

Banker in midst of heist controversy

FROM PAGE 1

What is more, Deguito was offloaded from a Philippine Airlines flight heading for Tokyo on Friday, after the Southeast Asian country's Anti-Money Laundering Council (AMLC) treating her as "part of the money-laundering scheme".

She was barred from leaving the country ahead of a Senate investigation into her alleged involvement in the cross-border remittance transaction.

A photo published yesterday on the Inquirer, the news site that broke the story, showed she was walking in Ninoy Aquino International Airport after being offloaded from the plane.

The news outlet said Deguito not knowing that she was on the lookout list of the Bureau of Immigration, had tried to leave the Philippines.

She was already aboard Philippine Airlines Flight 432 with her husband and son when immigration officials came aboard and took them off the plane.

David de Castro, spokesperson for the Manila International Airport Authority, said they were "off-loaded" on orders from the immigration bureau.

Nikki Reyes, spokesperson for the immigration bureau, said Deguito had been included in the immigration lookout list on orders of the Department of Justice.

A source told the Inquirer that Senator Serge Osmeña III, who is leading a Senate investigation into the alleged laundering, had asked the justice department to stop

were just following orders], she said.

She did not say where she and her family were taken, but an airport source told the Inquirer that they were taken to the immigration bureau's main office in Intramuros, Manila.

In the radio interview, Deguito also said she was "just a small person" to be blamed for the mess at RCBC.

"I'm just an employee. All I know is I never did anything wrong," she said.

Asked if she was willing to be a state witness in the investigation, Deguito said she was afraid to do so.

"It's the same. It will be like I'm in prison," she said. "What I know is, I did not do anything wrong. I did not steal anything. I did not get anything."

Now it emerges that the branch manager as well as the head of the bank apparently had the knowledge about the stealing of BB's money from its account with the New York Fed.

Businessman William S Go, one of six people under investigation for the alleged money laundering, said an affidavit submitted to the NBI claims that Deguito had told him that two bogus accounts had been set up at her branch to handle a large US dollar remittance coming from Bangladesh. It said the money was converted into pesos with the approval of the RCBC head office.

William Go denied being involved in the alleged money-laundering operation, claiming that Deguito had forged his signature to open an account in his

branch," said Deguito.

Tan has denied knowledge of the scheme.

On Friday, Tan's lawyer Francis Lim said Tan had offered to go on leave to give the bank a free hand in investigating the alleged money laundering.

In an interview on Monday, lawyer Ferdie Topacio said his client, Deguito, had told him that she received specific instructions directly from RCBC CEO Tan to allow the transfer of \$81 million into five accounts in her branch.

In a press statement on Wednesday, however, Tan branded "malicious" the "insinuations" that the RCBC top management had approved the multimillion-dollar transfer into the Jupiter branch, which later turned out to be part of an international money-laundering scheme.

Deguito said apart from the \$81 million "plus" that was credited to her branch, "there was a call [on February 9] from the settlement department of the bank that there was an additional payment but they no longer credited it (in the Jupiter branch accounts) because they reportedly said there was a recall."

"As to how much was that, I have no idea," she said.

Deguito said the money that was credited to her branch "went through the process".

"I was not the one who credited that straight. There is a department at the head office that handles the remittance. So there's a long process that needs to be followed before the money reaches my branch," she said.

Deguito said she instructed her assistant to e-mail the remittance department for information about the source of the funds and what they were intended for.

"They did not call me. [The money] was just credited in the account. And now it's all my fault," she said.

Deguito acknowledged that Michael Francisco Cruz, Jessie Christopher Lagrosas, Enrico Teodoro Vasquez, and Alfred Santos Vergara opened accounts at her branch.

Deguito said she first met the holders of the subject accounts on March 13, 2015, at Solaire Resort and Casino, claiming this was upon the referral of a casino high-roller.

The accounts were allegedly used for receiving the funds from the Bangladesh Bank that were to be transferred from its account in the New York Fed.

The accounts were later consolidated into one of Go's accounts at Deguito's branch and allegedly laundered through three casinos in Manila, reported the Inquirer.

The immigration bureau's order to stop Deguito from leaving the Philippines was a violation of constitutional and human rights, her lawyers said yesterday.

"We condemn in the strongest terms possible the blatant violation of the Constitutional and Human Rights of our client, Ms Maia Santos-Deguito, perpetrated by the Department of Justice and the Bureau of Immigration, in forcibly offloading her, her husband and 10-year-old son from a plane at the last minute that it was about to leave for Japan," lawyer Ferdinand Topacio said in a statement.

"The heavy-handed manner by which the offloading was done, which would not be out of place in a police state such as North Korea, has traumatised not only Ms Santos-Deguito and her husband, but worse, her child of tender years, who kept crying throughout the ordeal and even all the way back home, as he could not, in his young mind, understand why his plane going to Disneyland left without him," he added.

Hackers stole \$101 million from the BB's account with the New York Fed. Of the amount, \$20 million went to a bank in Sri Lanka, and the money has been recovered, according to the BB.



3 Possible behaviour of malware

Once installed, the Malware will:

1. Search saved confidential files
2. Generate unusual Internet activities that should come to notice of IT supervisors
3. May take screen shots of users silently
4. May log keystrokes to detect passwords
5. Send files to hackers

Dangerously exposed

FROM PAGE 1

The SWIFT statement read: "SWIFT and the central bank of Bangladesh are working together to resolve an internal operational issue at the central bank. SWIFT's core messaging services were not impacted by the issue and continued to work as normal."

So if the Fed was not compromised and neither was SWIFT, what may have gone wrong? Let's analyse the issue.

First we should know about SWIFT. It is a cooperative society under Belgium law owned by its member financial institutions that provide encrypted messaging service to facilitate global financial orders.

Its communication has so far proven hack-proof because these are end-to-end encrypted and sent through its own IP network infrastructure known as SwiftNet. As such there is no chance for outsiders to intercept messages using any malware or Man-in-the-Middle (MitM) attack.

MitM is an attack where the attacker secretly relays and alters the communication between two parties who believe they are directly communicating with each other, in this case, between Bangladesh Bank and the Fed.

But since SWIFT has its own protocol network and software which relies on high encryption, it is highly unlikely that an MitM attack breached the security.

So then what may happen? The answer may lie with the endpoint malpractice or abuse, in this case at the Bangladesh Bank.

The BB uses the BTCL backbone for all electronic communication. The mainframe server of Bangladesh Bank should have been connected with the BTCL with a secure intranet communication, which should be isolated from any sort of internet communication to avoid outside injection of malware. If this was the practice, then the SWIFT

communication should have been completely secure as the mainframe server has no possibility of being infected.

So the Bangladesh Bank should clarify if this network architecture it was following. And if this was being followed, the only way the SWIFT communication could have been exploited is by physical access to the mainframe server. This would clearly be a case of insider job.

But if the BB had not used intranet-based secure communication, then a different scenario comes out. In that case, it had used internet to connect with the BTCL server with an exposed endpoint to internet. Hackers then can use that endpoint to get inside the network of the central bank.

But suppose the BB had used intranet with the BTCL, still it could have an exposed endpoint if its mainframe server was connected with other computers or even a single computer on the premises which had internet access. In that case it would leave the system accessible to outsiders via that computer with internet access.

If this was the case, we are not dealing with an insider job but with a very sloppy IT architecture for which relevant people must be held accountable and, if proven, punished.

If malwares were injected, there would certainly be symptomatic signals. There would have been a sudden wave of outgoing data requests or some other symptoms that would have immediately raised alarm in the fire fighting section. What did the IT department do? Do they not have any network monitoring tool to detect suspicious network activities during weekend or off-office hours? Or was the system too weak that nobody checked the doubtful operations?

There are many more questions. For example, we still do not know when

the BB had first acted after the fund was transferred. Even in personal banking, an unauthorised transfer can be checked by taking immediate steps. So then why could the BB not stop the fund disbursement? Every fund transfer is notified through various platforms. In this case, is it enough of an explanation that the BB could not know about the fund transfer immediately because of Friday and Saturday being holidays and also days of the heist? This only reveals the sheer callousness of the central bank in handling its IT operations.

Where was the BB's two-way security policy? Even in simple day-to-day emailing, a user may enable a system that would generate a code on the user's mobile every time he wants to log in and he has to put that code to access his mail. If a simple email system can have such security measures then why should the BB not have a better or at least the same kind of security layer? Or is it that it did have the security layer but it was compromised because of an insider link?

With all the security measures mentioned here, the BB server could still be hacked if someone injects a malware physically using a USB drive or a CD Rom. Still, that makes it an insider job.

There are numerous other questions that remain unanswered. How the BB reacted to the whole thing also raises a lot of questions. It kept the thing under the wrap for about a month and did not even inform the finance ministry. We came to know about the incident only after the whole thing came out in the Philippines newspaper. Would we have ever known if the Manila-based newspaper did not publish the story? How do we know there were not more transfers we do not know about because these were not reported by newspapers?



Lawyer Ramon Esguerra shows a text message of his client William Go in Makati City on Friday. PHOTO: STAR

Deguito from leaving the country.

RCBC lawyers had asked Osmeña to intervene and keep Deguito in the country, the source said.

Deguito, at whose bank branch the \$81 million was transferred by unknown computer hackers from the BB's account in the Federal Reserve Bank of New York, is under investigation by the RCBC management.

The AMLC of the Philippines and the National Bureau of Investigation (NBI) are looking into the operation to launder the stolen money through the Philippine financial system.

The Senate committee will open its own investigation on Tuesday.

No charges have been brought against Deguito, but she said in a radio interview on Friday that immigration officers showed her a fax from the AMLC stating that she was "part of the money-laundering scheme".

"[It means] they should not allow me to escape from the law. But I'm not really escaping from anything," Deguito said.

She said she had been receiving death threats since reports of the alleged money laundering broke, but she was just taking her son to Disneyland in Tokyo as a birthday gift.

Deguito said the immigration officers showed her no subpoena. Neither from the Senate that summoned her to next week's hearing, nor from a court.

"[My lawyer] talked to the immigration officers, but they kept saying [they

name at the bank.

In a press conference on Friday, Go's lawyer Ramon Esguerra said the accounts in his client's name at the RCBC Jupiter branch were bogus and that Go's signatures were forged by the branch manager.

"Ms Santos [Deguito] admitted to me that she opened Centuryx's RCBC accounts to facilitate the deposit of a substantial amount of US dollar remittance allegedly coming from Bangladesh, which she later converted to Philippine pesos. She said her actions were all cleared and allowed by RCBC 'head office,'" Go said in a sworn statement that was distributed to the media at the press briefing.

Esguerra said Go and Deguito had known each other before the latter joined the RCBC.

Deguito said she knew Go, but denied Go's allegations raised through his lawyer Ramon Esguerra that she met with the businessman and asked him to sign documents that would close his account at her branch.

Asked whether Go was lying, she said, "I will answer that in the Senate."

Asked if RCBC president and CEO Lorenzo Tan knew about the alleged money laundering, she said she assumed he did.

"I'm not accusing him. I will just assume, because this is a huge amount of money. It will be credited to the treasury of the bank before it gets credited to our

Not a worker to be hired by KL

FROM PAGE 1

"There will not be one, let alone 1.5 million new foreign workers coming into our country," he said, according to Malaysian news site The Star Online.

Minister Nurul Islam or acting secretary Begum Shamsunnahar could not be contacted as their mobile phones were found switched off.

Mohammed Abul Basher, president of Bangladesh Association of International Recruiting Agencies (Baira), however, said such a decision of Malaysia was undignified for both the countries.

"Malaysia should have thought well ahead of the MoU signing [on February 18]," he told this correspondent.

He recalled that Malaysia in 2009 cancelled visas of 55,000 Bangladeshis, who therefore were financially affected.

The Malaysian deputy prime minister told reporters at Bagan Daton in Malaysia that employers who need workers will have to apply to legalise the existing foreigners without work permits or whose permits have expired.

Employers had until June 30 to legalise such foreign workers.

"If they can't hire anyone, they should just get the Malaysian Employers Federation, Federation of Malaysian Manufacturers and Malaysian Trade Union Congress to

help them find locals to do the job," said Zahid, who is also the home minister.

Following this, employers and recruitment agents would be dealt with more severely, he said.

"We will be pushing for those found guilty of trafficking and harbouring illegal workers to be caned," he added.

"Right now, they are not afraid because they think they can get away by paying a fine but that will not be the case anymore."

Yesterday's announcement of regularising the undocumented foreign workers is contrary to the statement of the same minister that all the undocumented foreign workers in Malaysia would be arrested and deported.

The policy changes of Malaysia are important as an estimated 2 lakh of the 6 lakh Bangladeshis in Malaysia are believed to be without valid papers, and recently there have been reports of more arrests of the foreign workers, including Bangladeshis, in various areas of Malaysia.

CONTROVERSIES

LABOUR RELATIONS BETWEEN Kuala Lumpur and Dhaka have been tarnished by malpractices and labour abuses that led to recruitment bans by Malaysia several times since formal labour recruitment from Bangladesh began in the 80s.

In late 2012, Malaysia had signed a

deal for recruiting workers only in plantation sector under G2G pact to eliminate brokers and reduce migration cost to less than Tk 40,000. But, since then only some 10,000 workers went there.

Malaysia termed it a failure of G2G though experts said certain quarters in the Malaysian government and agents made the G2G a failed programme.

In June last year, Malaysia declared it would recruit 1.5 million Bangladeshi workers through private sector. Initial plan was to recruit them in three years.

Malaysian trade unions and rights groups decried the announcement, arguing that the country was hosting over 2 million irregular migrants who needed to be regularised before making any fresh recruitment amid downturn of Malaysian economy.

The criticism became sharp when Malaysian media revealed that some private companies of the country, like Bestinet, Real Time Networking and Synerflux, had been lobbying Bangladesh and Malaysian governments to win contracts.

These companies were owned, directly or indirectly, by relatives of ministers. Of them, Synerflux was selected.

Lately, Baira and Bangladesh High Commission in Kuala Lumpur also warned that Malaysia's appointing Synerflux to regulate the labour recruitment would establish a monopoly.

HATIYA MOB BEATING

Death toll rises to four

The suspected robbery gang 'attacked police' before being beaten

OUR CORRESPONDENT, Noakhali

The death toll in Hatiya's mob beating of a suspected robber gang rose to four, after initial reports suggested three people died and three others were injured.

Early yesterday, police said they found three bodies on the spot and sent three injured to a hospital. Doctors there declared a fourth victim dead.

The dead are Akbar Siddiq, 28, of Joypurhat; Ashiqur Rahman, 27, and his younger brother Saiful Islam Sujon, 25, of Dinajpur; and Sunam, 25, of Chapainawabganj.

Two others -- Suman, 28, of Dinajpur and Abu Bakar, 35, of Chapainawabganj -- are being treated at Noakhali General Hospital, police said.

The incident happened at Chairman Ghat in Noakhali around 11:00pm on Friday, said Officer-in-charge Anisul Haque of Hatiya Police Station.

Quoting locals, police said a gang arrived at Chairman Ghat in a trawler.

Hatiya, surrounded by rivers, is no stranger to robbery.

When locals saw a group of strangers getting off from a boat at that hour, they grew suspicious and confronted them.

The six first introduced themselves as coast guards and then as police members.

The locals then called the police from a nearby police outpost.

At one point, the gang attacked the police members at the outpost and attempted to run away.

Three cops were injured in their attack, said the OC, adding that locals chased them down and beat them.

People also recovered some homemade sharp weapons from the trawler used by the robbery suspects, he added.

BB installing

FROM PAGE 1

surfaced whether the malware was installed through any BB official's computer.

Meanwhile, some officials have been opposing installation of the monitoring software on their PCs.

Speaking on condition of anonymity, a BB official said he is opposed to installing the new software without adequate scrutiny.

BB HIRES INFORMATIX

Soon after the heist, the central bank appointed World Informatics to improve its IT infrastructure. The firm has been hired for three years under a World Bank project, according to a BB official.

The appointment of the firm was under process, but it was expedited once the hacking came into light. The

central bank's board of directors approved the appointment last week.

The official said the company will have an additional responsibility to unearth the heist and ensure measures for future protection of the BB network.

The central bank had put "zero tolerance security" and robust firewalls in place in the back office of its foreign currency division. But the cyber gang used a powerful malware to break the firewall and managed to send fake payment orders to the US bank, added the official.

BB spokesperson Shubhankar Saha said Rakesh Asthana, founder of World Informatics, has been appointed as the IT governance specialist after the BB became convinced of his qualifications and vast work experience.

Upbeat Tigers

FROM PAGE 1

was rightly portrayed by former Sri Lankan batsman-turned commentator Russel Arnold when he said: "A curtailed-over match always brings in the risk-factor for the big teams."

Bangladesh are likely to field the same eleven against Oman that featured in their abandoned game against Ireland, where Mohammad Mithun came in for Nasir Hossain and Arafat Sunny paved the way for young left-arm pacer Abu Hider Rony.

Although the obvious question at the pre-match briefing was whether there was a chance for Mustafizur Rahman, now nursing a side strain, to play the final qualifier, Bangladesh's bowling coach Heath Streak, who attended the briefing, rejected the idea.

"No, not yet. We are still working on him. He has been in his rehab programme. We can't give any timeline. He might feel alright when he wakes up tomorrow [Sunday] but that is unlikely," said the former Zimbabwe all-rounder.

Asked how disappointing the persistent rain has been for the Tigers for the last couple of days, Streak said: "It has come down to the last game against Oman. Yes, the guys are up for it. It was good that we were able to bat for some time last night, it has been very positive for us. The guys have been upbeat and looking forward to tomorrow and hopefully the rain stays away."

He was also happy with Bangladesh's impressively growing pace battery.

"I think it all started when we went to Australia for the World Cup in 2015. We had to get our pace attack competitive if we had to compete there. That had made us work hard. We had to practice on what our abilities are. The effort and will to improve amongst the quick bowlers has been fantastic. The talent was always there, it was just a matter of getting them to do the right things," said a satisfied Streak.

When confronted with the question of Taskin Ahmed and Arafat Sunny being reported for their bowling actions, the Bangladesh bowling coach said that it was very disappointing.

"Taskin, Sunny and we are 100 per cent confident that they will be cleared. I have looked at the footage and there is no change in his [Taskin's] action. The coaching staff and few others have also looked into it and we believe he is fine. I am confident. I am not saying this just to support him, I honestly believe he is fine and he is going to play an important part for us in the World Cup," said a confident Streak.

Oman are a team Bangladesh have never played before. But Streak echoed Tigers captain Mashrafe Bin Mortaza's sentiment when he said that his team would play their own game instead of focusing on what the other team are doing.