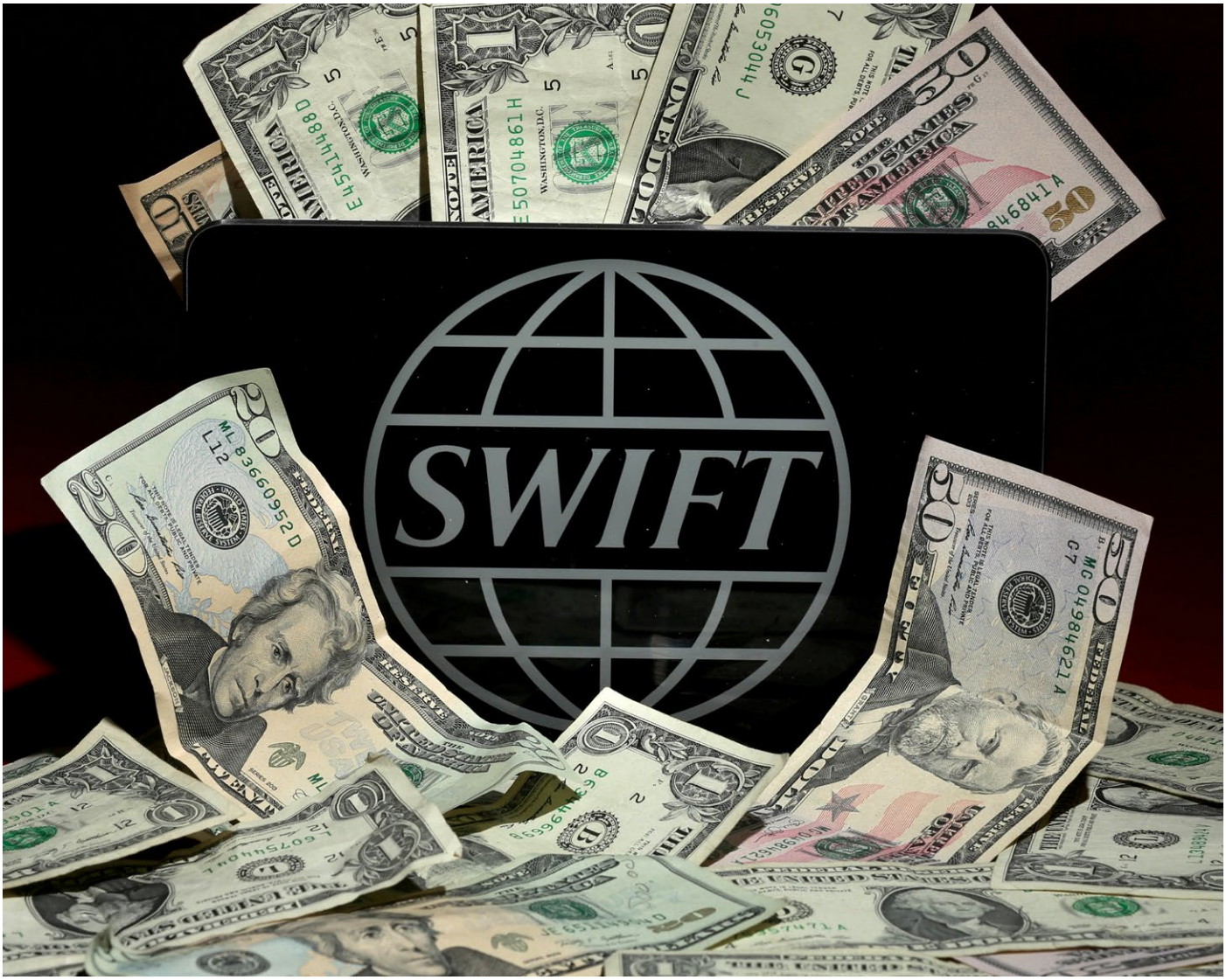


The Swift bank logo is pictured in this photo illustration. **Picture by Carlo Allegri**

How hackers stole $81 million from the Bangladesh central bank.

The Bangladesh Bank Heist

BY SERAJUL QUADIR, SHIHAR ANEEZ, TOM BERGIN, NATHAN LAYNE, KRISHNA N. DAS AND JONATHAN SPICER

MARCH 10 — DECEMBER 13 DHAKA/COLOMBO/LONDON/CHICAGO/NEW YORK

How a hacker's typo helped stop a billion dollar bank heist

BY SERAJUL QUADIR

MARCH 10 DHAKA

A spelling mistake in an online bank transfer instruction helped prevent a nearly $1 billion heist last month involving the Bangladesh central bank and the New York Federal Reserve, banking officials said.

Unknown hackers still managed to get away with about $80 million, one of the largest known bank thefts in history.

The hackers breached Bangladesh Bank's systems and stole its credentials for payment transfers, two senior officials at the bank said. They then bombarded the Federal Reserve Bank of New York with nearly three dozen requests to move money from the Bangladesh Bank's account there to entities in the Philippines and Sri Lanka, the officials said.

Four requests to transfer a total of about $81 million to the Philippines went through, but a fifth, for $20 million, to a Sri Lankan non-profit organisation was held up because the hackers misspelled the name of the NGO, Shalika Foundation.

Hackers misspelled "foundation" in the NGO's name as "fandation", prompting a routing bank, Deutsche Bank, to seek clarification from the Bangladesh central bank, which stopped the transaction, one of the officials said.

There is no NGO under the name of Shalika Foundation in the list of registered Sri Lankan non-profits. Reuters could not immediately find contact information for the organization.

Deutsche Bank declined to comment.

At the same time, the unusually large number of payment instructions and the transfer requests to private entities — as opposed to other banks — raised suspicions at the Fed, which also alerted the Bangladeshis, the officials said.

The details of how the hacking came to light and was stopped before it did more damage have not been previously reported. Bangladesh Bank has billions of dollars in a current account with the Fed, which it uses for international settlements.

The transactions that were stopped totalled $850-$870 million, one of the officials said.

Last year, Russian computer security company Kaspersky Lab said a multinational gang of cyber criminals had stolen as much as $1 billion from as many as 100 financial institutions around the world in about two years.

Iraqi dictator Saddam Hussein's son Qusay took $1 billion from Iraq's central bank on the orders of his father on the day before coalition forces began bombing the country in 2003, American and Iraqi officials have said. In 2007, guards at the Dar Es Salaam bank in Baghdad made off with $282 million.

> The transaction was too large for a country like us.
>
> A Pan Asia official

MONEY RECOVERED

Bangladesh Bank has said it has recovered some of the money that was stolen, and is working with anti-money laundering authorities in the Philippines to try to recover the rest.

A bank spokesman could not be reached for comment late on Thursday.

The recovered funds refer to the Sri Lanka transfer, which was stopped, one of the officials said.

Initially, the Sri Lankan transaction reached Pan Asia Banking Corp PABC.CM, which went back to Deutsche Bank for more verification because of the unusually large size of the payment, a Pan Asia official said.

"The transaction was too large for a country like us," the official said. "Then (Deutsche) came back and said it was a suspect transaction."

A Pan Asia spokesman could not immediately be reached for comment.

The dizzying, global reach of the heist underscores the growing threat of cyber crime and how hackers can find weak links in even the most secure computer networks.

More than a month after the attack, Bangladeshi officials are scrambling to trace the money, shore up security and identify weaknesses in their systems. They said there is little hope of ever catching the hackers, and it could take months before the money is recovered, if at all.

FireEye Inc's FEYE.O Mandiant forensics division is helping investigate the heist, people familiar with the matter told Reuters on Thursday.

The sources said Silicon Valley-based FireEye, which has investigated some of the biggest cyber thefts on record, was brought in by World Informatix, a smaller firm that is advising Bangladesh Bank on the investigation.

Security experts said the perpetrators had deep knowledge of the Bangladeshi institution's internal workings, likely gained by spying on bank workers.

The Bangladesh government, meanwhile, is blaming the Fed for not stopping the transactions earlier. Finance Minister Abul Maal Abdul Muhith told reporters on Tuesday that the country may resort to suing the Fed to recover the money.

"The Fed must take responsibility," he said.

The New York Fed has said its systems were not breached, and it has been working with the Bangladesh central bank since the incident occurred.

The hacking of Bangladesh Bank happened sometime between Feb. 4-5, over the Bangladeshi weekend, which falls on a Friday, the officials said. The bank's offices were shut.

Initially, the central bank was not sure if its system had been breached, but cyber security experts brought in to investigate found hacker "footprints" that suggested the system had been compromised, the officials said.

These experts could also tell that the attack originated from outside Bangladesh, they said, adding the bank is looking into how they got into the system and an internal investigation is ongoing.

The bank suspects money sent to the Philippines was further diverted to casinos there, the officials said.

The Philippine Amusement and Gaming Corp, which oversees the gaming industry, said it has launched an investigation. The country's anti-money laundering authority is also working on the case. ®

Additional reporting by **Jim Finkle** in Boston, **Jonathan Spicer** in New York, **Farah Master** in Hong Kong and **Shihar Aneez** in Colombo; Editing by **Paritosh Bansal** and **Raju Gopalakrishnan**

Sri Lankan in Bangladesh cyber heist says she was set up by friend

BY SHIHAR ANEEZ

MARCH 31 COLOMBO

When Hagoda Gamage Shalika Perera, a small Sri Lankan businesswoman, got a deposit of $20 million in her account last month, she said the funds were expected but had no idea they were stolen from Bangladesh's central bank in one of the largest cyber heists in history.

Unknown hackers breached Bangladesh Bank's systems between Feb. 4 and Feb. 5 and tried to steal nearly $1 billion from its account at the Federal Reserve Bank of New York.

Many of the payments were blocked. But $20 million made its way to Perera's Shalika Foundation before the transfer was reversed. Bangladesh central bank officers said they acted after a routing bank, Deutsche Bank, sought clarification on the transfer because hackers misspelled the company's name as "Fundation."

Another $81 million was routed to accounts in the Philippines, and diverted to casinos there, where the trail runs out.

The Philippines Senate is holding hearings in the case, but until now, few details had emerged on the Sri Lanka link.

In her first public comments on the case, Perera, a struggling businesswoman who heads Shalika, told Reuters she expected $20 million to come from the Japan International Cooperation Agency (JICA) to help fund a power plant and other projects in Sri Lanka. She said she had no direct dealing with JICA, but the deal was arranged by an acquaintance who she met in Sri Lanka but had connections in Japan.

Shalika was set up in October 2014 and says in its registration documents that it constructs low-cost houses and provides other social services.

Reuters was unable to independently confirm Perera's account or to reach the acquaintance she named, via the email and phone numbers she provided.

JICA, a Japanese government agency that provides official development assistance, said it has no ties with Shalika Foundation, including through any intermediaries.

"We have had no exchange with them, and that includes such areas as loans and grants," JICA spokesman Naoyuki Nemoto said.

The Sri Lankan police's criminal investigation division declined to comment because the probe is ongoing.

"GENUINE PEOPLE"

"We are very genuine people. We are not doing any illegal things," said Perera, speaking in English and Sinhalese in an interview

> Maybe they used this government organisation's name to make it believable.

Brigadier General Moin Uddin
The head of the Bangladesh government agency, the Bangladesh Rural Electrification Board

in Colombo, the Sri Lankan capital. The 36-year-old was accompanied by her husband, Ramanayaka Arachchige Don Pradeep Rohitha Dhamkin, also a director in her company.

Perera said she now thinks the acquaintance was either a victim of the hackers or in league with them, and she was hoodwinked into becoming a part of their scheme.

She showed Reuters a copy of an inward remittance advisory from the SWIFT bank messaging system to put the $20 million in her company's account. The remitting entity was shown as a Bangladesh government electricity agency that had taken a loan from JICA in 2010 to fund an electricity project.

The head of the Bangladesh government agency, the Bangladesh Rural Electrification Board, said it was "ridiculous" to think that the money could have come from them.

"Maybe they used this government organisation's name to make it believable," said Brigadier General Moin Uddin, the agency head.

Police have questioned Perera's acquaintance, according to an investigation report filed in the Colombo Magistrate's Court on Thursday. The man told authorities that a Japanese middleman had helped arrange the funding, according to the report.

The report provided the names of Perera's acquaintance whom Reuters has been unable to locate and the Japanese middleman. Reached by phone, the middleman said he was travelling and unable to provide immediate comment.

The court has ordered a travel ban on Perera, her husband, the acquaintance and four other people listed as directors of her company.

Perera maintains she is innocent and describes the government's move as "an injustice".

STRUGGLING BUSINESSWOMAN

Perera is, by her own admission, struggling. She said she has four other enterprises, including a publishing firm, an auto parts company, a construction company and a catering firm.

In 2014, losses from her publishing firm were so bad that she was forced to sell her computers. She said she now does her business from Internet cafes, and held meetings with potential investors at Pizza Hut and other restaurants.

In early February, Perera said her acquaintance, who had been helping her for more than a year to meet investors, told her to expect $20 million from JICA. Under their agreement, the payment would be split, between her power plant project and a housing project controlled by her acquaintance, she said.

According to a Sri Lankan police investigation report seen by Reuters last week, Perera told her bank, a Colombo branch of Pan Asia Bank PABC.CM, that the company expected to receive $20 million from a Japanese fund.

A Pan Asia Bank official declined to comment, citing the investigation.

Perera said she had not seen the report, which was submitted to the magistrate's court last week.

According to the report, bank officials said Perera left instructions with them to transfer $7.72 million to her own personal account and $11.12 million to an account controlled by her acquaintance once the transaction had cleared.

Perera confirmed she had given the instructions to the bank, and said they reflected the money earmarked for the two projects and commissions. The rest was to be used for taxes, she said.

The money was remitted by the Pan Asia Bank to Shalika Foundation's account on Feb 4, but the bank refused to release the funds as the amount was unusually large and sought further verification, according to last week's police report.

On Feb. 9, Perera was told by her bank that the Bangladesh central bank had asked for the transaction to be reversed, according to the report. ®

Additional reporting by **Ranga Srilal** in Colombo, **Serajul Quadir** in Dhaka and **Kiyoshi Takenaka** in Tokyo; Writing by **Paritosh Bansal**; Editing by **Raju Gopalakrishnan**

How the New York Fed fumbled over the Bangladesh Bank heist

BY KRISHNA N. DAS AND JONATHAN SPICER

JULY 21 DHAKA/NEW YORK

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 scrutinise 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 U.S. 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 U.S. 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 U.S.

> 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
Democratic congresswoman from New York

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 U.S. 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 U.S. 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 U.S. 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 a.m. 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 U.S. 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 judgements 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 U.S. economic sanctions or money laundering regulations. They may ask clients for more information.

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 U.S. 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 U.S. 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.

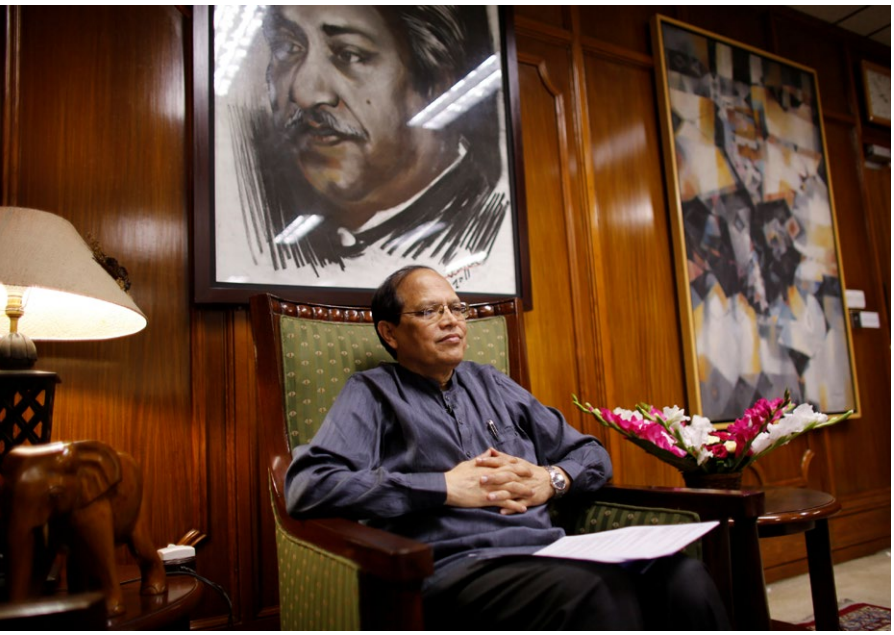
The hackers had infected the system with malware that disabled the printer, and Bangladesh bank officials did not see the Fed's query and knew nothing of the fraudulent transactions. Instead, according to a police report, Huda assumed there was simply a printer problem — which had happened in the past —and asked other officials to fix it. He left work at around 11:15 a.m.

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 realised 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 a.m., 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."

Only around 12:30 p.m. 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 realised something had gone horribly wrong. They scrambled to find out more, but did not tell Atiur Rahman, then the bank's governor, what



Bangladesh's central bank Governor Atiur Rahman poses inside his office in Dhaka. **Picture by Andrew Biraj**

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 a.m. in New York, would have been seen when CBIAS employees arrived at 7:30 a.m.. 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.

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. It has nothing to do with the SWIFT RTGS channel."

On Feb. 19, Alain Raes, SWIFT's head in Europe, the Middle East and Africa, again raised that possibility, writing in an email to Rahman: "While any conclusion would be premature given the limited evidence and our limited view on the events and their context, this could point to sophisticated outsider acting with help from a malicious insider from the Bangladesh Bank."

SWIFT, Haddad and Raes declined to comment on the issue for this story.

Bangladesh Bank declined to comment. A panel appointed by the Bangladesh government to investigate the heist said in a report in late May that it suspects some insider involvement. It gave no details. Senior police investigator Mirza Abdullahel Baqui said officials were being questioned but only for negligence.

Relations between Bangaladesh Bank and the New York Fed also soured. On Feb. 24, the bank wrote to the Fed asking what actions it had taken over the payments and why it had failed to stop them. In early May, Fazle Kabir, who had taken over as governor of Bangladesh Bank, wrote to William Dudley, president of the New York Fed, posing similar questions. Dudley telephoned Kabir to arrange a meeting in Basel, Switzerland, on May 10.

That meeting was chaired by Gottfried Leibbrandt, chief executive of SWIFT, who was accompanied by his general counsel. The New York Fed was represented by Dudley, Baxter, and other officials. Bangladesh Bank was represented by Kabir, other officials and Ajmalul Hossain, a prominent Dhaka lawyer.

The three parties agreed to cooperate. But according to people familiar with the discussion, the two banks left the meeting unsatisfied. The New York Fed is frustrated by Bangladesh Bank's refusal to share with it a review of its cyber security. Bangladesh Bank feels the Fed should have spotted the unusual nature of the transactions, according to a source close to the Asian bank. Further talks are planned, this time at the New York Fed's Wall Street headquarters.

The heist has already prompted a handful of formal requests for information from members of the U.S. Congress, and Fed Chair Janet Yellen faced questions on the incident during hearings last month. Maloney, who sits on the House Financial Services Committee that directly oversees the central bank, said she plans to ask the Republican chair to schedule a committee hearing on the incident.

She also told Reuters she plans to ask the New York Fed for a clearer explanation why five fraudulent payments were made back in February while the others were not. "Why? What was the difference?" she asked. ®

Jonathan Spicer reported from New York and **Krishna N. Das** from Dhaka. Additional reporting by **Sanjeev Miglani, Serajul Quadir** and **Ruma Paul** in Dhaka, **Karen Lema** and **Manny Mogato** in Manila and **Shihar Aneez** in Colombo, **Tom Bergin** in London and **Jim Finkle** in Boston.; Editing By **Richard Woods** and **Raju Gopalakrishnan**

Some Bangladesh Bank officials involved in heist -investigator

BY RUMA PAUL

DECEMBER 13 DHAKA

Some Bangladesh central bank officials deliberately exposed its computer systems and enabled hackers to steal $81 million from its account at the Federal Reserve Bank of New York in February, a top police investigator in Dhaka told Reuters on Monday.

The comments by Mohammad Shah Alam, head of the Forensic Training Institute of the Bangladesh police's criminal investigation department, are the first sign that investigators have got a firm lead in one of the world's biggest cyber heists, which had prompted months of international finger-pointing. Arrests are soon likely, he said.

On Thursday, the head of a Bangladesh government panel that investigated the heist said five bank officials were guilty of negligence but that they were only unwitting accomplices.

Alam told Reuters his investigations had discovered that some bank officials had knowingly created vulnerabilities in the bank's connection to the SWIFT global messaging and payments system.

"Bangladesh Bank's SWIFT network was made insecure by some bank employees in connivance with some foreign people," he said. "They knew what they were doing."

He declined to name the suspects or say how many there were.

Alam said investigators were now trying to find out how the mid-ranking officials were connected to the hackers and whether they benefited financially from the heist. Asked if the officials would be arrested, he said: "We are very close to it."

The apparent momentum comes after months of trading blame among Bangladesh Bank, the New York Fed, SWIFT, and a Philippine lender that received much of the stolen funds before they disappeared. The heist prompted an international probe headed by the U.S. Federal Bureau of Investigation.

Separately SWIFT, or the Society for Worldwide Interbank Financial Telecommunication, told Reuters its messaging system has been targeted in a "meaningful" number of other attacks this year using a similar approach as the Bangladesh incident.

Bangladesh Bank spokesman Subhankar Saha declined to comment on Alam's comments. A New York Fed spokeswoman also declined comment.

Another investigator in Dhaka, who declined to be named, said more than 100 Bangladesh Bank employees had been interviewed in connection with the heist, and some were barred from leaving the country.

In early February, the hackers used the SWIFT network to send fake orders requesting the transfer of nearly $1 billion from Bangladesh Bank's account at the New York Fed.

Many of the transfer orders were blocked or reversed but, after a series of oversights and miscommunications, the New York Fed ultimately sent $81 million to four fake accounts in a branch of Rizal Commercial Banking Corp (RCBC) in the Philippines. Most of the funds then disappeared into Manila's loosely regulated casino industry. ®

Additional reporting and writing by **Krishna N. Das** and **Jonathan Spicer**; Editing by **Raju Gopalakrishnan** and **Phil Berlowitz**