SWIFT Hack Leaves Little Room For Banks To Feign Ignorance

By Allison Grande
May 17, 2016

Law360, New York (May 17, 2016, 9:50 PM ET) -- The Society for Worldwide Interbank Financial Telecommunication recently alerted its members about a malware attack that hit at least two banks that use its platform to exchange secure messages, a warning that financial institutions would be wise to seize on to quickly shore up their defenses in order to reduce their chances of drawing the ire of both customers and regulators.

In **a notice sent to** its more than 11,000 members on Friday, SWIFT acknowledged that it had identified at least two instances in which unknown assailants first obtained valid operator credentials that they used to submit fraudulent messages requesting money transfers and other services through the SWIFT network, and then moved to cover up their misconduct by tampering with the confirmations that banks rely on to spot suspicious activity.

SWIFT warned its members that the attackers — who the platform hypothesized could have been either malicious insiders or external bad actors — appeared to have "deep and sophisticated knowledge of specific operational controls within the targeted banks," and offered several recommendations for how to improve cybersecurity controls that attorneys say platform members and other financial institutions can't afford to ignore.

"Even though it appears that this threat has been identified, it is notices like these that will be used against financial institutions when a breach occurs, resulting in a large-scale loss," said Craig Nazzaro, a member of Baker Donelson Bearman Caldwell & Berkowitz PC's consumer finance litigation and compliance group. "The actions you take today should showcase your institution was doing everything possible to provide the most up-to-date protection in this space."

By failing to take reasonable and immediate action to ensure that cybersecurity protections are up-to-date and able to guard against an attack like the one that SWIFT has described, financial institutions around the world run the risk of facing significant legal risk if they find themselves to be the next target of the attackers, especially if the incident results in a concrete injury, such as customers losing access to their funds for any amount of time, experts say.

"The financial institutions' customers will use previous warnings, such as this one from SWIFT, to show that a bank was on notice as to the risks and potential liability," Nazzaro said. "In the event of a breach, you need to be able to showcase the steps you have taken to protect your customers' data, their funds and your institution's overall safety and soundness in order to limit any liability you may face."

Companies that don't act may also be at an increased risk of being unable to secure the cyberinsurance coverage they need and of drawing attention from financial regulators around the world, according to attorneys.

"The situation where regulators would get involved is if there is a known vulnerability that the institution clearly had notice of but failed to act," White & Case LLP partner Kevin Petrasic said. "In that case, you could see enforcement actions."

Besides putting into place controls such as firewalls and enhanced employee training, SWIFT also advised its customers to "be forthcoming when these issues occur" so that the fraudsters can be tracked by the authorities and the platform can alert its other members of the risk, a step that could help to further reduce potential liability down the line, according to experts.

"Fast and complete notification is not only good public relations and helpful to reduce client losses, it naturally helps minimize bank liability for those losses," said Shaun G. Jamison, professor of law and assistant dean of information services at Concord Law School of Kaplan University.

While SWIFT made it clear that the banks are ultimately responsible for their own security and that it was confident that its own network, core messaging services and software had not been breached, it's not necessarily a given that the global financial messaging network will escape unscathed, attorneys say.

One possible way that SWIFT could be saddled with some of the liability is if the platform failed to give member banks any guidance about how to safely and securely install and use the network, experts say.

Although SWIFT's alert didn't identify the banks hit by the recent attacks, security researchers have reported that one of the attacks led to the theft in February of $81 million from the Bangladesh central bank, which was found not to have any firewall in place between the SWIFT network and the Internet at large, leaving hackers with easy access to the financial messaging platform.

"The only way that I feel the SWIFT system could be held to some degree of accountability is if they did not issue a proper installation procedure," said David King, senior manager of internal audit, risk and compliance at UHY Advisors Inc. "If SWIFT just went to the Bangladeshi bank and said, 'Thanks for signing onto our product, here's the software, go ahead and install it and don't worry about controls because we believe our system is secure,' if they had offered those type of promises and made no recommendations on how to install it — which there's no indication that they did — then that could trigger culpability."

Even if SWIFT doesn't face any exposure for the security breaches, the incidents should still push the platform to rethink what it requires from its customers in terms of security, experts say.

"It's surprising that there is no baseline level of security that SWIFT appears to require from banks," said David Ray, director of information governance at Consilio LLC. "While most laws are fairly vague when it comes to security, since security is such a rapidly moving target, SWIFT should at least have a responsibility to include stronger language about security standards in their contracts with banks that want to be part of the network."

While the international nature of the platform may make it difficult to come up with a security standard that could be widely applicable, experts were quick to note that there is some precedent for such a move. King specifically pointed to the payment card industry data security standard, or PCI DSS, which card-issuing companies that operate globally require merchants to follow if they want to accept their cards.

"It makes sense for there to be a threshold that participating banks need to meet before implementing the system and to be certified about their compliance on an annual basis moving forward," King said.

SWIFT would also be wise to rethink what some described as an outdated security system, according to experts.

"The SWIFT security architecture is based upon a cybercriminal threat of 2002 wherein firewalls and encryption were sufficient security controls to mitigate fraud," said Tom Kellermann, the CEO of Strategic Cyber Ventures LLC. "Today's cybercriminal is dramatically more sophisticated and organized than her 2002 counterpart. SWIFT and the financial institutions must alter their security architecture away from the castle-like construct of yesteryear and more towards a supermax prison environment wherein an adversary's intrusion is suppressed and diverted."

While the cyberattack detailed by SWIFT included elements that are combination of methods that have been seen in previous incidents — namely, the theft of security credentials to gain access to the system and the use of social engineering to manipulate records that the banks receive — the combination of the two were notable and should serve as a warning to both financial institutions.

"Since SWIFT itself may be too hard to crack, attackers are preying on the access points to steal credentials and abuse them," said A.N. Ananth, a co-founder of EventTracker.

Although SWIFT and others have characterized the attack as sophisticated, some experts contend the level of sophistication was not especially high. Instead, the attackers demonstrated a level of discipline that financial institutions should look to counter with a return to the basics.

"The more you get to know what the bad activity looks like, the more you can know what the good activity looks like," said Jeremy Wheeler, a senior architect of Alpine Cyber Solutions. "Security is not entirely a technical thing — it's also important to have a general know-how about how traditional banking works to be able to catch changes to that model."

Beyond taking basic steps such as strengthening monitoring and access controls, banks can also take more advanced steps to boost their defenses, such as engaging outside information security vendors and instituting a blockchain-based system that is more opened and decentralized.

"A blockchain-based system would have made it much more difficult, if not impossible, to pull off the theft without detection," Steptoe & Johnson LLPpartner Jason Weinstein said, noting that such a system would have likely blocked hackers both from getting into the SWIFT system to remove records of the transfers and to manipulate account balances to avoid detection, "kind of like how the thieves in 'Ocean's 11' hacked into the security cameras so they showed a vault full of money at the same time the vault was being emptied."

Whatever measures banks elect to implement, experts agree that inaction is not an option, and that the SWIFT announcement should at the very least serve as a glaring reminder that no system is secure and that even the most robust protections can be breached.

"This story shows that even banks and financial institutions known to be equipped by the most advanced security measures are once again blowing up the myth of having nonpenetrable systems," said

David Melamed, a senior research engineer at CloudLock. "There is unfortunately no online fortress that cannot be breached."