



STOCKS	
DSEX	CSCX
▲ 0.56%	▲ 0.42%
4,506.87	8,312.36

COMMODITIES	
 Gold ▼	 Oil ▼
\$1,578.50 (per ounce)	\$56.23 (per barrel)

ASIAN MARKETS			
MUMBAI	TOKYO	SINGAPORE	SHANGHAI
▲ 0.34%	▼ 1.01%	▼ 1.19%	▼ 7.72%
39,872.31	22,971.94	3,116.31	2,746.61

CURRENCIES				
	USD	EUR	GBP	CNY
BUY TK	83.95	92.21	109.85	11.79
SELL TK	84.95	96.01	113.65	12.43





**Quicker
Easier & Safer**

Fund transfer, Utility bill payment,
Top up mobile balance,
Credit card bill payment
& many more





Social Islami Bank Limited



BUSINESS

DHAKA TUESDAY FEBRUARY 4, 2020, MAGH 21, 1426 BS starbusiness@thedailystar.net

The billion-dollar hit job

REJAUL KARIM BYRON *and*
MD FAZLUR RAHMAN

The way unknown hackers hatched plans to steal money from the Bangladesh Bank's reserves with the New York Fed using the most sophisticated banking and payment channels as well their near-perfect preparation and timing will render many detective stories and Hollywood movies average.

This largely explained why the largest cyber hacking in history has still remained unresolved four years after it shook the financial world.

In February 2016, hackers breached the BB's systems and used the SWIFT messaging network to order the transfer of \$951 million from the central bank's account at the New York Fed.

Of the amount, \$81 million ended up in the bank accounts in the Philippines, which were quickly withdrawn and sucked in by the huge casino industry in the Southeast Asian country.

The hacking was so well-planned that it took the BB until the middle of March to retrieve the related SWIFT messages, according to the report of the government-sponsored probe committee.

A three-member committee led by former BB Governor Mohammed Farahuddin began working on March 20, 2016. The probe report was submitted in May 2017, but the government is yet to make the report public.

The 27-page report shed light on the people and the organisations whose actions might have paved the way for the hacking as well as the organisations that had the power to stop it but failed to do so. It made 70 recommendations to prevent repetition of such heists.

The root to hack the BB network and its reserves could be traced at least six months before the heist took place.

In August 2015, the computers of the BB were connected with the SWIFT network through the Real-Time Gross Settlement (RTGS), which is used to process local



transactions and without taking any expert opinion.

The establishment of the link on August 13 paved the way for the hackers to deploy malware in the SWIFT messaging system as it created scope for any computer of the local area network (LAN) to send SWIFT messages to the New York Fed, according to the probe report.

The report raised questions about the visit of a SWIFT official, who worked almost privately on the SWIFT system at the BB. Then the SWIFT officials also did not inform the BB officials how the link between the SWIFT and the BB-RTGS works.

The SWIFT official used the user ID and password of two BB officials to work in the system. So, it was not difficult to know about the finger stroke, password and other important codes.

The user ID and password of the two BB officials were compromised after January 24, 2016, the report said.

A malware was deployed into the SWIFT system on January 19 or 20, 2016 that copied the user ID and password; the credentials were later used in hacking and transferring the funds.

The malware identified is advanced and custom-designed to operate on servers processing SWIFT transactions.

It has the capability to bypass certain software security measures especially related to the BB's SWIFT environment and was rigged to securely erase all traces of activity and self-destruct on February 6, 2016 after accomplishing its goal, said the probe report quoting a primary report of world-renowned cyber security firm FireEye Mandiant.

The criminals chose the day for the hacking wisely: February 5 and 6 were weekends in Bangladesh, February 6 and 7 were weekends in the US and February 6 and 8 were bank holidays for the Chinese New Year in the Philippines.

Hackers, using the user name and password of a BB official of the accounts and budgeting department, generated 35 SWIFT messages

between 8.36pm on February 2016 and 3.59am the following morning and instructed the NY Fed to release around \$951.01 million to four beneficiaries through intermediary banks.

While the NY Fed's security system flagged the payment orders, five of them fell through, and \$101 million against them was released. Of the amount, \$81 million was wired to the Philippines (RCBC branch in Manila) and \$20 million to Sri Lanka's Shalika Foundation.

Ultimately, the Sri Lankan bank that received that payment order -- the Pan Asia Banking Corporation --flagged it because it misspelled the word "Foundation" as "Fundation". The size of the transaction was unusual, too.

Mandiant's probe showed that the traces to collect information, particularly the SWIFT messages, generated on February 4 were erased. SWIFT could not retrieve them.

Hackers usurped the Fedwire system -- which is developed and maintained by the Federal Reserve System and used to transfer large-dollar payments among Federal Reserve offices, depository institutions and federal

government agencies -- to steal funds from the BB's account at the New York Fed by transferring them to correspondent accounts held by RCBC, according to a court document of a case filed by the BB with a New York court.

The conspirators took advantage of certain features of the Fedwire system and timing to accomplish their theft. Fedwire system transfers are same-day and, in many cases, instantaneous. Transferred funds are often available and final when sent.

Armed with this knowledge, the conspirators sent the unauthorised payment orders after business hours at the start of the weekend in Bangladesh -- which is Friday and Saturday in Bangladesh -- in an attempt to action the transfers before the New York Fed or Bangladesh Bank could discover the theft, the case document said.

BB high-ups came to know about the stealing two days later. Still, the central bank decided to keep it secret.

Then Governor Atiur Rahman told the probe committee that he talked to Amando M Teranga Junior, then central bank governor of the Philippines, on February 11.

The Filipino governor said if utmost secrecy about the stealing can't be ensured the wrong-doers might escape and assured Rahman that the whole amount might be retrieved quickly if secrecy can be maintained, Rahman told the probe committee.

This led the then governor to decide not to report the incident to any intelligence agency until March 1.

But after the Inquirer of Manila broke the news on February 29, the whole world came to know about the incident.

WHO IS TO BLAME?

The central bank of Bangladesh, the SWIFT network and the New York Fed can't evade their responsibility in the reserve heist, said a probe report.

Rizal Bank of the Philippines did not act fittingly.

RCBC staged a scandalous drama by implementing the fund transfer messages on February 9 despite receiving "stop payment" requests from Dhaka.

Maia Santos-Deguito, manager of Jupiter branch that released the funds, said she had carried out the fund transfer orders "out of fear". RCBC CEO Lorenzo Tan resigned.

"It is a huge surprise that four accounts were opened with RCBC just by depositing \$500 six months before the heist and multi-million dollars were deposited in the accounts despite getting "stop payment requests", the report said.

READ MORE ON B3

Export diversification hinges on access to bonded warehouse

Analysts say at SANEM conference

STAR BUSINESS REPORT

Easing access of non-RMG sectors to bonded warehouse benefit, an opportunity to ensure duty-free import of raw materials of export items, is vital to diversify the country's export basket, said analysts yesterday.

The National Board of Revenue (NBR) provides duty-free import benefit to exporters under the bonded warehouse scheme and benefit is mostly enjoyed by apparel exporters.

Around 84 per cent of Bangladesh's export basket of \$40.5 billion in fiscal year 2018-19 was filled up by ready-made garments while the rest 16 per cent failed to reap the bonded warehouse

IMPORTS AND TAX EXEMPTION UNDER BONDED WAREHOUSE		
SECTOR	Fiscal Year: 2016-17	
	IMPORT TK IN CRORE	TOTAL IMPORT TAX EXEMPTED (Tk in crore)
RMG and knitwear	47,795	33,612
Footwear	127	47
Others	2,138	1,221
Total bonded imports	50,060	34,880

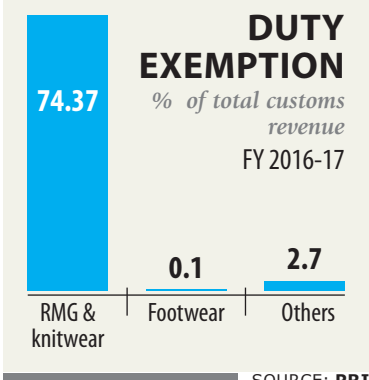
SOURCE: PRI

privilege fully.

Lack of readiness of the revenue authority to provide similar treatment to all export sectors, partly because of its inadequate resources to monitor all the bond

licence-holders, is blamed for non-RMG sectors' failure to reap full advantage of bond facility.

"Export diversification is linked to existence of bonded warehouse facility as it provides scope to buy



SOURCE: PRI

raw materials at international prices. This facility needs to be extended to other sectors," said Zaidi Sattar, chairman of the Policy Research Institute of Bangladesh.

READ MORE ON B3

'If we face any challenges, customers will suffer'

New Grameenphone CEO says they will focus more on innovation, local digital services

STAR BUSINESS REPORT

Grameenphone will give more emphasis on innovation and localisation of digital services in the days to come and raise its game further to understand the needs of customers, said Yasir Azman, chief executive officer of the country's leading mobile phone operator, yesterday.

The operator will go through a rough patch while ensuring a quality network if the ongoing disputes with the regulator are not resolved within the next few weeks, said Azman in his first press meet after becoming the first Bangladeshi national to take the reins of the company.

Grameenphone has not been able to invest as per its plans for the last six months and if the situation lingers for another six months, its



Grameenphone CEO Yasir Azman talks to reporters at its head office in Dhaka yesterday.

COLLECTED

network will fail to bear the huge loads of customers, he said.

"A large number of customers and businesses are dependent on our network. If we face any challenges, our customers will suffer," Azman said at the briefing at their headquarters in the capital.

He termed the situation critical, saying the regulator is being rigid with the allocation of second mobile numbering scheme, due to which existing allotment will run out within a week or two. Operators cannot also sell used SIMs.

Grameenphone has been barred by the regulator from rolling out new packages/services or importing network equipment in an attempt to pile up pressure on the operator to clear dues of Tk 12,580 crore as per audit claims.

READ MORE ON B3

GOVT PROMISES LIFT STOCKS

Stocks edged up in the last two sessions, mainly due to some positive developments, lifting the benchmark index of theDhaka Stock Exchange to over 4,500 points. The finance minister has announced that seven state-run companies will offload their shares, while Bangladesh Bank promised to offer liquidity support to the market.

DSEX rose to **4,506.87** points (advanced **25.36** points, or **0.56%**)

Daily turnover rose to Tk **506.35** crore (increased Tk **41.65** crore, or **8.97%**)

TOP FIVE GAINERS	
Company	Gain (in %)
Titas Gas	9.84
Usmania Glass	9.83
Fu Wang Food	9.24
Phoenix Finance 1st Mutual Fund	9.23
Advent Pharmaceuticals	9.05

TOP FIVE LOSERS	
Company	Loss (in %)
United Airways	10
Fu Wang Ceramics	6.83
LafargeHolcim	5.15
Golden Son	4.76
Shyampur Sugar	4.72

TOP SECTORAL GAIN	
Sector	Loss (in %)
Telecommunication	5.75
Fuel & Power	1.94
Textile	1.62
Engineering	1.55
Non-bank Financial Institutions	0.78

TOP TURNOVER	
Company	Average turnover
LafargeHolcim	Tk 40.83 in crore
Khulna Power	Tk 24.81 in crore
Summit Power	Tk 20.23 in crore
BSC	Tk 16.18 in crore
Grameenphone	Tk 15.24 in crore

DSE BROAD INDEX

