The Bangladesh bank hack and compliance programmes

A cyber heist in February 2016 saw unknown hackers make off with over $100 million from Bangladesh's central bank; the losses could have been even more substantial if it hadn't been for the actions of other banks who blocked 31 of the attempted wire transfers made by the hackers due to money laundering suspicions. Michael L. Yaeger, Melissa G.R. Goldstein and Kimberly G. Monty of Schulte Roth & Zabel LLP detail how this attack took place, and discuss the cyber security lessons to be learned, which include pointers on how compliance programmes in other areas, such as AML, might be used to bolster cyber security practices.

This past February, hackers robbed more than $100 million from Bangladesh's central bank using stolen credentials to authenticate their fraudulent wire transfers. Predictably (and appropriately), much of the public discussion following the attack has focused on technological improvements such as software updates. Yet a robust cyber security programme is not just about technological controls: it should also include administrative procedures. As the saying goes, security is not a product, but a process. And the Bangladesh cyber heist illustrates that banks can improve that process by drawing from their other compliance efforts, such as their anti-money laundering ('AML') programme. In fact, as bad as Bangladesh's loss was, it would have lost an additional $869 million if other banks had not blocked 31 of the hackers' wire transfers due to suspicions of money laundering. As banks face increasingly frequent and sophisticated cyber attacks, it is worth considering if further improvements to AML programmes and international AML regulations would also improve banks' security.

Bank robbery in the 21st century

Late on 5 February 2016, hackers attempted to siphon $950 million from an account of Bangladesh's central bank, the Bank of Bangladesh, held at the New York Bank for the Federal Reserve (the 'New York Fed'), through a series of 35 fraudulent messages sent through the 'SWIFT' interbank messaging system[1]. The messages directed that the money be transferred to private bank accounts, including personal bank accounts, of individuals and financial institutions in Sri Lanka and the Philippines. The SWIFT messages contained the credentials necessary to authenticate the transfer requests and appeared to come from a server in Dhaka used by the Bank of Bangladesh. The New York Fed approved five of the transfers, totaling over $100 million. Later that day, the New York Fed became suspicious that such large sums of money would be transferred to personal accounts in Sri Lanka and the Philippines, and flagged the requests for the Bank of Bangladesh's review, including the five requests it had already approved. But the New York Fed was unable to make contact with Bank of Bangladesh employees because Friday and Saturday are the Bangladeshi weekend.

Though Bank of Bangladesh employees periodically check SWIFT messages over the weekend, malware installed by the hackers had rendered the bank's SWIFT terminal unresponsive and had disabled a printer set up to print SWIFT messages. These issues prevented the Bank of Bangladesh from retrieving the messages from the New York Fed asking the bank to reconfirm the transactions. When Bank of Bangladesh employees returned to work on Sunday, they manually printed the messages, but by that time the New Yorkers were off for their weekend. When the conflicting weekends were finally over on Monday, the remaining 30 transfers were cancelled, but the five transfers approved by the New York Fed on Thursday, totaling over $100 million, had already been processed.

Of those five executed transactions, only one was flagged and reversed at its destination in Sri Lanka, where it was to be deposited in the account of a newly formed non-governmental organisation. The remaining four transfers, totaling $81 million, were sent to the Philippines, where they

were deposited in bank accounts that the Philippine government alleges were opened in the name of a local businessman using forged documents. The funds were then moved through a local money transmitter to several destinations: a local casino (where proceeds were apparently used to buy casino chips), an online gambling company, and points unknown.

Once the funds disappeared into the casinos the case went cold, as the Philippines' anti-money laundering law exempts casinos from reporting suspicious activity and prohibits authorities from compelling casinos to aid the investigation. Though authorities have traced some funds to gambling junkets and Chinese nationals Weikang Xu, Kam Sin Wong, Gao Shu Hua, and Ding Zhi Ze, these individuals may only be recipients of a portion of the criminal proceeds, not perpetrators of the cyber attack. Despite investigations and cooperation between the four countries involved, officials have been unable to locate the majority of the funds or identify the hackers.

Further, the affected parties have not been entirely cooperative. The attack has also sparked recriminations, with Bangladeshi officials threatening suit and accusing the New York Fed of "irregularities," and the New York Fed and information security consultants accusing the Bank of Bangladesh of failing to comply with operating procedures and implementing the most basic cyber security measures. Atiur Rahman, the Governor of the Bank of Bangladesh, resigned on 15 March. The New York Fed and SWIFT officials maintain that their systems were not breached and that the cause was an internal issue at the Bank of Bangladesh.

The Bank of Bangladesh may have been especially vulnerable to hackers because its network did not have a firewall and used unsophisticated, second-hand switches, which prevented the Bank from isolating the SWIFT terminal's network from other points of entry. And in October 2015, the Bank linked its SWIFT system to a common payment platform for commercial banking, which may have further exposed its server to attacks (including 'phishing' attacks over email). In any event, the attackers infected as many as 32 computers on the Bank of Bangladesh's system with malware. According to the cyber security firm FireEye, Inc., which the Bank hired to investigate the matter, the hackers deployed keylogger software, which registers strokes on a keyboard, to steal the Bank of Bangladesh's SWIFT credentials. It is unclear whether the Bank of Bangladesh violated SWIFT's security procedures, which SWIFT maintains are proprietary and has refused to divulge.

The attack on the Bank of Bangladesh succeeded by exploiting technological weaknesses, but also human error, cultural differences between Bangladesh and New York, and jurisdictions with relatively weak AML laws

Upgrading the banks' technology

One unsurprising but still urgent lesson from this crime is that banks should continue to fortify their technological defences. The Bank of Bangladesh's lack of a firewall is striking, as is the lack of separation between the Bank's SWIFT terminal and the rest of its network. But institutions that have taken those particular precautions should not get comfortable. As Reuters reported, SWIFT has told its customers that the Bangladesh heist was not an isolated incident but rather one "of a number of recent cyber incidents in which malicious insiders or external attackers have managed to submit SWIFT messages from financial institutions' back-offices, PCs or workstations connected to their local interface to the SWIFT network." In addition, FireEye told Reuters that it "has observed activity in other financial services organisations that is likely by the same threat actor behind the cyber attack on the Bank of Bangladesh." Presumably, at least some of these incidents involved banks with more robust protections than those used by the Bank of Bangladesh. The vulnerability of other banks is also indicated by the fact that SWIFT decided to release a mandatory security update ('Access Alliance') to the software that banks use to access the SWIFT system.

But technical controls are only part of a robust cyber security programme, which must also include administrative controls and employee training. The attack on the Bank of Bangladesh succeeded by exploiting technological weaknesses, but also human error, cultural differences between Bangladesh and New York, and jurisdictions with relatively weak AML laws. Accordingly, an effective cyber security programme must understand that the territory to defend extends far beyond software or hardware vulnerabilities.

Security through compliance: training for suspicion

The good news is that existing compliance programmes in other areas can also serve to bolster cyber security. In particular, the attack on the Bank of Bangladesh highlights the value that AML compliance can have for cyber security. Speaking broadly, a functioning AML programme is designed to identify suspicious financial activity, which can be done through both automated and manual monitoring systems, and further analysis and investigation of suspicious activity[2]. Even though the transfer requests from Bangladesh appeared to be fully authentic, the New York Fed

questioned them because the intended recipients included personal bank accounts in the Philippines, which were unlikely to have a legitimate reason to receive millions of dollars from Bangladesh's central bank. Further, Deutsche Bank, the routing bank for one of the transactions to the Philippines, blocked a transaction due to money laundering-related suspicions.

Cyber security benefits from similar techniques - such as monitoring a network for unusually large data uploads or downloads - and in the banking business it is not surprising that the two forms of monitoring would complement each other. Tracking anomalous money flows and data flows may answer similar questions. Through training and experience, bankers develop an AML mindset, and that mindset can be leveraged to support cyber security programmes and help thwart attacks. AML experts operate on the assumption that money laundering attempts will occur, and AML experts learn (and train others) to detect and distinguish suspicious activity from typical, low-risk transactions. Indeed, it was the money laundering suspicion raised by bankers at Deutsche Bank and in Sri Lanka that allowed bankers to intercept, and ultimately recover, millions of dollars before they reached the hackers' pockets. Thus, a strong AML compliance programme, including robust transaction monitoring systems and analysts actively clearing alerts, may mitigate against a breach once cyber criminals have gained access to a bank's systems.

Filling gaps in international AML regulation

While many countries have strong AML regulations, and financial institutions spend millions of dollars on AML compliance, sophisticated criminals can detect and exploit the weaknesses that exist in other countries, as the Bank of Bangladesh hackers did with great success. The broad exemption for casinos in Filipino law, combined with a readily available remittance transfer network, allowed the hackers to steal tens of millions of dollars and maintain anonymity. Similarly, several other countries including Mexico, Cambodia and India still exempt casinos from their AML regulations. And like the Philippines, these countries are also well-serviced by remittance transfer providers. They therefore may serve as points of opportunity for future cyber attacks. Accordingly, it is worth considering whether to implement new AML regulations in these countries. The Philippines Senate has since amended the AML law to add casinos to the list of entities required to report suspicious activity to the Anti-Money Laundering Council, and perhaps other countries' legislatures should follow suit. Though technology is central to a strong cyber security programme, stronger international AML laws may also help thwart future cyber attacks.

Michael L. Yaeger Special Counsel
Melissa G.R. Goldstein Associate
Kimberly G. Monty Associate
Schulte Roth & Zabel LLP, New York
michael.yaeger@srz.com

1. SWIFT is an acronym for the Society for Worldwide Interbank Financial Telecommunication, a cooperative of approximately 3,000 financial institutions.
2. Suspicious activity reporting is required under the Bank Secrecy Act for any transaction that is conducted or attempted by, at, or through the bank, that involves or aggregates at least $5,000 in funds or other assets, and that causes the bank to know, suspect, or have reason to suspect that: '(i) The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation; (ii) The transaction is designed to evade any requirements of this chapter or of any other regulations promulgated under the Bank Secrecy Act; or (iii) The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.' 31 C.F.R. § 1020.320. The Bank Secrecy Act and its implementing regulations require financial institutions to establish AML programs, which at a minimum must include: the development of risk-based internal policies, procedures and controls; designation of a compliance officer; an ongoing employee training program; and an independent audit function to test programs. See 31 U.S.C. § 5318(h).