How US Fed fumbled over Bangladesh Bank heist

The most audacious cyber-heists ever

DHAKA: Jupiter. That single word, by a stroke of luck, helped stop the Federal Reserve Bank of New York from paying nearly $1 billion to the cyber-criminals behind a notorious bank heist earlier this year, according to sources familiar with the incident. When hackers broke into the computers of Bangladesh's central bank in February and sent fake payment orders, the Fed was tricked into paying out $101 million. But the losses could have been much higher had the name Jupiter not formed part of the address of a Philippines bank where the hackers sought to send hundreds of millions of dollars more.

By chance, Jupiter was also the name of an oil tanker and a shipping company under United States' sanctions against Iran. That sanctions listing triggered concerns at the New York Fed and spurred it to scrutinize the fake payment orders more closely, a Reuters examination of the incident has found. It was a "total fluke" that the New York Fed did not pay out the $951 million requested by the hackers, said a person familiar with the Fed's handling of the matter. There is no suggestion the oil tanker or shipping company was involved in the heist. The Reuters examination has also found that the payment orders sent by the hackers were exceptional in several ways. They were incorrectly formatted at first; they were mainly to individuals; and they were very different from the usual run of payment requests from Bangladesh Bank. Yet it was the word Jupiter that set the loudest alarm bells ringing at the New York Fed. Even then it appeared to react slowly.

By the time the fraud was discovered, the New York branch of the US central bank had approved five of the payments. It took $101 million from Bangladesh Bank and paid it to accounts in Sri Lanka and the Philippines - including $81 million to four accounts in the names of individuals. Most of that $81 million remains lost. It was among the most audacious cyber-heists ever to emerge shining a light on worrying weaknesses in the global financial system and into a little-known corner of the US Federal Reserve: its Central Bank and International Account Services unit (CBIAS), which one former employee described as a "bank within a bank."

Interviews with investigators, lawyers and current and former central bank officials in several countries, as well as a Reuters review of payment messages, emails and other documents, show disarray and bungling at all the financial institutions involved. But the most striking is the inertia and clumsiness at the New York Fed, the most powerful of the US central bank's 12 regional units and a mainstay of global finance. The heist revealed that the New York Fed lacked a system for spotting potential fraud in real time - even though such systems are used elsewhere - instead relying at times on checking payments after they were made, usually for problems such as violating US sanctions.

Months of bitter finger-pointing over who is to blame for the fiasco have damaged the sensitive diplomacy of correspondent banking, where big Western institutions are entrusted with safeguarding the treasures of smaller economies. Bangladesh Bank is now preparing a legal case to seek compensation for what it says were failures by the Fed, according to a source close to the Asian bank. It also claims that errors by SWIFT, a messaging system used to make international bank transfers, made the bank vulnerable to hackers. Bangladesh Bank spokesman Subhankar Saha said the institutions were working together to try to recover the missing money. He declined to comment further. The New York Fed has denied making missteps and repeatedly said its systems were not compromised. In response to a series of questions from Reuters about its actions during the heist and in the days that followed, it declined to comment, citing a criminal investigation by the US Department of Justice and the Federal Bureau of Investigation.

SWIFT - the Society for Worldwide Interbank Financial Telecommunication, a cooperative used by over 11,000 financial institutions around the world - has denied responsibility for any weaknesses in the way Bank Bangladesh operated and installed the SWIFT system. A spokesman said: "We continue to support the bank and cooperate with the investigations. We look forward to receiving a full account of the security incident."

Officials are still investigating the heist. But the Reuters examination has uncovered new details about how the New York Fed was slow to react to warning signs and how communications broke down between it and Bangladesh Bank. The Fed relied almost entirely on the SWIFT messaging system with, in this case, little backup for emergencies. Miscommunications and clunky payment processes meant that most of the stolen money disappeared without trace before it could be recovered.

"I couldn't believe that that much money could be lost in the SWIFT system, and in the whole federal system for central banks," Carolyn Maloney, a Democratic congresswoman from New York, told Reuters. Maloney, who was the first US lawmaker to publicly raise questions about the incident, added: "It's a wake-up call and it has to be corrected. To me, I see it as a threat to the confidence people could have in the central banking system."

Last month, the New York Fed said it took steps to "help strengthen the safety of global payments in light of the potential vulnerabilities." It did not give specifics. But the source familiar with the Fed's handling of the Bangladesh affair told Reuters that the Fed has now set up a 24-hour hotline for emergency calls from some 250 account holders, mostly central banks, around the world.

The hack

Unlike the Fed, the world's most influential central bank whose New York headquarters sits atop 508,000 gold bars stored below street level, Bangladesh Bank is not a large and powerful operation with a global footprint. It had not protected its computer system with a firewall, and it had used second-hand $10 electronic switches to network computers linked to the SWIFT global payment system, according to Mohammad Shah Alam, head of the Forensic Training Institute of the Bangladesh police's criminal investigation department.

Hackers may have exploited such weaknesses after Bangladesh Bank connected a new electronic payment system, known as real time gross settlement (RTGS), in November last year. However, it remains unknown exactly who broke into its systems or how they did it. What is evident, according to investigative reports by cyber-security company FireEye seen by Reuters, is that someone obtained the computer credentials of a SWIFT operator at Bangladesh Bank, installed six types of malware on the bank's systems and began probing them in January.

The hackers did a series of test runs, logging into the system briefly several times between Jan 24 and Feb 2. One day they left monitoring software running on the bank's SWIFT system; on another they deleted files from a database. On Thursday, Feb 4, the hackers began sending fraudulent payment orders via SWIFT. It was late evening in Bangladesh and most of the staff had gone home. The hackers appear to have timed the heist to coincide with the weekend that in Bangladesh began the following day.

The first SWIFT message arrived at the New York Fed just after 9:55 am and ordered the transfer of $20 million from the central bank of Bangladesh to an account in Sri Lanka. Over the next four hours, 34 more orders arrived asking the US central bank to move a total of nearly $1 billion from the account it holds for Bangladesh Bank. Compared to the great maelstrom of global finance, the sums were unremarkable: The New York Fed handles about $800 billion of payments a day. Nevertheless, the Bangladesh orders were odd, surprisingly odd.

First, all 35 of the messages lacked the names of "correspondent banks" - the necessary next step in the payment chain -according to a senior Bangladesh Bank official and a person familiar with the New York Fed's handling of the payments. That fault meant the orders could not immediately be fulfilled. Second, most of the payments were to individuals rather than institutions, according to police investigators in Dhaka and a source close to Bangladesh Bank.

And third, the slew of payments that morning was out of whack with the usual pattern of orders from Bangladesh Bank. Over the eight months to January 2016, Bangladesh Bank had issued 285 payment instructions to the Fed, averaging fewer than two per working day, according to a source close to Bangladesh Bank. None of those payments had been to an individual, the source said. The U.S. central bank allows payments to individuals, but it's not common and is generally discouraged, according to one of the former New York Fed employees. The New York Fed declined to comment on the number of payments it typically received from Bangladesh Bank or whether staff had found the numerous messages on Feb. 4 surprising or suspicious.

Missed warning signs

At the New York Fed, such payment orders are handled by a small group of CBIAS staff who tend to keep to themselves, according to five former employees and senior officials who worked on the team or closely with it. The unit looks after the foreign accounts of mostly central banks and its work is sometimes like "economic diplomacy," said one of the sources, with staff having to make judgments on confidential payments ordered by a wide range of clients.

A subset of about 10 staff actually process payment requests, according to the sources. These staff, some fairly junior, can find up to 100 requests waiting for them when they arrive in the morning and may manually review hundreds of payments during the day. Most of the transactions are automatically executed. But when there is a problem, staff mainly check for SWIFT formatting and authentication, and violations of US economic sanctions or money laundering regulations. They may ask clients for more information.

NEW YORK: The American flag flies above the Wall Street entrance to the New York Stock Exchange. — AP

When the first 35 messages from Bangladesh Bank were rejected for incorrect formatting, the hackers simply fixed the formatting and sent another 35 requests for payment to the same beneficiaries as before. This time the New York Fed cleared five of them, despite the oddities. They were properly formatted, SWIFT authenticated and went through automatically. The Fed monitors for unusual transactions, but its system had a weakness: While credit card companies can spot unusual patterns in real time, the New York Fed typically looks back through payments, usually the day after they are requested, according to two of the former employees.

After the five payments had been made, staff did flag "several" other requests for review to check whether they complied or not with US sanctions, according to a letter that Thomas Baxter, the New York Fed's general counsel, later sent to Rep. Maloney. That manual review found that the payments were "potentially suspicious," Baxter wrote. The Reuters examination found that on that Thursday Fed staff had sufficient concerns about 12 of the payment requests to send a message to Bangladesh Bank at the end of the day, New York time. "The payments contained individuals as beneficiaries and have varying details," the message said.

But it was nearly 4 a.m. on the weekend in Bangladesh and no one was available to respond. Besides, the hackers had sabotaged Bangladesh Bank's systems to stop messages getting through. It was only the following day, Friday Feb 5, that the Fed began a full manual review of the orders from Bangladesh Bank, according to Baxter's letter and sources in Bangladesh. Baxter, the New York Fed's top lawyer, said in his letter that such reviews can occur after payments have been made.

Sources in the United States and Bangladesh said that it was at this stage that the presence of the name Jupiter in the payment orders rang alarm bells. One of the Fed's responsibilities is to avoid violating US laws and prevent payments to sanctioned companies or individuals. It was just a stroke of luck that the name Jupiter featured on a sanctions list, thus raising a red flag.

Dhaka delay

Jubair Bin-Huda, a joint director of Bangladesh Bank, was on duty that weekend and arrived at the bank's offices in Dhaka around 10:30 a.m. on Friday, Feb. 5, according to a police report. He and a colleague went to collect the latest SWIFT acknowledgement messages, which would normally have printed off automatically. They found none. They tried to print the messages manually but failed. The hackers had infected the system with malware that disabled the printer, and Bangladesh bank officials did not see the Fed's query and knew nothing of the fraudulent transactions. Instead, according to a police report, Huda assumed there was simply a printer problem - which had happened in the past -and asked other officials to fix it. He left work at around 11:15 am.

Since it was a Friday, the Islamic holy day, all other officials left the office at around 12:30 p.m., leaving the printer fix until later, the police report says. Later that day, Fed officials sent two other SWIFT messages to Dhaka. The first asked the same question for four of the five transactions that had already been cleared - and those four transactions included the name Jupiter. The second message asked about the 30 other payment instructions, including those queried the day before, according to sources close to Bangladesh Bank and an internal bank document seen by Reuters.

The messages did not get through. And the New York Fed did not reach out to Dhaka in any other way. It would often take up to three days for clients like Bangladesh to respond to SWIFT messages, said one former New York Fed employee. But the person added that by that point the New York Fed should have realized someone was trying to wire a billion dollars out of the account "and that's something way outside the norm." Huda returned to work on Saturday, Feb 6, around 9 am, and tried again to use the printer, only to discover the SWIFT software was not starting. Whenever he tried to boot it up, a message appeared on the monitor, saying "a file is missing or changed."

SWIFT messages

Only around 12:30 pm did bank staff finally manage to print the SWIFT messages. That's when they first saw the fraudulent transactions and the Fed's queries, and realized something had gone horribly wrong. They scrambled to find out more, but did not tell Atiur Rahman, then the bank's governor, what had happened until the next day. Rahman told Reuters he did not initially appreciate the gravity of the situation. "I never thought that this will become such a big event," he said. "The concerned deputy governor did not explain to me what really went wrong. He just told me that there was an incident like this and that they had already asked for stop payment. They were hopeful the money would be returned."

Rahman said deputy governor Abdul Quasem had told him the money was "still in the system" and would be recovered soon. "I said, 'do as you need, it's your department, so take care of it'," Rahman told Reuters. It later became clear much of the money would not be recovered, and Rahman resigned from Bangladesh Bank in March. Quasem, who also left the bank in March, declined to comment, citing ongoing investigations into the affair.

Tardy fed

As the scale of the theft sank in that weekend, the Fed's reliance on SWIFT messaging, its lack of alternative communications and its inertia became apparent. Since Bangladesh Bank's SWIFT system was still not fully working, officials there hunted for other ways to contact the Fed in New York. Lacking any obvious point of contact, they searched the Fed's website and found an email address - but it was only monitored during weekday business hours. On Saturday they fired off three emails to that address over several hours. The first included the line: "Our system has been hacked. Please stop all payment (debit) instructions immediately."

It was the weekend and Fed staff did not respond. That email address was unlikely to be synced to their mobile phones, according to a former New York Fed employee. Huda followed up with several calls and a fax to numbers obtained from the Fed website, according to a source close to Bangladesh Bank. Those numbers were also marked as weekday-only contacts and the Fed still did not respond.

On Monday, staff at Bangladesh Bank finally managed to get their SWIFT system operating and sent a message headed "Top urgent" to the New York Fed saying 35 payment orders were fake. "Please recall back funds if transferred from your accounts," it said. That message, sent around 1 am in New York, would have been seen when CBIAS employees arrived at 7:30 am. According to former CBIAS employees and senior officials at the New York Fed, it would have dropped like a bomb. The New York Fed, citing the criminal investigation, declined to comment on its communications with Bangladesh Bank and on what it did that Monday to attempt to recall Bangladesh Bank's money.

It was only on Monday evening in New York and Tuesday morning in Dhaka - four days after the heist began - that the New York Fed told Bangladesh Bank that it had alerted the correspondent banks to the fraud. A payment of $20 million to an account in Sri Lanka had already been reversed because of a spelling error in the request. But for four other payments made out to individuals it was too late: $81 million had gone to a Philippines bank and from there disappeared into the giant money-go-round that is the country's casino industry. (See related story: The Philippine connection).

The blame game began soon afterwards. SWIFT bridled at suggestions of flaws in its network and rejected any responsibility for the way Bangladesh Bank had installed its RTGS real-time gross settlement system. On Feb 11 and 14, Eddie Haddad, SWIFT's managing director for Asia Pacific, sent emails - seen by Reuters -to Rahman, then still governor of Bangladesh Bank. The emails implied that someone within the bank may have been involved in the heist. One said: "I have looked at the logs and the irregular message details, a user account was compromised within BB. —Reuters

EXCHANGE RATES

Al-Muzaini Exchange Co.

CURRENCY	BUY	SELL
	ASIAN COUNTRIES	
Japanese Yen	2.861	
Indian Rupees	4.518	
Pakistani Rupees	2.894	
Srilankan Rupees	2.084	
Nepali Rupees	2.826	
Singapore Dollar	225.070	
Hongkong Dollar	39.113	
Bangladesh Taka	3.868	
Philippine Peso	6.448	
Thai Baht	8.712	
	GCC COUNTRIES	
Saudi Riyal	80.950	
Qatari Riyal	83.386	
ani Riyal	788.462	
Bahraini Dinar	806.160	
UAE Dirham	82.648	
	ARAB COUNTRIES	
Egyptian Pound - Cash	31.250	
Egyptian Pound - Transfer	34.559	
Yemen Riyal/for 1000	1.219	
Tunisian Dinar	136.980	
Jordanian Dinar	428.350	
Lebanese Lira/for 1000	2.163	
Syrian Lira	2.0163	
Morocco Dirham	31.426	
	EUROPEAN & AMERICAN COUNTRIES	
US Dollar Transfer	303.400	
Euro	336.470	
Sterling Pound	403.520	
Canadian dollar	232.940	
Turkish lira	99.740	
Swiss Franc	310.860	
Australian Dollar	229.670	
US Dollar Buying	302.200	
	GOLD	
20 Gram	266.540	
10 Gram	136.190	
5 Gram	68.940	

Dollarco Exchange Co. Ltd

Rate for Transfer	Selling Rate
US Dollar	302.900
Canadian Dollar	232.445
Sterling Pound	393.145
Euro	335.450
Swiss Frank	298.925
Bahrain Dinar	801.276
UAE Dirhams	82.700
Qatari Riyals	83.910
Saudi Riyals	81.495
Jordanian Dinar	427.030
Egyptian Pound	34.013
Sri Lankan Rupees	2.088
Indian Rupees	4.508
Pakistani Rupees	2.888
Bangladesh Taka	3.857
Philippines Pesso	6.431
Cyprus pound	159.630
Japanese Yen	3.980
Syrian Pound	2.395
Nepalese Rupees	3.805
Malaysian Ringgit	76.475
Chinese Yuan Renminbi	45.630
Thai Bhat	9.585
Turkish Lira	104.965

Bahrain Exchange Company

CURRENCY	BUY	SELL
	Europe	
British Pound	0.392136	0.407136
Czech Korune	0.004379	0.016379
Danish Krone	0.040925	0.045925
Euro	0.0327915	0.0336915
Norwegian Krone	0.031696	0.036896
Romanian Leu	0.057018	0.087018
Slovakia	0.009051	0.019051
Swedish Krona	0.031251	0.036251
Swiss Franc	0.301728	0.312728
Turkish Lira	0.096793	0.107093
Australasia		
Australian Dollar	0.218988	0.230988
New Zealand Dollar	0.207066	0.216566
America		
Canadian Dollar	0.226207	0.235207
Georgina Lari	0.137008	0.137008
US Dollars	0.299250	0.304250
US Dollars Mint	0.299750	0.304250
Asia		
Bangladesh Taka	0.003397	0.003981
Chinese Yuan	0.044011	0.047511
Hong Kong Dollar	0.037039	0.039789
Indian Rupee	0.004376	0.004786
Indonesian Rupiah	0.000019	0.000025
Japanese Yen	0.002788	0.002968
Kenyan Shilling	0.003120	0.003120
Korean Won	0.000257	0.000272
Malaysian Ringgit	0.071286	0.077286
Nepalese Rupee	0.002861	0.003031
Pakistan Rupee	0.002728	0.003018
Philippine Peso	0.006352	0.006652
Sierra Leone	0.000067	0.000073
Singapore Dollar	0.218655	0.228655
South African Rand	0.015377	0.023877
Sri Lankan Rupee	0.001677	0.002257
Taiwan	0.009358	0.009538
Thai Baht	0.008347	0.008897
	Arab	
Bahraini Dinar	0.798072	0.806572
Egyptian Pound	0.027140	0.032258
Iranian Riyal	0.000084	0.000085
Iraqi Dinar	0.000182	0.000242
Jordanian Dinar	0.424763	0.433763
Kuwaiti Dinar	1.000000	1.000000
Lebanese Pound	0.000147	0.000247
Moroccan Dirhams	0.019363	0.043363
Nigerian Naira	0.001252	0.001887
Omani Riyal	0.781502	0.787182
Qatar Riyal	0.082511	0.083961
Saudi Riyal	0.079807	0.081107
Syrian Pound	0.001286	0.001506
Tunisian Dinar	0.133513	0.141513
Turkish Lira	0.096793	0.107093
UAE Dirhams	0.081166	0.082866
Yemeni Riyal	0.001371	0.001451