Special Report: Cyber thieves exploit banks' faith in SWIFT transfer network

reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD

Tom Bergin, Nathan Layne

Banks
Updated

By Tom Bergin, Nathan Layne

11 Min Read

LONDON/CHICAGO (Reuters) - Shortly after 7 p.m. 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.

The SWIFT logo is pictured in this photo illustration taken April 26, 2016. REUTERS/Carlo Allegri/Illustration/File Photo

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.

SYSTEMIC RISK

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 unauthorized 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.

FIGHT OVER LIABILITY

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.

ANATOMY OF A CYBER HEIST

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.

Additional reporting by Jim Finkle in Boston and Alexandra Valencia in Quito; Editing by David Greising and Brian Thevenot

Our Standards: The Thomson Reuters Trust Principles.

for-phone-onlyfor-tablet-portrait-upfor-tablet-landscape-upfor-desktop-upfor-wide-desktop-up