While not confirmed, there is evidence of connections between the attackers and North Korea and whispers that BCB employees may have been complicit.

Causes and contributing factors

3.3 While those facts alone have been seen by many in the financial services sector as cause for alarm, a closer examination of the details of the attack provides further insights:

- The hackers timed their attack over a weekend, and making use of the time difference between Bangladesh and New York and an Islamic holiday in Bangladesh. In doing so, they were able to capitalise on confusion and miscommunication between BCB and the NY Fed, ensure that the transfers would go undetected by the BCB and that any attempts by the NY Fed to verify the transfer requests would be futile.
- The BCB and NY Fed did not have in place any secondary means of communicating with each other, other than by SWIFT messaging (which had been compromised by the attack). The NY Fed did not attempt to contact BCB via any other means when their SWIFT messages went unanswered, and when BCB tried contacting the NY Fed when their suspicions were first raised, they used a generic email address on the NY Fed's website, which was not monitored over the weekend.
- While the attack was conducted via the SWIFT network, most commentators point to poor security measures at BCB that allowed the installation of the malware in BCB's systems and access to legitimate SWIFT credentials.
- The NY Fed typically checked for suspicious activity the day after transfers, rather than as they occur, meaning that, once detected, it was too late to reverse the transactions or reverse the funds. In addition, both parties missed a number of warning signs:
    - The initial 35 requests were rejected because of missing details, before being corrected and resubmitted by the attackers, and accepted by the NY Fed.

- Most of the payments were made to individuals rather than institutions.
- BCB had, on average, been sending less than one SWIFT request per day, rather than 35.
- BCB did not realise the printing issue was a sign of a much more serious situation.

Lessons learned[1]

- The technical vulnerabilities in this case were in BCB's system and processes. No matter how secure the SWIFT network may be, a bank will be still vulnerable if hackers are able to breach local security measures and/or access employee credentials.
- SWIFT should be informed of breaches so they can better understand the frequency and seriousness of such breaches and respond appropriately.
- Banks should have contingency plans for breaches via the SWIFT network, including alternate forms of communication, and considering monitoring over holiday periods (traditionally fraud attempts are mostly executed during holiday seasons).[2]
- Financial institutions should have red flag procedures that catch suspicious requests and are dealt with before the request is approved and processed.

4. GENERAL REGULATORY AND LEGAL RISK

4.1 The BCB heist was obviously very specific in its objectives – the theft of money. However, as noted above, cyber attacks are carried out with all manner of objectives, causing a range of different types of harm. In addition to the financial, operational and reputational impacts, an organisation can therefore be exposed to a range of legal risks. The extent of these will depend on a number of factors:

- the nature of any assets or information that are lost or compromised (eg, personal information, trade secrets, bank account details);
- the volume and sensitivity of those assets or information;
- whether the organisation is a public sector organisation or subject to sector-specific regulation (eg, health information);
- what contractual obligations the organisation owes to third parties in respect of the assets or information (eg, customers); and
- how the organisation responds to and deals with the breach.

4.2 The first and most crucial step in any organisation's security strategy will therefore be in understanding the obligations and responsibilities it has relating to assets and information it holds.

4.3 In a general sense, an organisation could be exposed to liability in the following areas:

[1] For a more detailed analysis of prevention measures, see PwC's report: http://www.pwc.com/us/en/financial-services/financial-crimes/publications/assets/swift-bangladesh-robbery-2016.pdf

[2] https://www.netguardians.ch/news/2016/8/16/hackers-use-of-swift-network-means-banks-worldwide-need-deeper-layers-of-security-defense

Breach of contract

4.4 Failure to keep systems, assets or information secure may put an organisation in breach of contractual obligations owed to third parties, whether customers, partners or suppliers, including:

- breach of specific 'data security' obligations;
- breach of confidentiality obligations relating to the third party's information;
- breach of generic provisions relating to service standards (for example) the use of 'reasonable skill and care';
- inability to perform contractual obligations as required, due to unavailability of systems or information (unless saved by a broad force majeure clause); and
- triggering of indemnity obligations relating to loss of data, breach of confidentiality or putting the third party in breach of applicable laws (such as privacy legislation).

4.5 Contractual obligations may also be relevant to the way in which an organisation reacts to a security incident, to the extent contracts set out requirements for notifying the counterparty.

4.6 A third party cyber attack (such as ransomware or other denial of service) may lead to a consideration of whether force majeure provisions come into play, relieving a bank of obligations it may have otherwise had to customers, and the exposure it would have had as a result of its inability to act on its customers' instructions. However, a force majeure clause should not be thought of as a 'get out of jail free' card: the wording of most force majeure provisions would require, as a pre-condition, that reasonable steps have been taken to avoid the effect of the force majeure event, which leads back to an assessment of whether the bank's security practices and measures were adequate or 'appropriate'. Even where such a pre-condition is not spelt out, it may be implied or read in by the requirement in applicable consumer protection legislation for consumer contract terms to be 'fair'.

4.7 Going forward, it is likely that more and more consumer-facing contracts will expressly deal with an organisation's inability to perform as a result of cyber attacks, so that there is certainty around the extent of obligations and exposure.

Banco del Austro v Wells Fargo Bank

4.8 A claim of this nature is currently being played out in litigation between Banco del Austro and Wells Fargo.

4.9 In *Banco del Austro v Wells Fargo Bank*,[3] the District Court of the Southern District of New York considered an application to dismiss proceedings brought by Banco del Austro against Wells Fargo for not detecting fraudulent orders received via the SWIFT network.

4.10 In January 2015, Wells Fargo authorised the transfer of USD$12 million following receipt of fraudulent SWIFT communications from the Ecuadorean bank (the circumstances were almost identical to those that occurred during the BCB heist). Banco del Austro argued that, even though it was Banco del Austro's system that was hacked, Wells Fargo should bear the loss of the cyber

[3] *Banco del Austro v Wells Fargo Bank* 1:2016cv00628, 18 October 2016 (SDNY).

attack because it should have recognised that there was something wrong with the SWIFT messages it received (even though these messages were authorised SWIFT messages).

4.11 The motions for breach of contract and negligence were dismissed, but the motion under the Universal Commercial Code (**UCC**) was not. The decision is significant as it is a test of whether a correspondent bank could be held liable for authorising authenticated SWIFT transfer messages. Under section 4-A-202 of the UCC, the risk of loss is allocated to the bank that received and honoured the unauthorised orders (the correspondent bank). However, section 4-A-202(2) provides an exception where a bank and its customer agree that the bank will verify the authenticity of orders pursuant to a security procedure. So long as the security procedure is "commercially reasonable", the customer must bear the loss so long as the bank proves that it accepted the payment order in good faith and in compliance with the security procedure.[4] The Court held that it would need to determine the "commercial reasonableness" of the agreed-upon security procedure, or whether Wells Fargo complied with reasonable commercial standards of fair dealing when it processed the orders, and so could not dismiss the motion.[5] The case is yet to progress to a full hearing.

4.12 Further details regarding that case and its factual background are set out in the second case study in the Appendix.

Breach of privacy legislation

4.13 If a security breach involves a loss of, or unauthorised access to, personal information, then there may be a breach of obligations under applicable privacy legislation to take measures to keep that information secure. Under New Zealand's Privacy Act 1993, Information Privacy Principle 5 addresses security measures for organisations in possession of personal information:

> *An agency that holds personal information shall ensure –*
>
> *(a) that the information is protected, by* ***such security safeguards as it is reasonable in the circumstances to take****, against –*
>
> *(i) loss; and*
>
> *(ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and*
>
> *(iii) other misuse; and*
>
> (b) *that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.*

4.14 An agency's security obligations turn on what is "reasonable in the circumstances". This mirrors the standard of care required in privacy legislation in comparable jurisdictions (such as the EU, UK and Australia), which call for organisations to take 'reasonable', 'appropriate' or 'adequate' security measures. The lack of any prescriptive requirements can present a challenge for organisations looking for certainty as to whether they have taken sufficient action, and a continuous assessment of evolving risks and responsibilities.

[4] At 2.
[5] At 6.

4.15 In response, a number of privacy regulators have issued guidance relating to security measures that should be put in place to keep personal information secure. For instance,

- In New Zealand, the Privacy Commissioner has published a 'Data Safety Toolkit' which provides guidance to organisations on how this obligation should be applied, and how security breaches can be prevented and dealt with: https://www.privacy.org.nz/news-and-publications/guidance-resources/data-safety-toolkit/
- The Office of the Australian Information Commissioner has published a *Guide to securing personal information*: www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

4.16 It should be noted that the recommendations and guidance contained in these publications set out the measures that are relevant to protection of personal information only, and (to some extent) a prediction of how privacy regulators may respond following a security incident. However, privacy regulators' recommendations may not go far enough if an organisation is obliged to secure more sensitive systems, assets or information.

4.17 In New Zealand at least, financial penalties for breach of the Privacy Act are reasonably modest (except in the most flagrant of cases). However, a data loss affecting many thousands or hundreds of thousands of customers could create significant aggregate liability, and it is likely that financial penalties available for breaches of the Privacy Act will increase over the coming years as New Zealand privacy law is reformed.

4.18 There have been significant penalties handed down in other jurisdictions for breaches of comparable privacy legislation following security incidents – for example, TalkTalk was fined £400,000 by the (UK) Information Commissioner's Office.

Breach of directors' duties

4.19 Company directors' duties may be relevant should a security incident reveal poor corporate governance and/or a lack of sound information management practices. In particular, duties under applicable companies legislation that require directors to act in the best interests of the company, or exercise a reasonable level of care, skill and diligence, may become a relevant consideration in the assessment of any board decisions around the level of investment or focus applied to cyber security preventative measures. Those sorts of duties would suggest that, at a minimum, directors should:

- ensure that security against cyber threats is a regular agenda item;
- be educated and aware of information security issues and what 'best practice' involves;
- be informed about the potential risks there could be to the company;
- be continuously assessing how the steps taken by the company compare with steps taken by other companies facing the same level of risk;
- understand the company's legal obligations and requirements (legislative, contractual and regulatory); and
- invest appropriately in safeguarding a company's information and systems.

4.20 The (New Zealand) Institute of Directors has recently published a 'Cyber-Risk Practice Guide', which sets out five key principles to assist directors to understand and approach cyber risk at board level.[6] As indicated by the guide, "directors must understand cyber risk as part of enterprise risk" and a failure to do so could well be seen as a breach of director's duty.

Common law claims

4.21 In addition to claims in contract, cyber security breaches could also give rise to claims against banks in respect of:

- common law banker/customer confidentiality obligations; and
- breaches of the banker/customer mandate.

Banker/Customer Confidentiality

4.22 While the Privacy Act covers obligations in respect of individuals, there has been a long held duty for banks to keep all customer information confidential (except where the banks are required to disclose by law, public duty, to protect the bank's own interests or with client consent). This applies to all customers and most relevantly to corporate customers of banks (*Tournier v National Provincial and Union Bank England* [1924] 1 KB641).

4.23 If, as a result of a cyber security breach of a bank's system, confidential information relating to corporate customers is disclosed, then potential damages claims against banks arising from that disclosure could be substantial.

Banker/Customer Mandate

4.24 The banker/customer relationship is essentially a debtor/creditor relationship (where the customer has deposits with the bank).

4.25 While the relationship between the banker and the customer is essentially contractual, it has been long held that provisions are implied into that relationship because of its special nature which can only be negated by express provisions to the contrary (*Tai Hing Cotton Mill Limited v Liu Chong Hing Bank Limited* [1986] AC80).

4.26 A key element of a banker's duty of care is to only act on the valid instructions of the customer in making payments from their account. In the case of cheques, for example, a bank is liable if it pays out from a customer's account on the basis of a forged cheque. That liability arises at common law no matter how good the forgery and regardless of the whether the customer took care to secure its cheque books, although liability is often now modified in customer terms and conditions.

4.27 The same principles will apply equally to electronic and digital payments.

4.28 Much of the debate since the advent of internet banking has been in relation to the obligations of customers to protect their pin numbers and computers from unauthorised access to mitigate the risk to banks of acting on fraudulent electronic instructions.

[6] "Cyber-Risk Practice Guide – Put cybersecurity on the agenda before it becomes the agenda" Institute of Directors <https://www.iod.org.nz/Governance-Resources/Publications/Practice-guides/Cyber-Risk-Practice-Guide>

4.29 There has been little thought given to date on the increasing risk that the bank's systems themselves could be threatened by cyber attack and payments made from customer accounts directly from bank systems (ie not originating from a customer's computer or system).

4.30 In this case, the starting point would be that there was not a valid customer instruction on which to act. The bank would still have owed its customer the same amount before and after the fraudulent transfer took place because an unauthorised transfer request would have been ineffective to reduce the bank's debt to its customer.

4.31 If the accounts had not been hacked, but instead there had been a denial of service attack against a bank, the question of liability is potentially more complex. In practice, customers may simply be unable to give instructions to their bank to make a payment electronically. Similarly, customers may not be able to receive payments into their accounts.

4.32 The starting point is that the banks would be liable for losses that customers suffer because the banks were not able to fulfil their duty to process payment instructions on behalf of their customers or to act as agent for the collection of funds for their customers. In this instance, contractual claims are likely to include "consequential and indirect losses" where, for example, a failure to make a payment on the due date caused a customer to be in breach of a contract or unable to secure goods or services at a particular price. There is also a risk of reputational damage.

4.33 Much of this risk may be insurable. To the extent it is not, banks could attempt to mitigate it through customer contracts. However, that is likely to be very controversial.

5. REGULATION IN THE FINANCIAL SERVICES SECTOR

New Zealand

5.1 The response in New Zealand to regulating the cyber security of financial institutions has so far been very hands-off. The Reserve Bank of New Zealand (**RBNZ**) has not imposed specific cyber security requirements on the entities for which it is the prudential supervisor, but instead treats cyber risk as a type of operational risk that is dealt with through the general prudential supervision framework.

5.2 Toby Fiennes, Head of Prudential Supervision at the RBNZ, said in a speech on 19 July 2017 that the RBNZ considered in 2016 whether to introduce more prescriptive requirements related to cyber security. However, firms have "strong reputational and financial incentives to address the cyber risks they face".[7] Further, Mr Fiennes stated:[8]

> Given our systemically-focused objectives, the existence of industry guidelines and our consideration that public and private incentives are relatively well aligned, to date we have not imposed prescriptive cyber security regulations on the financial sector. We doubt that doing so now would appreciably improve the outcome, when both the technology and threat landscape is changing so rapidly.

[7] Toby Fiennes, Head of Prudential Supervision, Reserve Bank of New Zealand "The Reserve Bank, cyber security and the regulatory framework" (speech delivered to the Future of Financial Services (10th Annual) Conference, Auckland, 19 July 2017), available at http://www.rbnz.govt.nz/research-and-publications/speeches/2017/speech-2017-07-19, at 7.
[8] At 7.

5.3 The RBNZ has committed to reviewing this policy stance from time to time to ensure it remains appropriate.[9]

5.4 The current policy not to specifically regulate cyber security in financial institutions is due to a recognition by the RBNZ that "[t]he dynamic cyber environment means organisations have to be nimble in their approach to cyber security – focused on outcomes, rather than prescription compliance exercises" and an acknowledgement that international guidance may be helpful to assist in the development of cyber risk management frameworks.[10]

5.5 However, while there are no globally accepted standards for cyber security in the banking or insurance sectors, the Bank of International Settlements' Committee on Payments and Market Infrastructures (**CPMI**) and the Board of International Organization of Securities Commissions (**BIOSC**) has published "Guidance on cyber resilience for financial markets infrastructures" (available at http://www.bis.org/cpmi/publ/d146.htm). The CPMI and BIOSC are the same entities that publish the "Principles for financial markets infrastructures" which the RBNZ uses as the basis for its supervision of financial markets infrastructures in New Zealand.[11] Therefore, the Guidance on cyber resilience is likely to be considered as an appropriate standard for New Zealand entities to work towards (although the RBNZ has acknowledged that these standards "are aspirational at the moment").[12]

5.6 The RBNZ acknowledged that addressing cyber security in financial institutions is not a 'one size fits all' exercise but they expect the entities they regulate to "draw on guidance … to develop cyber resilience practices that are appropriate for their business models and robust to the risks they face".[13]

5.7 The RBNZ has previously noted that New Zealand has been less exposed to cyber-heists compared to many other countries, but that it is important for the industry to remain ahead of the game on cyber-security and to be cautious when adopting new technologies and payment solutions.[14]

Australia

5.8 Australia has no specific regulations, however, some Australian financial oversight bodies such as the Australian Prudential Regulation Authority, Australian Securities and Investments Commission and ASX have indicated they intend to improve cyber security management by financial services. Whether this will result in regulations similar to that in New York remains to be seen.[15]

5.9 In its *Payments System Board Annual Report*, the Reserve Bank of Australia (**RBA**) noted the reports of cyber attacks targeting SWIFT's financial messaging network.[16] While the RBA did not

[9] At 7.
[10] At 7.
[11] At 8.
[12] At 8.
[13] At 8.
[14] Grant Spencer, Deputy Governor of the Reserve Bank of New Zealand "Innovation with resilience – a Central Banker's perspective" (Payments NZ conference, Auckland, 8 November 2016) at 4.
[15] http://www.corrs.com.au/thinking/insights/bold-cyber-security-regulations-for-the-financial-services-industry-will-we-see-them-in-australia/
[16] Reserve Bank of Australia *Payments System Board Annual Report* (Australia, 16 September 2016) at 48.

indicate that it is itself responding to these risks, it did outline the response being taken by SWIFT with the launch of its Customer Security Programme[17].

United States

5.10 While the general global trend matches New Zealand's approach in providing guidelines and best practice rather than specific regulations, the United States is one exception, where there has been an active effort to regulate the cyber security of financial institutions. In 2016, the United States began development of a comprehensive framework for cyber security in financial institutions. However, there was criticism that the framework was unnecessary for an industry that is already subject to a wide range of federal, state and international cyber security regimes[18]. In addition, the Trump administration seems to have retreated from regulating in general, especially regulation of a broad nature, as was proposed here.[19]

5.11 The proposed framework was a joint effort of three federal banking regulators: the Federal Reserve Bank, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation. The regulations were to apply to institutions with consolidated assets of USD$50 billion or more.

5.12 The proposed framework addressed the following five areas:[20]

- Cyber Risk Governance
- Cyber Risk Management
- Internal Dependency Management
- External Dependency Management
- Incident Response, Cyber Resilience and Situational Awareness

5.13 This framework, while complex, is also broad enough to be applicable to many different institutions and not become redundant with changing technology in the short to medium term. It remains to be seen whether the current United States government will do anything further with these proposed federal regulations, although there is minimal expectation of any further action.

New York State

5.14 At a state level, New York has recently implemented Cybersecurity Requirements as mandated by the New York State Department of Financial Services. Announced in February 2017, these regulations came into force on 1 March 2017 with a 180 day transition period for most obligations.[21] They cover all institutions operating under a licence, registration, charter, certificate, permit, accreditation or other authorisation under banking, insurance or financial services law. This is an incredibly broad scope of operation. However, there are some limited exceptions from some of the requirements for entities with less than 10 employees, less than USD$5 million in gross revenue or less than USD$10 million in year-end total assets.

[17] See https://www.swift.com/myswift/customer-security-programme-csp
[18] http://www.cadwalader.com/resources/clients-friends-memos/proposed-federal-cybersecurity-regulations-for-financial-institutions-face-an-uncertain-future
[19] Ibid.
[20] Ibid.
[21] Ernst & Young "*Cybersecurity requirements for financial services companies"* February 2017.

5.15 The final regulations are less arduous than many proposals during the consultation phase of bringing these regulations into force, although many organisations will still have a lot of work to implement programmes in the required timeline.[22] Among the key features of these new regulations, organisations are required to have in place procedures and programmes relating to:[23]

- Cybersecurity policy
- Risk assessment, testing and compliance
- Personnel, resources and training
- Access, application security and encryption
- Audit trail
- Incident response and notifications

5.16 These regulations are broad, overarching and in-depth. They create a significant obligation for financial institutions in New York State to comply in various ways. These are the first mandatory regulations of their kind relating to financial institutions and cybersecurity.

Canada

5.17 Canada has guidelines from oversight bodies such as The Office of the Superintendent of Financial Institutions but no specific regulations for financial institutions.[24] No regulations have been implemented in response to the threat of cyber attacks against the SWIFT system, but the Bank of Canada has recognised cyber threats as a vulnerability in its June 2017 *Financial System Review*.[25] The *Review* noted the important role that the public sector has to play in protecting against cyber attacks to uphold confidence in the financial system, but only goes so far as to outline existing preventative measures rather than proposing new regulations. Existing measures include a network of public and private sector partners that enable the sharing of meaningful intelligence on cyber risks and threats, together with self-assessment guidance from the Office of the Superintendent of Financial Institutions and a requirement by the Bank of Canada that financial market infrastructures comply with international standards.[26]

United Kingdom

5.18 While general (and non-mandatory) cyber security standards and frameworks exist (and extend to financial institutions), there are no specific regulations in the UK relating to cyber risk in the financial services sector. The Financial Conduct Authority has stated that it expects a security culture in all firms it supervises,[27] and no specific steps have been taken to regulate cyber risk.

5.19 However, following the BCB heist, it was reported in May 2016 that the Bank of England ordered United Kingdom banks to "detail steps taken to secure computers connected to the SWIFT bank messaging network".[28] Banks were ordered to conduct a compliance check to confirm whether they

[22] Ibid.
[23] Ibid.
[24] http://business.financialpost.com/news/fp-street/new-yorks-new-financial-cyber-security-laws-have-canadian-experts-taking-note/wcm/b115a3aa-46b7-4742-90fc-d6afb2d05251
[25] Bank of Canada *Financial System Review* (Canada, June 2017) at 17–18.
[26] At 18.
[27] http://www.lexology.com/library/detail.aspx?g=79434b7c-f59e-4450-869e-a85a9364abb0
[28] Andrew MacAskill and Jim Finkle "Exclusive – UK banks ordered to review cyber security after SWIFT heist" (Reuters, 19 May 2016).

are following security practices recommended by SWIFT, including user entitlement reviews and reviewing computer logs for digital evidence of compromises. This review has not been confirmed by the Bank of England.

Singapore

5.20 While no official regulations apply in Singapore, other steps are being taken in relation to the cyber security of financial institutions, such as recently collaborating with the Financial Services Information Sharing and Analysis Centre to create an Asia and Pacific Regional Intelligence and Analysis Centre to encourage regional sharing of financial cyber security threats and information.[29]

[29] http://www.mas.gov.sg/News-and-Publications/Media-Releases/2016/FS-ISAC-and-MAS-Establish-APAC-Intelligence-Centre.aspx

Appendix

Bangladesh Central Bank and NY Federal Reserve – Anatomy of a cyber heist

1. BANGLADESH CENTRAL BANK HEIST

Fact summary:

1.1 On 4 Feb 2016, hackers used SWIFT credentials of Bangladesh Central Bank (**BCB**) employees to send more than three dozen fraudulent money transfer requests to the Federal Reserve Bank of New York (**NY Fed**) asking it to transfer millions of BCB's funds to bank accounts in the Philippines, Sri Lanka and other parts of Asia.

1.2 The hackers succeeded in getting US$81 million sent to Rizal Commercial Banking Corporation in the Philippines (**Rizal Philippines**) via four different transfer requests into four different accounts in the Manila branch, and US$20 million to Pan Asia Banking in a single request. BCB managed to halt US$850 million in other transactions.

1.3 Global cybersecurity company Kaspersky Lab produced a report based on investigations into the Bangladesh incident and other cybersecurity breaches.[30] The Report examines whether Lazarus Group, a known hacking group, was behind the Bangladesh heist. The Report concludes Lazarus hacking software was definitely involved, and that there are strong links between the Group and North Korea. The Lazarus Group also has connections to the Sony hack.

How it happened:

Timing	Sequence of events
May 2015	Hackers open multiple fraudulent accounts at Rizal Bank in the Philippines to hold stolen funds. They deposit $500 into each account, which then sit inactive. The hackers use fake names to set up these accounts.
29 January 2016	Hackers install malware on SWIFT Access Alliance to give them persistent access to the system, learn how the secure message platform worked and gain access to the SWIFT-issued digital certificates required to authenticate to the SWIFT network. *Software/systems:* 1. **SWIFT network and SWIFT Access Alliance software:** The Society for Worldwide Interbank Financial Telecommunication (**SWIFT**) provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure and reliable environment. The system uses Business Identifier Codes (BICs, popularly known as SWIFT codes). SWIFT is a financial messaging system (it sends payment orders), and does not hold accounts for its members or perform any form of clearing or settlement. Access Alliance is SWIFT's market leading messaging interface and enables customers to connect to SWIFT via single or multiple destinations with maximum automation of system management tasks. *2.* **Custom-made malware**: Malware that tracks and records activity, and hides malicious tracks, including preventing the printer from printing SWIFT messages. See here for

[30] Kaspersky Lab *Lazarus under the hood* 3 April 2017: https://securelist.com/files/2017/04/Lazarus_Under_The_Hood_PDF_final.pdf

	technical details: http://baesystemsai.blogspot.co.nz/2016/04/two-bytes-to-951m.html#more
4 February 2016 Late evening in Bangladesh[31]	Hackers use credentials of legitimate BCB employees to access and make fraudulent transfer requests via the SWIFT network. It is unclear how they came to hold the credentials, but it has been suggested that insiders may have collaborated with the attackers by providing their credentials.[32] Other reports suggest BCB did not have firewalls installed on its networks, or had weak firewalls, allowing the hackers to breach the network and access the credentials that way.[33]
4 February 2016 Thursday From 9:55am in NY	The first SWIFT message is received by the NY Fed, containing instructions to transfer $20 million from BCB's account to an account with PAN Asia Bank in Sri Lanka. 34 further orders are received over the next four hours instruction transfers totalling almost $1 billion.[34] The NY Fed rejects the first 35 messages for incorrect formatting, as they lack the names of the "correspondent bank" (required for the next step in the chain). The hackers fix this issue and re-send the requests. The NY Fed clear 5 requests automatically at this point totalling $101 million, as they are correctly formatted and SWIFT authenticated. The remaining 30 (totalling some $850 million) are rejected for further formatting errors, and of those, by the end of the day (Thursday) 12 have been flagged by NY Fed staff as potentially suspicious. NY Fed sends queries to BCB via SWIFT regarding those suspicious requests.
5 February 2016 Friday Early morning in Bangladesh	The cover-up malware installed on BCB's network prevents the automatic printing of the sent and received messages via the SWIFT network, and deletes the database records of the transfers. BCB do not respond to any of NY Fed's SWIFT messages, as the messages are not getting through to BCB, and no staff are on hand because of the time difference.
5 February 2016 Friday NY Business hours	NY Fed begin a full manual review of the orders received from BCB.
5 February 2016 Friday morning	Officials arrive at BCB in the morning and discover there are no SWIFT printouts, which should appear automatically. They attempt a manual print, which fails. Software on the terminal that connects to the SWIFT network indicates that a critical system file is missing or has been altered. Senior officials go home at midday because it is an Islamic holy day.
5 February 2016 Friday NY Business hours	NY Fed send further messages to BCB querying four of the five transactions that have already been cleared. These four transactions contain the name "Jupiter Street" (part of the address of a Philippine bank). By chance, "Jupiter" is also a name flagged by the US government as part of sanctions against Iran (the name of an oil tanker and shipping company), and so it triggers a query. The SWIFT messages are not making it through to BCB, and although the NY Fed is not receiving any responses, staff do not try to contact BCB in any other way (it would often take up to three days for clients to respond to SWIFT messages).
6 February 2016 Saturday 12:30pm in Bangladesh	BCB finally fix the printer error and manage to print the SWIFT messages, discovering there is a major problem. BCB is still unable to send SWIFT messages, and cannot find another way to contact the NY Fed. BCB attempts to email the NY Fed using an address found on their website, but the email

[31] Bangladesh is 10 hours ahead of New York.
[32] https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/
[33] https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/
[34] http://www.reuters.com/investigates/special-report/cyber-heist-federal/

	is only monitored during the week. Other attempts to telephone and fax are left unanswered.
8 February 2016 Monday Bangladesh business hours	BCB manage to send a SWIFT message to NY Fed stating that the 35 payment orders were fake and to recall funds if already cleared. This arrives at 1am NY time. According to BCB, it also sends SWIFT messages to Rizal Bank asking it to freeze the money that had arrived into the four accounts. It is a holiday in the Philippines, and the messages are not seen immediately. (Rizal Philippines officials later said the SWIFT messages from BCB had been wrongly formatted and were not marked as urgent, so they went into a large pile of unread messages. In any case, under Philippine law, stolen funds cannot be frozen until a criminal case is lodged).[35]
8 February 2016 Monday NY business hours	NY Fed tells BCB they are able to reverse the US$20 million sent to PAN Asia Bank in Sri Lanka because of a spelling error in the request, which holds things up at the Sri Lanka end. The four other payments made to the Rizal accounts totalling $81 million are irretrievable.
Following days	The money sent to the Philippines is moved out of the four accounts. The accounts are subsequently frozen by Rizal at the request of BCB, but only in time to save US$68,000. The other funds disappear into the casino industry.

The systems exploited:

Systems / procedures	Details of exploitation
SWIFT systems (specifically SWIFT Access Alliance software)	The software behind the SWIFT network was not itself compromised, but the hackers found other ways to exploit weaknesses in the system as a whole.[36] BAE Systems released a blog post revealing their analysis of the software behind the attack.[37] 1. **Use of SWIFT credentials** – access to the appropriate SWIFT credentials allows authentication of SWIFT messages. Because the hackers had legitimate credentials of relevant BCB employees, there was no need to "hack" the SWIFT messaging system to send transfer requests. 2. **Malware** – the hackers exploited local BCB admin rights enabling them to install monitoring and cover-up software that interfaced with the local SWIFT Alliance Access software. This enabled them to learn how the secure message platform worked and gain access to the SWIFT-issued digital certificates required to authenticate SWIFT transfer requests. Malware was specifically tailored for BCB with the ability to bypass checks made by BCB software. It is likely the malware was not easily detectable by broad-release anti-malware programs because of its custom nature.[38] The hackers also used their admin privileges to install malware (possibly "Evtdiag.exe") to cover their tracks. The malware includes a module that replaces a 2-byte conditional jump with a do-nothing instruction "effectively forcing the host application to believe that the failed check has in fact succeeded," thereby giving itself the ability to execute database transactions, BAE said. One of the malware's actions disabled the printer that was configured to automatically print all sent and received messages, in order to prevent BCB employees from discovering the fraudulent transactions. The hackers designed

[35] http://www.reuters.com/investigates/special-report/cyber-heist-federal/
[36] https://www.theregister.co.uk/2016/04/25/bangladeshi_malware_screwed_swift/
[37] http://baesystemsai.blogspot.co.nz/2016/04/two-bytes-to-951m.html#more
[38] http://www.pwc.com/us/en/financial-services/financial-crimes/publications/assets/swift-bangladesh-robbery-2016.pdf

	their malware down to the exact make of the printer used at BCB. SWIFT have noted that the malware can only be deployed if attackers somehow manage to compromise the target's systems by exploiting security vulnerabilities.[39]
Local security	There are suggestions that BCB did not have adequate IT security measures in place, and this allowed the hackers to access BCB systems: 1. **Lack of adequate firewall** – the hackers (possibly with insider help) reportedly inserted the malware into the SWIFT terminal used by BCB via a poorly configured network switch not guarded by a firewall.[40] Reports indicate the bank had been relying on vulnerable $10 second-hand networking gear.[41] Hackers may have exploited such weaknesses after BCB connected a new electronic payment system, known as real time gross settlement (RTGS), in November 2015.[42] 2. **Insider help** - Mohammad Shah Alam, head of the Forensic Training Institute of the Bangladesh police's criminal investigation department in Dhaka told Reuters that some BCB officials deliberately exposed its computer systems and enabled the theft, but declined to identify those officials by name.[43]
Communications	Even when suspicions arose, neither the NY Fed nor BCB could communicate with the other in any effective way, because the hackers had disabled the one relied upon method, SWIFT messages: 1. **Weekends/holidays** – the hackers timed things so that BCB would be difficult to reach when the NY Fed grew suspicious, and that the NY Fed would be difficult to reach when BCB finally received word from them. There were insufficient "after hours" systems in place. 2. **No secondary method** – when the NY Fed heard nothing back from BCB they did not attempt to contact them another way, as this was standard practice. When BCB urgently needed to contact the NY Fed and found the SWIFT messages were not working, they had no other contact details on hand. Internet searches provided only "during business hours" communication via email, telephone and fax. 3. **Missed warning signs** – the NY Fed missed a number of warning signs, including when the 35 requests were automatically rejected the first time because of missing "correspondent bank" details, the fact that most of the payments were to individuals and not institutions, and the fact that BCB usually sends less than one SWIFT request a day on average.[44] Also, the NY Fed typically looks back through payments the day after the request, rather than checking for suspicious patterns as they occur.[45] Once suspicions were confirmed, the NY Fed did not persist in trying to contact BCB other than via SWIFT messages. BCB did not realise the failed printing was an indication of a much more serious situation.

Subsequent lawsuits:

Legal action	Details

[39] http://www.securityweek.com/custom-malware-used-81-million-bangladesh-bank-heist
[40] http://www.reuters.com/investigates/special-report/cyber-heist-federal/ ; https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/
[41] https://www.theregister.co.uk/2016/04/25/bangladeshi_malware_screwed_swift/
[42] http://www.reuters.com/investigates/special-report/cyber-heist-federal/
[43] http://www.reuters.com/article/us-usa-cyber-swift-exclusive-idUSKBN1412NT
[44] http://www.reuters.com/investigates/special-report/cyber-heist-federal/
[45] http://www.reuters.com/investigates/special-report/cyber-heist-federal/

Civil suit against NY Fed (not pursued)	Reports indicated that BCB initially hired a US lawyer to help bring proceedings against the NY Fed, seeking compensation for alleged errors made by the NY Fed and SWIFT that left BCB vulnerable.[46] But, in August 2016 a BCB spokesperson stated they had "no plan at that time to go for any legal action against the Fed bank or SWIFT" and that they would join forces instead.[47] NY Fed claims that it authenticated the transfer instructions using a "commercially reasonable security procedure", being the SWIFT authentication protocol. This is a deliberate phrase, as it mirrors the language of the New York Uniform Commercial Code. Banco del Austro's current lawsuit against Wells Fargo contents that that the SWIFT authentication protocol isn't "commercially reasonable" (see the next case study for details).[48]
Philippines money laundering prosecutions	The Philippines Department of Justice resolved to indict several individuals for money laundering in connection with the Bangladesh heist, including former manager of Rizal Philippines, Maia Santos-Deguito, and owners of remittance firm Philrem Corporation. They face trial for violations of the Republic Act (RA) 9160 (or the Anti-Money Laundering Act of 2001).
Bangladesh government suits against international orgs (not pursued)	Bangladesh government decided not to file lawsuits against any international organisation connected with the theft. Ajmalul Hossain QC conducted the legal procedure of attempting to recover the lost funds, and noted "We have already traced and recovered $15.25 million, and we aim to recover the rest of the money the same way we recovered that money."[49]

[46] http://www.reuters.com/article/us-usa-fed-bangladesh-idUSKCN0WO2JQ; http://www.reuters.com/article/us-cyber-heist-bangladesh-idUSKCN10R0OG; http://www.reuters.com/investigates/special-report/cyber-heist-federal/
[47] http://www.reuters.com/article/us-cyber-heist-bangladesh-idUSKCN10R0OG
[48] http://digital.freshfields.com/post/102dkd1/ny-fed-and-bangladesh-bank-patching-things-up-pun-intended
[49] http://www.dhakatribune.com/business/banks/2016/11/10/bangladesh-will-not-sue-anyone-bb-heist/

2. BANCO DEL AUSTRO HEIST – ECUADOR

Fact summary:

2.1 On 12 January 2015 and in the days following, hackers used the SWIFT credentials of a Banco del Austro (**BDA**) employee to make fraudulent transfer requests across the SWIFT messaging network to Wells Fargo (**WF**). It is unclear how the hackers accessed the credentials. The hackers used the credentials to access previously cancelled or rejected payment requests that remained in BDA's SWIFT outbox. They then altered the amounts and destinations on the transfer requests and reissued them.

2.2 Over ten days, $12 million was transferred from BDA accounts at WF and sent to bank accounts in Hong Kong, USA and Dubai.

2.3 BDA has brought proceedings against WF for failing to notice to red flags.

How it happened:

Timing	Sequence of events
12 January 2015 Shortly after 7pm Outside BDA business hours	A message from a secure computer terminal at Banco del Austro in Ecuador instructed WF to transfer money to bank accounts in Hong Kong, USA and Dubai. Thieves used the SWIFT credentials of a BDA employee to make fraudulent transfer requests across the SWIFT messaging network. It is unclear how the thieves accessed the credentials. Hackers were able to circumvent local security to gain access to the SWIFT messaging system.[50]
Next 10 days	$12 million of BDA's money transferred by WF, $9 million of this ended up in bank accounts in Hong Kong belonging to HK shell companies. Just under $1.5 was transferred to an account in the name of a Jose Mariano Castillo at Wells Fargo in Los Angeles (and just under $1 million of this was returned to BDA). See diagram below for illustration.
Over a week since first transfer	BDA finally discovers the fraudulent transfers have occurred.
Early 2015	BDA files proceedings in Hong Kong against the web of companies that received or handled funds (see the *Subsequent lawsuits* section for details).
28 January 2016	BDA files a lawsuit against WF (see the *Subsequent lawsuits* section for details).
May 2016	SWIFT learns about the heist, after a Reuters inquiry.[51]

Systems/procedures exploited:

2.4 The heist was carried out by essentially the same means as the Bangladesh heist.

2.5 The hackers' access to the SWIFT credentials meant they could request transfers over the system. SWIFT CEO Gottfried Leibbrandt noted "At the end of the day, we weren't breached. It was, from our perspective, a customer fraud".[52]

[50] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/ecuadorean-bank-loses-12m-via-swift
[51] http://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD; http://www.reuters.com/article/us-cyber-heist-hongkong-insight-idUSKCN0YN4BH
[52] http://thehill.com/policy/cybersecurity/280673-lawsuit-exposes-9m-cybertheft-using-banking-software

2.6 SWIFT was not notified about the attack, and only learnt of it later through a Reuters inquiry.[53] SWIFT, however, has no rule specifically requiring client banks to report hacking thefts. Banks often do not report such attacks out of concern they make the institution appear vulnerable, former SWIFT employees and cyber security experts told Reuters.[54]

Subsequent lawsuits:

***Banco Del Austro, SA v Wells Fargo Bank*, NY District Court**	
28 January 2016 Initial suit filed in NY District Court	BDA seeks to hold WF responsible for the lost funds on the following grounds: 1. **Violation of the New York Uniform Commercial Code (UCC)** – or the "bad faith and commercial reasonableness" argument. UCC article 4-A governs the procedures, rights and liabilities arising out of commercial electronic funds transfers, including liability for unauthorised transfers. As a default rule, the article allocates the risk of loss to the bank that receives and honours unauthorised orders. But an exception provides that parties may agree that transfers should be verified pursuant to a "security procedure", and where transfer orders are verified in this way the order is effective whether or not it has been "authorised", so long as the security procedure is "commercially reasonable". In these circumstances, the customer must bear the risk. Such a security procedure exists between WF and BDA – their agreement adopts "the SWIFT authentication procedures in accordance with the SWIFT User Handbook". Under UCC, the customer must be reimbursed if (1) the authorising bank failed to act in good faith or (2) the security procedure was not commercially reasonable. BDA alleges WF were in breach of both. 2. **Breach of contract** – BDA alleges that the agreement between it and WF incorporated additional safeguards above and beyond the SWIFT procedures, including certain "know your customer" fraud detection policies (they argue this is incorporated because the agreement is stated as governed by US Law and the UCC). BDA assert WF breached these additional requirements. 3. **Negligence** – BDA alleges that WF violated its duty of care by negligently honouring the transfers.
18 October 2016 WF's motion to dismiss is decided by Judge Kaplan	WF sought to dismiss BDA's claims in *Banco Del Austro, SA v Wells Fargo Bank, NA (No 1)* 27 (SDNY 2016).[55] Judge Kaplan decided on each ground as follows: 1. **Breach of contract claim thrown out** – the agreement between BDA and WF expressly states it constitutes the entire agreement between the parties, which requires WF to adhere to SWIFT authentication procedure only (i.e. the agreement does not incorporate additional requirements such as "know your customer" safeguards). BDA does not allege that WF failed to follow this procedure, and so this argument must fail. 2. **Negligence claim thrown out** – the UCC specifically precludes "common law claims when such claims would impose liability consistent with the rights and liabilities expressly created by article 4-A". 3. **Alleged violations of UCC article 4-A claim will continue** – BDA argues that the agreed upon security procedure cannot possibly comply with reasonable commercial standards of fair dealing because it failed to detect the alleged fraud, and that reliance on the SWIFT system alone therefore constituted bad faith. Judge Kaplan decides that

[53] http://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD
[54] http://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD
[55] http://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2016cv00628/452772/27/

	the facts alleged do not permit the Court to rule as a matter of law that use of the SWIFT system, with nothing more, constituted a commercially reasonable security procedure in the context of this particular customer-bank relationship, and so this claim should proceed to trial.
Ongoing	Parties are now undergoing discovery (which may take some time) before moving to full trial.