Cyber thieves exploit banks' faith in SWIFT transfer network

REUTERS, *London/Chicago*

SHORTLY after 7pm on January 12, 2015, a message from a secure computer terminal at Banco del Austro (BDA) in Ecuador instructed San Francisco-based Wells Fargo to transfer money to bank accounts in Hong Kong.

Wells Fargo complied. Over 10 days, Wells approved a total of at least 12 transfers of BDA funds requested over the secure SWIFT system.

The SWIFT network - which allows banks to process billions of dollars in transfers each day - is considered the backbone of international banking. In all, Wells Fargo transferred $12 million of BDA's money to accounts across the globe.

Both banks now believe those funds were stolen by unidentified hackers, according to documents in a BDA lawsuit filed against Wells Fargo in New York this year.

BDA declined comment. Wells Fargo, which also initially declined comment on the lawsuit, said in a statement to Reuters on Friday that it "properly processed the wire instructions received via authenticated SWIFT messages" and was not responsible for BDA's losses.

BDA is suing Wells Fargo on the basis that the U.S. bank should have flagged the transactions as suspicious.

Wells Fargo has countered that security lapses in BDA's own operations caused the Ecuadorean bank's losses. Hackers had secured a BDA employee's SWIFT logon credentials, Wells Fargo said in a February court filing.

SWIFT, an acronym for the Society for Worldwide Interbank Financial Telecommunication, is not a party to the lawsuit.

Neither bank reported the theft to SWIFT, which said it first learned about the cyber attack from a Reuters inquiry.

"We were not aware," SWIFT said in a statement responding to Reuters inquiries. "We need to be informed by customers of such frauds if they relate to our products and services, so that we can inform and support the wider community. We have been in touch with the bank concerned to get more information, and are reminding customers of their obligations to share such information with us."

SWIFT says it requires customer to notify SWIFT of problems that can affect the "confidentiality, integrity, or availability of SWIFT service."

SWIFT, however, has no rule specifically requiring client banks to report hacking thefts. Banks often do not report such attacks out of concern they make the institution appear vulnerable, former SWIFT employees and cyber security experts told Reuters.

The Ecuador case illuminates a central problem with preventing such fraudulent transfers: Neither SWIFT nor its client banks have a full picture of the frequency or the details of cyber thefts made through the network, according to more than dozen former SWIFT executives, users and cyber security experts interviewed by Reuters.

The case - details of which have not been previously reported - raises new questions about the oversight of the SWIFT network and its communications with member banks about cyber thefts and risks. The network has faced intense scrutiny since cyber thieves stole $81 million in February from a Bangladesh central bank account at the Federal Reserve Bank of New York.

It's unclear what SWIFT tells its member banks when it does find out about cyber thefts, which are typically first discovered by the bank that has been defrauded. SWIFT spokeswoman Natasha de Terán said that the organization "was transparent with its users" but declined to elaborate. SWIFT declined to answer specific questions about its policies for disclosing breaches.

On Friday, following the publication of this Reuters story, SWIFT urged all of its users to notify the network of cyber attacks.

"It is essential that you share critical security information related to SWIFT with us," SWIFT said in a communication to users.

Reuters was unable to determine the number or frequency of cyber attacks involving the SWIFT system, or how often the banks report them to SWIFT officials.

The lack of disclosure may foster overconfidence in SWIFT network security by banks, which routinely approve transfer requests made through the messaging network without additional verification, former SWIFT employees and cyber security experts said.

The criminals behind such heists are exploiting banks' willingness to approve SWIFT requests at face value, rather than making additional manual or automated checks, said John Doyle, who held a variety of senior roles at SWIFT between 1980 and 2005.

"SWIFT doesn't replace prudent banking practice" he said, noting that banks should verify the authenticity of withdrawal or transfer requests, as they would for money transfers outside the SWIFT system.

SWIFT commits to checking the codes on messages sent into its system, to ensure the message has originated from a client's terminal, and to send it to the intended recipient quickly and securely, former SWIFT executives and cyber security experts said. But once cyber-thieves obtain legitimate codes and credentials, they said, SWIFT has no way of knowing they are not the true account holders.

The Bank for International Settlements, a trade body for central banks, said in a November report that increased information sharing on cyber attacks is crucial to helping financial institutions manage the risk.

"The more they share the better," said Leo Taddeo, chief security officer at Cryptzone and a former special agent in charge with the FBI's cyber crime division in New York.

SWIFT, a cooperative owned and governed by representatives of the banks it serves, was founded in 1973 and operates a secure messaging network that has been considered reliable for four decades. But recent attacks involving the Belgium-based cooperative have underscored how the network's central role in global finance also presents systemic risk.

SWIFT is not regulated, but a group of ten central banks from developed nations, led by the National Bank of Belgium, oversee the organization. Among its stated guidelines is a requirement to provide clients with enough information to enable them "to manage adequately the risks related to their use of SWIFT."

However, some former SWIFT employees said that the cooperative struggles to keep banks informed on risks of cyber fraud because of a lack of cooperation from the banks themselves. SWIFT's 25-member board of directors is filled with representatives of larger banks.

"The banks are not going to tell us too much," said Doyle, the former SWIFT executive. "They wouldn't like to destabilize confidence in their institution."

Banks also fear notifying SWIFT or law enforcement of security breaches because that could lead to regulatory investigations that highlight failures of risk management or compliance that could embarrass top managers, said Hugh Cumberland, a former SWIFT marketing executive who is now a senior associate with cyber security firm Post-Quantum.

Cases of unauthorised money transfers rarely become public, in part because disagreements are usually settled bilaterally or through arbitration, which is typically private, said Salvatore Scanio, a lawyer at Washington, D.C.-based Ludwig & Robinson. Scanio said he consulted on a dispute involving millions of dollars of stolen funds and the sending of fraudulent SWIFT messages similar to the BDA attack. He declined to name the parties or provide other details.

Theoretically, SWIFT could require its customers, mainly banks, to inform it of any attacks - given that no bank could risk the threat of exclusion from the network, said Lieven Lambrecht, the head of human resources at SWIFT for a year-and-a-half through May 2015.

But such a rule would require the agreement of its board, which is mainly made up of senior executives from the back office divisions of the largest western banks, who would be unlikely to approve such a policy, Lambrecht said.

This week, Vietnam's Tien Phong Bank said its SWIFT account, too, was used in an attempted hack last year. That effort failed, but it is another sign that cyber-criminals are increasingly targeting the messaging network.

In the Ecuadorean case, Wells Fargo denies any liability for the fraudulent transfers from BDA accounts. Wells Fargo said in court records that it did not verify the authenticity of the BDA transfer requests because they came through SWIFT, which Wells called "among the most widely used and secure" systems for money transfers.

BDA is seeking recovery of the money, plus interest. Wells Fargo is attempting to have the case thrown out.

New York-based Citibank also transferred $1.8 million in response to fraudulent requests made through BDA's SWIFT terminal, according to the BDA lawsuit against Wells Fargo.

Citibank repaid the $1.8 million to BDA, according to a BDA court filing in April. Citibank declined to comment.

For its part, Wells Fargo refunded to BDA $958,700 out of the $1,486,230 it transferred to an account in the name of a Jose Mariano Castillo at Wells Fargo in Los Angeles, according to the lawsuit. Reuters could not locate Castillo or verify his existence.

The BDA-Wells Fargo case is unusual in that one bank took its correspondent bank to court, thus making the details public, said Scanio, the Washington attorney. BDA acknowledged in a January court filing that it took more than a week after the first fraudulent transfer request for BDA to discover the missing money.

After obtaining a BDA employee's SWIFT logon, the thieves then fished out previously canceled or rejected payment requests that remained in BDA's SWIFT outbox.

They then altered the amounts and destinations on the transfer requests and reissued them, both banks said in filings.

While Wells Fargo has claimed in court filings that failures of security at BDA are to blame for the breach, BDA has alleged that Wells could easily have spotted and rejected the unusual transfers. BDA noted that the payment requests were made outside of its normal business hours and involved unusually large amounts.

The BDA theft and others underscore the need for banks on both sides of such transactions - often for massive sums - to rely less on SWIFT for security and strengthen their own verification protocols, Cumberland said.

"This image of the SWIFT network and the surrounding ecosystem being secure and impenetrable has encouraged complacency," he said.

Preparation of banks in implementing Basel III

PRASHANTA K BANERJEE

AS part of a consistent journey to enhance the loss absorption capacity and resilience of the banks through increasing the capital and improving the quality thereof, Bangladesh Bank has given directions to banks to implement Basel III from January 01, 2015 in phases and fully by January 01, 2019. As Basel III framework was basically the response of the global banking regulators to deal with the factors, more specifically those relating to the banking system that led to the global economic crisis or the great recession, Basel III provides improved risk management systems in banks. By practising these risk management systems, banks therefore are expected to be more shock absorbent in future.

Any change, big or small, of whatever nature brings some challenges. So it is expected that Bangladeshi banks will face several challenges to implement Basel III. But we are convinced that challenges are not onerous and these are worth facing up to. The first and foremost challenge is to maintain the increased amount of capital. As per the guidelines of Bangladesh Bank, banks maintained 10 percent of risk-weighted asset in 2015, but gradually it will go up and finally banks will maintain 12.50 percent in 2019 when full implementation of capital ratios will be executed. Besides, banks need to maintain leverage ratio of 3 percent based on amount of Tier-I capital as percentage to total exposure of banks. Seemingly, private commercial banks (PCBs) are capable of increasing these percentages comfortably. However, the recent deterioration of asset quality of state-owned commercial banks (SCBS) and some PCBs has created uncertainty about their capacity to generate capital internally. In this perspective, banks can initiate to amplify their internal ability for generating capital through reducing costs, ensuring quality of loans and forming loan portfolio contemplating the risk weights fixed by Bangladesh Bank. In case of necessity of adding capital from external sources, the government may follow traditional trajectory through injecting new capital to SCBs for ensuring sufficient amount of capital. PCBs may also go for issuing seasoned issues for extra amount of capital from external sources. Additionally, banks can raise the amount of capital by offloading a certain percentage of shares, inviting organisations like International Finance Corporation (IFC), and Islamic Corporation for the Development of the Private Sector (ICD) for participation in banks' capital and issuing different debt securities.

Fiscal and monetary authority can motivate banks for utilising these innovative options for the enhancement of capital through giving necessary policy supports. It is well accepted that the government may not inject capital to SCBs for unlimited period from the taxpayers' money. Banks, therefore, need to enhance their internal capacity to increase necessary amount of capital for covering risk exposure they undertake.

In case of liquidity framework, Liquidity Coverage Ratio (LCR) and Net Stable Funding Ratio (NSFR) are actually framed as liquidity performance parameters. Through these ratios, banks can visualise well ahead of incurring liquidity problems and take necessary steps to address this problem without the help of the central bank. It is anticipated that banks of Bangladesh will not face major challenges in maintaining both ratios. Bangladesh Bank has already observed ability of banks in maintaining ratios on a trial basis almost for one year and found all banks with a few exceptions are capable to maintain these parameters.

A few other factors like technology, skills development and governance are being considered as challenges in implementing Basel III. The revised approaches for using risk-weighted assets will be dependent on a number of computational requirements. Banks may need to upgrade their systems and processes to be able to compute an amount of risk-weighted assets as well as capital requirements based on revised guidelines. Apart from technological upgradation, higher specialised skills development in the supervised banks and within Bangladesh Bank is a challenge to ensure proper implementation of Basel III. Top management and human resource development policy of banks, thus, need to get tuned with this requirement. The central bank also needs to hone skills in regulating and supervising under the new system.

The Basel Committee on Banking Supervision added a separate principle on corporate governance in its core principles in 2012. It is welcomed in Bangladesh in the sense that while strong capital gives financial strength, it cannot assure good performance unless good corporate governance exists. We need to fix and ensure this issue for the interest of having a strong financial sector like global community. We believe that banks of Bangladesh have the capacity to address these challenges for the full implementation of Basel III. If any lacking does exist, it is expected that banks will take required initiatives to bridge the gap.

The writer is a professor of banking and finance and director (research, development & consultancy) of Bangladesh Institute of Bank Management.

As populations swell and water becomes scarce, food prices could double

REUTERS, *London*

SWELLING populations and demand for food combined with ever scarcer water and land resources could lead to a doubling of food prices and trigger civil unrest in some developing countries, a new report says.

Demand for food with a higher environmental impact, such as meat, has surged as emerging countries like China and India grow in size and in wealth, said Martin Halle, policy analyst at Global Footprint Network (GFN).

"A few things are very clear: the demand for food is going up tremendously because of population growth," he told the Thomson Reuters Foundation.

"[Food production] is becoming more unstable because climate change is affecting production, in the context of growing land and water scarcity. There's very little leeway between supply and demand."

In the past, countries were able to meet those demands by growing more food on more land. But this has come at a cost, Halle said, since the planet is now running out of water and arable land.

The last time the world saw a severe food crisis was in 2007 and 2008, the report said, when extreme weather events hit major grain producing regions the year earlier, causing spikes in the demand and cost of food.

The higher prices led to social and political unrest in North Africa, the Middle East and South East and South Asia.

The report published this week by GFN and the United Nations Environment Programme (UNEP)said most of the same countries, namely Morocco, Bangladesh, Tunisia and Indonesia, are again at risk if food prices were to increase in the next few years.

Climate change and extreme weather patterns will further increase volatility in food production, Halle added, meaning food prices will become more unstable in the coming years.

"The real game-changer comes when you factor in the environmental constraints - climate change, land scarcity and water scarcity, and all of these are linked," said Halle.

Drought is becoming more frequent and severe in places like southern Africa, and that -- combined with the recent El Nino phenomenon -- is taking a heavy toll on rural lives and economies.

For example, maize prices in South Africa, the continent's top producer of the staple crop, reached near record highs late 2015, in the face of rolling heat waves and poor rains over key growing areas.

Using models from data across 110 countries, the study found that if the cost of food doubled, household spending would increase by more than 10 percent in 37 countries.

Five African countries -- Benin, Nigeria, Ivory Coast, Senegal and Ghana -- would be the worst affected in terms of highest percentage loss to GDP.

The major emerging economies of China and India are forecast to lose $161 billion and $49 billion in gross domestic product (GDP) respectively with a doubling of food commodity prices.

"What this provides is a litmus test," said Ivo Mulder, economics advisor at UNEP. "We are overusing what is available for us and we don't really know what the magnitude of the risk is."