CLCT

WILLIAM & MARY LAW SCHOOL

Cybersecurity and Information Security Newsletter

Issue 10 | September 14, 2021

Table of Contents

- TD Bank sued by customer for failure to protect against online theft
- Senator Warner introduced legislation to bolster cyber breach notification

Please feel free to submit cybersecurity and information security news items or request related topics to Daniel Shin (dshin01@wm.edu).

TD Bank sued by a customer for failure to protect against online theft

On August 10, 2021, Moore Capital Holdings LLC (Moore Capital) filed a lawsuit against TD Bank, NA, (TD Bank) for its "total and systemic failure to respond" against a cyber fraud scheme that led to a fraudulent wire transfer of almost $300,000. *Case 1:21-cv-15029 Complaint*, available here. The case is at a preliminary stage at the time of publication, and TD Bank has yet to respond to Moore Capital's allegation. *1:21cv15029, Moore Capital Holdings Llc V. Td Bank, N.A. (LexisNexis)*, available here.

Background according to Moore Capital

Moore Capital is a private equity company based in Bryn Mawr, Pennsylvania, which specializes in the acquisition and management of industrial and commercial real estate properties. *Business customer sues TD Bank after losing almost $300,000 in a cyber crime*, available here. Moore Capital is a customer of TD Bank, one of the 10 largest banks in the U.S., and a subsidiary of The Toronto-Dominion Bank of Toronto, Canada. *Company Fact Sheet*, available here.

Moore Capital was a victim of an evolved type of business email compromise (BEC) attack. A BEC attack involves threat actors inducing victims to wire money by presenting a fraudulent email from other persons—who are usually in a position of control or seniority to the person receiving the email—that appears to be legitimate. *Business Email Compromise (Federal Bureau of Investigation)*, available here. Unlike the traditional BEC attack, the attack vector (a mechanism used to exploit a cybersecurity or information security vulnerability) was a fraudulent website that appeared to be a legitimate but fake TD Bank's website.

On April 29, 2021, one of Moore Capital's employees attempted to access TD Bank's online platform to create a new account. *Case 1:21-cv-15029 Complaint*, *supra* at 7. Instead of connecting to TD Bank's official banking website, the web browser redirected the employee to a fake but identical-looking webpage that has a similar-looking URL address. Not knowing that the website was fake, the employee entered his credentials for the new account and the fake webpage prompted him to enter his phone number.

Subsequently, the employee received a phone call with a caller identification "TD Bank," where the caller identified himself as a TD Bank employee. The alleged TD Bank employee stated that an existing TD Bank account user needed to log in to authenticate the employee's credentials, so a second employee entered his information on the fake webpage. The alleged TD Bank employee and the fake webpage said that the first employee's account would be activated within 15 minutes.

Shortly thereafter, there was an internet connection problem at Moore Capital's office. At the same time, Moore Capital's principal, Zachary Moore (Moore), received a wire transfer alert on his phone, stating that a wire transfer of $90,650.00 had been initiated from the firm's account to a previously unknown account. A few minutes later, Moore received another wire transfer alert of $94,150.00 from the firm's account to another previously unknown account.

Both transfer alerts noted that TD Bank customers could contact the bank via the nearest branch or the published phone number if they had any questions. Moore knew immediately that the wire transfers were fraudulent and called TD Bank using the published number on the wire alerts. Unfortunately, the published number was a general services line that connected

him to an automated answering system. Moore hung up the phone and called a local TD Bank branch, where he reported the fraud incident. He asked to speak with the branch assistant manager, but the branch representative told him that she was unavailable. The branch representative reassured Moore that the fraud would be reported immediately internally.

Ten minutes later, Moore received a third wire alert with a transfer of $91,450.00 to a third unknown account. He immediately called the branch again to alert them to the third fraudulent wire transfer. Asking "the branch representative how a third wire could have been transmitted ten minutes ***after*** Moore had reported the fraud in exactly the manner instructed by TD Bank in the Wire Alerts . . . [t]he branch representative stated that he had no idea." *Case 1:21-cv-15029 Complaint*, *supra* at 9 (emphasis in original).

Later in the day, Moore received a call from the branch assistant manager that "she reported the fraud internally and had finally frozen [Moore Capital's] account (20 minutes after Moore reported the fraud incident)." *Id.*, *supra* 10. The branch assistant manager "unequivocally stated that TD Bank would reimburse [Moore Capital] for any loss of the Wired Funds if, following TD Bank's fraud response, the funds could not be recovered." *Id.* Moore was later told by a TD Bank employee that "all three wires had been 'immediately' recalled" as soon as he had reported them.

Despite TD Bank's continued reassurances, Moore was unable to get key details on the progress of the fraud investigations, including whom at TD Bank was assigned to the fraud investigation. He later found out that TD Bank did not immediately initiate wire recalls. Based on the advice of Moore Capital's counsel, Moore filed an IC3 complaint with the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3). He also contacted the receiving banks of the fraudulent wire funds to initially monitor the situation and later attempt to stop the transfers.

Based on Moore Capital's complaint, TD Bank ultimately failed multiple times to inform Moore of any significant progress on the fraud investigation. Based on contacts from the Federal Bureau of Investigation, the firm learned that TD Bank commonly fails to work with law enforcement on fraud incident matters, "with the bank typically refusing to either provide information to the FBI or obtain information from the agency in furtherance of its own incident response." *Id.* at 18.

At the time of publication, Moore Capital alleges that no fraud investigator from TD Bank contacted the firm, and the firm has not been able to recover the lost wire funds. As such, Moore Capital alleges that TD Bank, among others, was negligent for (1) failing to have any fraud incident response plan in place, (2) failing to train its employees to investigate and respond to fraud reports, (3) failing to initiate wire recalls promptly, (4) failing to take steps to freeze wired funds on receiving banks, and (5) failing to work with law enforcement agencies in response to fraud incidents. (Note, these are a summary of the charges.) The firm notes that TD Bank made prior representations in its marketing literature that "it has a duty to attempt to minimize fraud related losses after one of its customers reports being the victim of wire transfer or payment fraud." *Id.* at 19.

Analysis

The law of negligence deals with cases involving a party's "failure to behave with the level of care that someone of ordinary prudence would have exercised under the same circumstances." *Negligence (Legal Information Institute)*, available here. To advance a negligence claim in torts, the plaintiff (the party bringing the claim) needs to establish that (1) the defendant—the party being sued—owed a legal duty to the plaintiff; (2) the defendant breached that duty; (3) the plaintiff suffered an injury; and (4) there is proof that the defendant's breach caused the injury to the plaintiff.

It should be noted that TD Bank has not yet responded to Moore Capital's claims, including the background information of the alleged failure of fraud prevention. Although there is a possibility that the lawsuit may proceed as is, this newsletter cautions the audience that the case may also be dismissed due to other legal issues.

Nevertheless, Moore Capital's allegations are noteworthy because the firm is attempting to use the tort law of negligence to hold TD Bank accountable with respect to the fraud incident response, which is unusual in the area of cybercrime and fraud incident response. Moore Capital has the burden of establishing that TD Bank's conduct over the course of the fraud incident response fell below the standards that a reasonable bank would have. If Moore Capital is successful with some of its claims, this case may set the much-needed standard for holding parties accountable for not executing proper incident responses in situations where those services were relied upon.

Senator Warner introduced legislation to bolster cyber breach notification

On July 21, 2021, U.S. Senator Mark Warner of Virginia introduced the *Cyber Incident Notification Act of 2021* (CINA), which mandates cyber breach notifications by federal agencies, federal contractors, and critical infrastructure operators to the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS). The Senate bill designates CISA as the agency "to receive cybersecurity notifications from other Federal agencies and covered entities." *S.2407 - Cyber Incident Notification Act of 2021*, available here.

The introduction of CINA comes as President Biden recently met with the private sector and education leaders to bolster cybersecurity partnerships among industry and other entities. *FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity (White House)*, available here.

CINA Summary

Aiming to increase the visibility of the cyber intrusion landscape at a national level, the bill develops a cyber threat information sharing system (Cyber Intrusion Reporting Capabilities) managed by CISA that would cover government and relevant private sector entities.

CINA requires federal agencies and covered entities to submit a cybersecurity intrusion notification to CISA within 24 hours after confirming a cybersecurity intrusion or a potential

cybersecurity intrusion incident. Covered entities include federal contractors, owners or operators of critical infrastructure, and nongovernmental entities that provide cybersecurity incident response services. After receiving a cybersecurity intrusion notification, the Director of CISA is required to respond to the reporting entity within two business days.

Critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety." 42 USC § 5195c, available here. The Director of CISA is tasked to determine which critical infrastructure is covered under CINA's mandatory cyber intrusion reporting requirements "based on assessment of risks posed by compromise of critical infrastructure operation." *S.2407 - Cyber Incident Notification Act of 2021, (d) Required Rulemaking*, available here.

CINA provides an enforcement mechanism to the Director of CISA if federal agencies and other covered entities fail to adhere to the mandatory breach notification requirements. *S.2407 - Cyber Incident Notification Act of 2021, (h) Enforcement*, available here. Under this bill, the Director is empowered to levy monetary penalties against covered entities that have violated or are in the process of violating the reporting requirements. If a federal agency is found to be in violation, the incident is referred to the agency's inspector general "as a matter of urgent concern."

This bill also provides limited legal immunity for covered entities against lawsuits arising from submitting cyber breach notifications to CISA. *S.2407 - Cyber Incident Notification Act of 2021, (g) Protection From Liability*, available here.

Currently, the Senate bill has 14 cosponsors, with a large number of Senators from the Senate Select Committee on Intelligence, chaired by Senator Warner. *See Committee Membership List*, available here.

Analysis

Citing cybersecurity incidents ranging from the SolarWinds to the Colonial Pipeline attacks, Senator Warner noted that "there is currently no federal requirement that individual companies disclose when they have [been] breached." *Following SolarWinds & Colonial Hacks, Leading National Security Senators Introduce Bipartisan Cyber Reporting Bill*, available here. Although there is no federal law *explicitly* mandating cyber breach notification from private entities, on February 21, 2018, the U.S. Securities and Exchange Commission (SEC) published interpretative guidance that requires all publicly traded companies to make timely disclosures of cybersecurity incidents through existing SEC reporting requirements. *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, 17 CFR Parts 229 and 249, available here. *See Issue 3 of our newsletter: Carnival reported ransomware attack and data breach in SEC filing*, available here.

If passed, CINA would provide a much-needed cybersecurity breach notification requirement for both private and *federal* entities, facilitating federal cyber response and potentially limiting collateral damage from cyber attacks.

Mandating cybersecurity breach notification complements the soft governance approach of encouraging private and nongovernmental entities to create a self-regulatory framework to enhance the nationwide cybersecurity landscape. When the White House collaborated with

the private sector and education leaders to announce multiple cybersecurity initiatives, the federal government signaled its openness to invite other key stakeholders to strengthen the nation's cybersecurity resiliency.

At the same time, the SolarWinds and the Colonial Pipeline attacks highlighted the pressing need of protecting federal cyber systems and the nation's critical infrastructure. If passed, CINA would create a leveled breach notification requirement for federal and covered entities while giving room for private and nongovernmental sectors to manage their self-regulatory cybersecurity framework.