How to hack other mobile

Continue

Twitter Investigation Report On July 15, 2020, a 17-year old hacker and his accomplices breached Twitter's network and seized control of dozens of Twitter accounts assigned to high-profile users. For several hours, the world watched while the Hackers carried out a public cyberattack, by seizing one high-profile account after another and tweeting out a "double your bitcoin" scam. The Hackers took over the Twitter accounts of politicians, celebrities, and entrepreneurs, including Barack Obama, Kim Kardashian West, Jeff Bezos, and Elon Musk, as well as Twitter accounts of several cryptocurrency companies regulated by the New York State Department of Financial Services. And for several hours Twitter seemed unable to stop the hack. In monetary value, the Hackers stole over $118,000 worth of bitcoin. But more significantly, this incident exposed the vulnerability of a global social media platform with over 330 million total monthly active users and over 186 million daily active users, including over 36 million (20%) in the United States.[1] In short, Twitter plays a central role in how we communicate and how news is spread. More than half of U.S. adults get their news from social media "often" or "sometimes."[2] Given that Twitter is a publicly traded, $37 billion technology company, it was surprising how easily the Hackers were able to penetrate Twitter's network and gain access to internal tools allowing them to take over any Twitter user's account. Indeed, the Hackers used basic techniques more akin to those of a traditional scam artist: phone calls where they pretended to be from Twitter's Information Technology department. The extraordinary access the Hackers obtained with this simple technique underscores Twitter's cybersecurity vulnerability and the potential for devastating consequences. Notably, the Twitter Hack did not involve any of the high-tech or sophisticated techniques often used in cyberattacks – no malware, no exploits, and no backdoors. The implications of the Twitter Hack extend far beyond this garden-variety fraud. There are well-documented examples of social media being used to manipulate markets and interfere with elections, often with the simple use of a single compromised account or a group of fake accounts.[3] In the hands of a dangerous adversary, the same access obtained by the Hackers–the ability to take control of any Twitter users' account–could cause even greater harm. The Twitter Hack demonstrates the need for strong cybersecurity to curb the potential weaponization of major social media companies. But our public institutions have not caught up to the new challenges posed by social media. While policymakers focus on antitrust and content moderation problems with large social media companies, their cybersecurity is also critical. In other industries that are deemed critical infrastructure, such as telecommunications, utilities, and finance, we have established regulators and regulations to ensure that the public interest is protected. With respect to cybersecurity, that is what is needed for large, systemically important social media companies. This Report reviews the facts surrounding the Twitter Hack, the reasons why it occurred, and what could be done to prevent future incidents. The Report also recommends steps for improved cybersecurity oversight of large social media companies. Part II of this Report describes background information about Twitter's platform, the ever-expanding influence of social media platforms such as Twitter, and how this influence continues to affect markets and the national conversation around elections and disinformation. It also describes the Department's role in protecting consumers and the financial services industry. Part III sets forth a detailed timeline of the Twitter Hack. This includes a description of key events and Twitter's response. Part IV details the Twitter Hack's impact on the Department's cryptocurrency licensees and their timely efforts to protect their customers from the fraud. It also describes the substantial threat cryptocurrency fraud poses to the industry. Part V addresses the cybersecurity weaknesses at Twitter that made the Twitter Hack possible. This includes a lack of leadership, vulnerability to social engineering, and a failure to address the new vulnerabilities caused by the pandemic-driven shift to mass remote working. Part VI identifies best practices that address the weaknesses the Twitter Hack exposed. The Report recommends specific steps cryptocurrency companies can take to combat similar fraud. The Department also recommends cybersecurity measures that will reduce the likelihood that a similar cyberattack will succeed. Part VII makes recommendations for improving our society's defenses against cybersecurity lapses that can lead to social media manipulation. It addresses the need for a regulation and a regulator focused on large social media companies' cybersecurity resiliency. [1] J. Clement, Twitter: Number of Monthly Active Users 2010-2019, Statista (Aug. 14, 2019), (noting that in early 2019, Twitter averaged over 330 million total monthly active users); Twitter, Inc., Q2 2020 Letter to Shareholders (July 23, 2020), (stating that Twitter averaged over 186 million daily active users, of which 36 million (nearly 20%) were in the United States). [3] See Section II.C, infra. Governor Andrew M. Cuomo and the New York State Legislature created the Department in 2011 as the merger of the former Banking and Insurance Departments, and widened the Department's purview to include "the regulation of new financial services products,"[4] by establishing "a modern system of regulation, rulemaking and adjudication" responsive to the needs of the banking and insurance industries and New York consumers and residents.[5] As part of its mission, the Department protects New York consumers and businesses against fraud and cybersecurity threats in connection with financial products and services, including those related to cryptocurrency. The Department has instituted critical cybersecurity standards for global financial institutions that are models for regulators worldwide. In 2016, the Department launched its first-in-the-nation cybersecurity regulation that requires all DFS-regulated financial institutions to implement a risk-based cybersecurity program and to report any attempted or executed unauthorized access to their information systems.[6] The regulation has served as a model for other regulators, including the U.S. Federal Trade Commission ("FTC"), multiple states, and the National Association of Insurance Commissioners ("NAIC"). In 2017, DFS advised the NAIC on its Data Security Model Law, which is based on DFS's cybersecurity regulation. Eleven states have adopted the Model Law and the U.S. Treasury Department has urged all states to adopt the model as soon as possible.[7] In 2019, the FTC proposed amendments to its Safeguards Rule under the Gramm-Leach-Bliley Act to include more detailed data security requirements that were expressly based on DFS's regulation.[8] The Conference of State Bank Supervisors has proposed a Nonbank Model Data Security Law that is also based expressly on DFS's cybersecurity regulation.[9] Under the leadership of Superintendent Linda A. Lacewell, the Department in 2019 became the first state or federal financial regulator in the nation to create a Cybersecurity Division to protect consumers and industries from cyber threats. DFS recruited Justin Herring, the former chief of the Cybercrimes Unit at the U.S. Attorney's Office for the District of New Jersey, to lead the Cybersecurity Division. As the Superintendent has repeatedly stated, cybersecurity is the biggest threat to industry and government, bar none. The Department is also committed to providing safe, stable, and open markets to those involved in virtual currency business activity ("VCBA"). In 2015, New York promulgated its pioneering virtual currency regulation to define VCBA and set forth the licensing and supervisory schemes.[10] To date, the Department has authorized over two dozen entities to conduct VCBA in New York and with New Yorkers. The DFS license is seen as the gold standard for cryptocurrency companies and is frequently included in the companies' marketing materials as a sign of credibility with proposed counterparties, investors and customers. Superintendent Lacewell also formed the Department's Research & Innovation Division in 2019 to advance New York's position as a global hub of financial innovation, including fintech, insurtech, and cryptocurrency. Led by Matthew Homer, the Division works to ensure that New Yorkers have safe access to the cryptocurrency marketplace and that New York remains at the center of technological innovation with forward-looking regulation. Consistent with its leadership in protecting New Yorkers, the Department is an integral part of the New York State Cybersecurity Advisory Board. Since 2013, the Department's Superintendents have co-led the Advisory Board with the Governor's Homeland Security policy lead. The Board, comprised of experts, advises the Governor's administration on developments in cybersecurity and recommends protections for New York State's critical infrastructure and information systems, including election security and operations. The Twitter Platform Since approximately July 2006, Twitter has operated www.twitter.com, a social networking and micro-blogging website that enables users to send "tweets"–brief updates of 280 (previously 140) characters or less–to their "followers" (i.e., users who sign up to receive such updates) via email and text. Twitter users (either via the website or mobile application) can follow other individuals, as well as commercial, media, governmental, or nonprofit entities.[11] Twitter users can also send and receive direct, non-public messages ("DMs").[12] Twitter maintains internal account management tools to manage a broad range of issues relating to Twitter user accounts. Twitter issues authorized employees a username and password to access the internal account management tools. A screenshot posted on Twitter on July 15 showed an internal tool the Hackers accessed:[13] Some of the internal tools include nonpublic information about each Twitter user account, including the account's associated email address, phone number, and the Internet Protocol ("IP") address for the user's login location. In response to user requests, authorized Twitter employees use the internal tools, in part, to update email addresses, reset forgotten or expired passwords, or enable or disable multifactor authentication ("MFA"), an extra layer of security requiring an auto-generated code to access an account. Twitter employees also use the internal tools to block or limit distribution of content of specific tweets or from user accounts. Such limitations can be imposed either in response to requests from countries that prohibit content that violates local law, or to enforce violations of the Twitter Rules governing user conduct.[14] Social Media's Power in Our Modern Society Twitter and other large social media companies are popular, and often provide valuable services. Using Twitter, consumers can receive updates from friends and acquaintances, breaking news from media outlets, or public safety and emergency updates from government authorities. In many instances, tweets invite users to click on links to other websites, including websites that consumers may use to obtain commercial products or services. The Twitter Hack also highlights the risk associated with social media platforms such as Twitter. As described below, it was jarringly easy for a teenager and his young associates to hack Twitter and hijack accounts belonging to some of the most prominent people and organizations in the world. The Hackers focused on classic fraud. But such a hack, when perpetrated by well-resourced adversaries, could wreak far greater damage by manipulating public perception about markets, elections, and more. In recent years, Twitter and other social media platforms have been used to influence financial markets, with devastating effects. For example, in 2013, the S&P 500 lost $136.5 billion of value minutes after hackers took over the Associated Press's Twitter account and falsely tweeted that two explosions at the White House harmed President Obama.[15] Financial criminals use social media in "pump-and-dump" schemes to temporarily inflate the price of stocks through false or misleading tweets; when they sell their shares and stop promoting the stock, the resulting plunge in shares' value harms unsuspecting investors.[16] Multiple studies show that tweets influence trading volume and future market activity whether their content is true or false.[17] Social media can also disrupt elections and public institutions. In July 2020, the office of the Director of National Intelligence announced that foreign nations–primarily China, Russia and Iran–were attempting to interfere with democratic processes, using influence measures in social and traditional media.[18] This is consistent with a recent Senate intelligence report, which found that Russian online influence operations during the 2016 elections were designed to undermine faith in democratic institutions and provoke social discord.[19] Such influence is possible largely because of Americans' reliance on social media. In early 2019, Twitter averaged over 330 million monthly active users.[20] By mid-2020, Twitter averaged over 186 million daily active users, of which nearly 20% (36 million) were in the United States.[21] More than half of U.S. adults get their news from social media "often" or "sometimes." [22] In 2020, social media was one of the top-ranking sources of news for Americans after news apps and websites, especially among those under 50 years old.[23] Concurrently, public trust in the broader media ecosystem has been declining: a 2019-20 poll found "low levels of public trust in the nation's polarized media environment," which opens possibilities for misinformation to thrive.[24] Given the importance of social media platforms in communications globally and the history of prior attacks, incidents like the Twitter Hack expose the risks to the stability and integrity of elections, financial markets and national security. [4] N.Y. Fin. Servs. L. § 102(f). [5] N.Y. Fin. Servs. L. § 102(b). [9] See Conf. of State Bank Supervisors, CSBS Model Data Security Law. [12] Twitter Help Center, About Direct Messages. [18] Statement by NCSC Director William Evanina: 100 Days until Election 2020 (July 24, 2020). [19] U.S. Senate Select Committee on Intelligence Report. [20] Clement, supra note 3. [21] Twitter, Inc., Q2 2020 Letter to Shareholders, supra note 3. [24] Gallup, Inc. et al., American Views 2020: Trust, Media and Democracy The Attackers Used Fraudulent Means to Access Twitter's Network and Internal Applications[25] On July 14 and 15, 2020, the Hackers attacked Twitter.[26] The Twitter Hack happened in three phases: (1) social engineering attacks to gain access to Twitter's network; (2) taking over accounts with desirable usernames (or "handles") and selling access to them; and (3) taking over dozens of high-profile Twitter accounts and trying to trick people into sending the Hackers bitcoin. All this happened in roughly 24 hours. Phase One: Stealing Credentials through Social Engineering The Twitter Hack started on the afternoon of July 14, 2020,[27] when one or more Hackers called several Twitter employees and claimed to be calling from the Help Desk in Twitter's IT department. The Hackers claimed they were responding to a reported problem the employee was having with Twitter's Virtual Private Network ("VPN"). Since switching to remote working, VPN problems were common at Twitter. The Hackers then tried to direct the employee to a phishing website that looked identical to the legitimate Twitter VPN website and was hosted by a similarly named domain. As the employee entered their credentials into the phishing website, the Hackers would simultaneously enter the information into the real Twitter website. This false log-in generated an MFA notification requesting that the employees authenticate themselves, which some of the employees did. The Department found no evidence the Twitter employees knowingly aided the Hackers. Rather, the Hackers used personal information about the employees to convince them that the Hackers were legitimate and could, therefore, be trusted. While some employees reported the calls to Twitter's internal fraud monitoring team, at least one employee believed the Hackers' lies. The first Twitter employee whose account the Hackers compromised did not have access to the internal tools that would allow them to takeover Twitter user accounts. Instead, the Hackers used this initial compromise to navigate Twitter's internal websites and learn more about Twitter's information systems. The Hackers reviewed Twitter's intranet websites containing information about how to access other internal applications. On July 15, the Hackers targeted Twitter employees who had access to the internal tools. Some of them were part of the department responsible, in part, for responding to sensitive global legal requests, such as court orders or content removal requests, as well as for developing and enforcing policies to prohibit abusive online behavior. Phase Two: Stealing "OG" Twitter Accounts After gaining the ability to take over a Twitter user's account, the Hackers first focused on so-called "original gangster" ("OG") Twitter usernames, which are usually designated by a single word, letter, or number and adopted by Twitter's early users. Because they are coveted markers of online credibility among later users, anyone who can successfully hijack an OG username can potentially sell access to it for thousands of dollars. Between approximately 3 a.m. and 10 a.m. on July 15, 2020, the Hackers allegedly discussed through online chat messages the takeover and sale of OG Twitter usernames in exchange for bitcoin, which Twitter confirmed resulted in the compromise of multiple accounts.[28] Soon, however, the Hackers turned to more public means of demonstrating their successful infiltration of Twitter's internal systems. Just before 2:00 p.m. on July 15, the Hackers hijacked multiple OG Twitter accounts and tweeted screenshots of one of the internal tools from some of the accounts to the accounts' respective followers.[29] Phase Three: The High-Profile Bitcoin Scam After their initial infiltration, the Hackers escalated the Twitter Hack. Notably, in this phase, the Hackers targeted "verified" accounts, which Twitter defines as "an account of public interest" typically "maintained by users in music, acting, fashion, government, politics, religion, journalism, media, sports, business, and other key interest areas." A verified account is denoted by a blue verified badge that "lets people know that an account of public interest is authentic."[30] As savvy users of online social media platforms, the Hackers likely knew that tweets from verified accounts would make their fraudulent demands for bitcoin appear more legitimate. The Hackers first manipulated Twitter accounts connected to well-known cryptocurrency companies and individuals. At approximately 2:16 p.m., they hijacked the account of cryptocurrency trader "@AngeloBTC" and tweeted the following announcement requesting bitcoin:[31] The Hackers then sent several DMs to multiple Twitter users from the "@AngeloBTC" account that included a link to a bitcoin wallet for payment. The Hackers further escalated the Twitter Hack and changed the fraud scheme by tweeting payment requests directly from overtaken cryptocurrency companies' accounts, as shown below.[32] At approximately 3:18 p.m., the Hackers seized the account of Binance, a cryptocurrency exchange and sent the following tweet, which included a link which linked to a bitcoin scam address:[33] Between approximately 3:26 p.m. and 4:12 p.m., the Hackers hijacked ten cryptocurrency-related accounts (including Department-regulated entities Coinbase, Gemini Trust Company, and Square, Inc.[34]) using variations of this message, as more fully explained in Part IV. The Hackers then raised the stakes significantly and targeted verified Twitter accounts with millions of followers. Between 4:17 p.m. and 6:05 p.m., the Hackers sent tweets from compromised accounts belonging to high-profile figures and companies such as Elon Musk, Tesla Inc.'s CEO; Bill Gates, Microsoft Corporation's co-founder; rapper and entrepreneur Kanye West and media personality and entrepreneur Kim Kardashian West; Joseph R. Biden, Jr., former Vice President and current Democratic Presidential Candidate; Warren Buffet, Berkshire Hathaway, Inc.'s CEO; Floyd Mayweather Jr., undefeated professional boxer; Uber, Inc.; and Apple, Inc. The Hackers also used some of the compromised accounts to resend the same bitcoin scam tweets multiple times. Given the number of followers for each high-profile user account, the fraudulent tweets reached millions of potential victims across the globe. The Hackers stole approximately $118,000 worth of bitcoin through the Twitter Hack. The Twitter Hack Exposed Consumers' Nonpublic Information Overall, 130 Twitter user accounts were compromised during the Twitter Hack. Of those, 45 accounts were used to send tweets. For seven of the Twitter accounts involved, the Hackers also downloaded account information through Twitter's "Your Twitter Data" ("YTD") tool, which provides a summary of a Twitter account's details and activity. Information in the YTD includes the user's profile information, tweets, DMs, media (including images, videos, and GIFs attached to tweets and DMs), a list of the account's followers, a list of accounts the user follows, the user's address book, demographic information that Twitter has inferred about the user, information about ads the user has seen or engaged with on Twitter, and more.[35] The YTD is available to a user by logging into the account, re-entering the account password and making the request. When the Hackers accessed the one of the internal tools, they used it to generate YTD requests for the seven accounts for which data was downloaded and requested data for another 52 accounts for which data was not downloaded. Twitter confirmed it reached out directly to any account owner whose YTD was downloaded. None of the seven were verified accounts. Twitter believes that for up to 36 of the 130 targeted accounts, the Hackers also accessed DM inboxes, including a verified account of an elected official in the Netherlands. In the week following the Twitter Hack, Dutch politician Geert Wilders confirmed to multiple news sources that unauthorized DMs were sent from his Twitter account. According to Twitter, no other former or current elected officials' accounts had their DM inbox accessed.[36] Twitter's Response Twitter first became aware of this attack when several employees reported suspicious log-ins and phone calls on the morning of July 15. Twitter's internal incident response team was investigating these suspicious calls when, around 3:18 p.m., the takeovers of the cryptocurrency companies' accounts started. Twitter's incident response team rushed to respond, but it was hours before they were able to expel the Hackers from their systems. Despite the very public nature of the Twitter Hack, Twitter did not publicly report any real-time updates. Instead, for most of July 15, Twitter's only public acknowledgement was its deleting tweets revealing screenshots of one of the internal tools and tweets linked to the scam. At approximately 5:45 p.m., Twitter tweeted a statement saying it was "aware of a security incident impacting accounts on Twitter" and was "taking steps to fix it."[37] Unfortunately for users, those steps included preventing many verified accounts from tweeting or changing passwords and locking accounts where a password had been changed within 30 days of the incident, which Twitter confirmed at 6:18 p.m. Multiple public institutions could not access their accounts to communicate -- for example, the National Weather Service could not tweet a tornado advisory,[38] and even the Department's Twitter account was unavailable for several hours.[39] Internally, Twitter resorted to dramatic measures to stem the damage from the Twitter Hack. It severely limited or revoked its employees' access to its internal systems to prevent the Hackers from further infiltrating its systems or individual accounts, leading to long delays in responding to users' account maintenance requests. It also instituted an aggressive verification process during which every Twitter employee—starting with CEO Jack Dorsey—was required to attend a video conference with a supervisor and manually change their passwords in front of their supervisor.[40] Approximately three hours after its initial announcement, at 8:41 p.m., Twitter reported that most accounts could resume tweeting, although the functionality might be inconsistent. The Department's Investigation On July 16, Governor Cuomo asked the Department to investigate the Twitter Hack in light of concerns about the cybersecurity of our communications systems, and their importance to elections. The next day, the Department issued subpoenas, and later interviewed witnesses and reviewed documents. The Department also surveyed our cryptocurrency entities to study the Twitter Hack's impact on their operations and cybersecurity protocols. [26] Three of these men have since been publicly identified and were arrested in July and August 2020: Graham Ivan Clark, Mason John Sheppard, and Nima Fazeli. At least one other individual was involved. See Press Release, U.S. Dep't of Justice, Three Individuals Charged For Alleged Roles In Twitter Hack (July 31, 2020) ("DOJ Press Release"); Kate Conger & Nathaniel Popper, Florida Teenager Is Charged as "Mastermind" of Twitter Hack, N.Y. Times (July 31, 2020) (updated Sept. 1, 2020); Nick Statt, Twitter Hack Conspirators May Include a 16-Year-Old from Massachusetts, The Verge (Sept. 2, 2020). [27] All times referenced in this Report are in Eastern Daylight Time. [28] See DOJ Press Release, supra note 26 (describing charges and attaching affidavits describing the Hackers' actions). [30] Twitter retains the sole right to designate an account as verified and may remove verification at any time without notice. Twitter Help Center, About Verified Accounts. As of October 6, 2020, with few exceptions, the verification program is suspended until further notice and future requests for verification will not be accepted. Id. [31] Larry Cermak, The Twitter Account Hacks: A Comprehensive Timeline of Events, The Block (July 16, 2020). [32] After the "@AngeloBTC" DMs, Sheppard and Fazeli declined to participate further in the Twitter Hack, while Clark, and potentially an unidentified teenager, continued to take over other accounts. See Nathaniel Popper & Kate Conger, Hackers Tell the Story of the Twitter Attack from the Inside, N.Y. Times (July 17, 2020) (updated July 31, 2020), available here. [33] Carlos Park, Large Scale Twitter Hack Rocks Crypto World, The Daily Chain (July 29, 2020). [34] Jack Dorsey is CEO and Chairman of Square, CEO of Twitter, and co-founder of both. [35] Twitter Help Center, How to Access Your Twitter Data. [37] Twitter Support (@TwitterSupport), Twitter (July 15, 2020, 5:45 p.m.) [39] Indeed, while the Department's Twitter account was down, the Superintendent used her personal Twitter account to warn consumers about the scam. See Linda A. Lacewell (@LindaLacewell), Twitter (July 15, 2020, 7:18 p.m.) [40] Thompson & Barrett, How Twitter Survived, see supra note 37. Phase 3 of the Twitter Hack was aimed squarely at cryptocurrency exchanges, including DFS-regulated entities authorized to engage in VCBA ("Cryptocurrency Companies") and their customers. Cryptocurrency Companies whose Twitter accounts were hacked, however, responded quickly to block impacted addresses, demonstrating the maturity of New York's cryptocurrency marketplace and those authorized to engage within it. Their actions show that New York continues to set a high standard and attract only the most responsible actors. To be clear, the Cryptocurrency Companies were not themselves hacked, but they were impacted in two ways. First, the Twitter accounts of four entities, or their parent, were hacked. Second, even for entities whose Twitter accounts were not hacked, their customers were still susceptible to being tricked by other hacked accounts; customers at four Cryptocurrency Companies (including two whose Twitter accounts were hacked) transferred or attempted to transfer bitcoin because of the Twitter Hack. In response to the Twitter Hack, the Department instructed the Cryptocurrency Companies at 6:59 p.m. on July 15, 2020, to block the bitcoin addresses the Hackers used, if they had not done so already. Two days later, the Department surveyed the Cryptocurrency Companies and subsequently requested additional information regarding their security around social media and their response to hacks.[41] The survey data below illustrates the swift efforts taken to block transfers to the fraudsters' bitcoin addresses and safeguard customer funds. The Cryptocurrency Companies providing wallet services whose Twitter accounts were hacked (Coinbase, Gemini and Square) rapidly blocked the bitcoin addresses the Hackers posted on Twitter.[42] From the survey, each of the three Cryptocurrency Companies blocked the Hackers' addresses within 40 minutes of their Twitter accounts being hacked. Through its survey, the Department additionally learned: Fifteen Cryptocurrency Companies blocked transfers to the addresses the Hackers posted on Twitter and seven did not.[43] Four Cryptocurrency Companies actively blocked their customers' attempts to send bitcoin to the Hackers' bitcoin addresses: Coinbase blocked approximately 5,670 transfers, valued at approximately $1,294,000. Square blocked 358 transfers, valued at approximately $51,000. Gemini blocked two transfers, valued at approximately $1,800. Bitstamp blocked one transfer, valued at approximately $250. Despite efforts, Gemini, Square, and Coinbase advised that in the minutes before the blocking of addresses, a handful of customers were induced to make transfers to the Hackers' accounts, totaling approximately $22,000 in losses. These are the only reported Cryptocurrency Company client losses and represent just 1.63% of the value of the blocked transfers. The Department also sought information about additional measures Cryptocurrency Companies took to protect their social media accounts following the Twitter Hack, which included: Reviewing settings and changing passwords; Conducting better brand monitoring across platforms; and Creating a matrix document of social media account users and access controls for better tracking and auditing. When asked to describe the security measures the Cryptocurrency Companies used to protect their social media accounts generally, the key responses included: Using strong, unique passwords; Using MFA; Avoiding using SMS-based MFA, which is more susceptible to hacks; Limiting employee access to social media accounts; Actively monitoring the social media accounts for unauthorized posts; Employing a social media security monitoring provider to monitor the Cryptocurrency Company's account and its high-profile principals' accounts; and Storing credentials with a third-party password management provider. Cryptocurrency Scams Pose Risks to Cryptocurrency Companies, Their Customers, and the Market In 2019 alone, millions of people globally lost over $4.3 billion to cryptocurrency scams.[44] This is a significant increase from approximately $650 million in 2018.[45] During the global pandemic, scammers continue to defraud victims; the Department, among others, has recognized an increase in cryptocurrency scams during this time.[46] During the first half of 2020, scammers stole over $380 million.[47] In the cryptocurrency space, scammers often rely on virtual versions of tried-and-true schemes. For example, the Hackers deployed a classic impersonation or "trust trading" scam. As previously discussed in Section III.A.3, the Hackers took over Verified Twitter accounts of prominent names in technology, entertainment, and politics to induce victims to relinquish their cryptocurrency on the promise of immediately doubling their initial investments. Similar trust trading scams accounted for about 71% of all self-reported crypto scams since June 2018.[48] One high-profile example in the news involves Elon Musk, who is frequently impersonated by trust trading scammers, as he was during the Twitter Hack. To take one illustrative example, in November 2018 hackers took over certain verified Twitter accounts that had significant followings, including Pantheon Books, a subsidiary of Knopf Doubleday Publishing, and changed the names and profiles so they appeared to be Musk's Twitter account: Impersonating Musk on Twitter has been lucrative; one news report indicated victims lost nearly $200,000 in bitcoin.[49] Musk tweeted a warning to his followers:[50] Collectively, these scams have resulted in substantial losses. From July 2019 to June 2020, Chainalysis, a blockchain analysis company, tracked approximately $100 million from victims located in North America lost to cryptocurrency to scammers.[51] Unfortunately, many victims will not recover the monies lost to these scams, so the best defense is not to become the next victim. [41] The Department surveyed 25 Cryptocurrency Companies, but only received 22 replies because three of the Cryptocurrency Companies' replies covered two Cryptocurrency Companies, as they have the same management and do not have separate Twitter accounts. [42] The fourth Cryptocurrency Company, whose parent's Twitter account was hacked, did not block any addresses because it does not provide wallet services. [43] Not all Cryptocurrency Companies blocked transfers, in part owing to their business models (e.g., bitcoin ATM operators), which rely on other Cryptocurrency Companies for custody and transfer services, or which only allow transfers to safelisted addresses. [45] Ciphertrace Report at 5. [51] The Chainalysis 2020 Geography of Cryptocurrency Report. The Twitter Hack is a cautionary tale about the extraordinary damage that can be caused even by unsophisticated cybercriminals. The Hackers' success was due in large part to weaknesses in Twitter's internal cybersecurity protocols. The problems started at the top: Twitter had not had a chief information security officer ("CISO") since December 2019, seven months before the Twitter Hack. A lack of strong leadership and senior-level engagement is a common source of cybersecurity weaknesses. Strong leadership is especially needed in 2020, when the COVID-19 pandemic has created a host of new challenges for IT and cybersecurity. Like many organizations, in March Twitter transitioned to remote working due to the pandemic. This transition made Twitter more vulnerable to a cyberattack and compounded existing weaknesses. The Hackers directly exploited Twitter's shift to remote working. The ramp up to total remote working in March 2020 put a strain on Twitter's technology infrastructure, and employees had frequent problems with the VPN connections to the network.[52] The Hackers took advantage of these issues and pretended to be calling from Twitter's IT department about a VPN problem, and then persuaded employees to enter their credentials into a website designed to look identical to the real VPN login website. The Hackers' claims were far more credible–and ultimately successful–because Twitter's employees were all using VPN connections to work and routinely experiencing VPN problems that required IT's assistance. The Hackers relied on a simple tactic to hack into Twitter: social engineering. Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information which is later used for fraudulent purposes. Perhaps the most well-known type of social engineering attack is phishing – the use of deceptive emails to trick the recipient into, say, opening a malicious attachment or providing their username and password. The Hackers used "vishing," social engineering over the phone. Phishing and vishing are among the most common methods that hackers use to get access to a network. For example, between January and July 2020, approximately one-third of the significant cybersecurity incident notices filed with the Department involved phishing or vishing. The Hackers also relied on basic information about Twitter and its employees to make their deception more credible. The Hackers appear to have conducted research to identify basic functions and titles of Twitter employees, so that they could better impersonate Twitter's IT department.[53] And conversations during the vishing calls themselves could have provided more information about Twitter's internal operations. Armed with these personal details, the Hackers successfully convinced several Twitter employees that they were from Twitter's IT department and stole their credentials.[54] Earlier this year, the Department issued guidance to its regulated entities to identify and assess the new security risks created by the pandemic, and similar warnings were issued by other public and private sources.[55] Notably, Twitter did not implement any significant compensating controls after March 2020 to mitigate this heightened risk to its remote workforce, and the Hackers took advantage. To its credit, Twitter has advised the Department that it is now implementing additional security controls to prevent similar attacks in the future, such as improved MFA and additional training on cybersecurity awareness, and in late September 2020 it announced the hire of a new CISO. But the consequences of the Twitter Hack show why it is critical for Twitter and other social media companies to implement robust controls before they experience a cyber incident, not after. [53] Such research is common and could include scraping information available on public social media websites and associated personal websites such as work or sports teams. Social media webpages can include personal data such as home addresses, work or personal cellphone numbers, places of employment, and the names of work or personal associates. Vishing and Cyber Criminals During Covid-19, Security Magazine (Apr. 30, 2020). The Department has identified several practices that help prevent and/or mitigate cybercrimes such as the Twitter Hack. This includes anti-fraud practices for Cryptocurrency Companies and cybersecurity measures that are appropriate for most organizations. Best Practices for Cryptocurrency Companies The Twitter Hack highlighted the effective controls and strategies that had been put in place at the Cryptocurrency Companies in New York to block fraud and prevent the misuse of our financial systems. The Department has identified several best practices for Cryptocurrency Companies. The relevance of these best practices to Cryptocurrency Companies will vary depending on their unique business models and risk profiles. Block Cryptocurrency Addresses Associated with Scammers Companies facilitating cryptocurrency transfers should continue to proactively identify and quickly block addresses known to be used by fraudsters. Speed matters. As the Twitter Hack demonstrated, when companies have practices in place to monitor, identify, and quickly block suspect addresses, they can protect their customers from loss. Such efforts are important to building public confidence and trust for this nascent industry. Restrict Transfers to Pre-Approved Addresses Another step some companies are taking is to restrict cryptocurrency asset transfers only to addresses that have already been approved, also called "safelisting" (a/k/a "whitelisting"). When practical, some Cryptocurrency Companies have adopted this process, through which a customer pre-approves addresses to which transfers from the Cryptocurrency Company can be made. A customer's adding a new address can take a day or more to complete, which could prevent any hasty transfer decisions, including those made in connection with the Twitter Hack. The Department, however, recognizes that safelisting may not be suitable for all Cryptocurrency Companies, including those with thousands of customers; the manual nature of adding addresses could be unrealistic to implement. A Cryptocurrency Company may also find it difficult to use safelisting if its customers spend their cryptocurrency with different merchants; adding a new merchant's address each time the customer wants to shop somewhere new would seemingly defeat the purpose of using cryptocurrency for purchases. As an alternative to safelisting, some Cryptocurrency Companies have added controls for larger transfer requests, requiring MFA or delaying the transfers for a period of time. Improve the Marketing of Legitimate Promotions Cryptocurrency Companies should not run promotions and contests that look like common

scams. Companies that run promotions that are difficult to distinguish from scams confuse customers and set them up to be victimized. Promotions publicized on Twitter and other social media that offer prize money for retweets or sharing an individual's account information should be accompanied by additional information to help a consumer verify the authenticity of the promotion. Educate Consumers About Spotting Scams The Department encourages Cryptocurrency Companies to educate consumers about scams. Cryptocurrency is a new and growing industry, and new consumers entering the space are often not aware of common and recurring scams. Just as companies, schools, and governments conduct cybersecurity awareness training, consumers need training on how to protect themselves from hacks and scams. The Department, therefore, recommends Cryptocurrency Companies regularly update their customers, especially retail customers, about identified and potential risks. Conduct Scam Monitoring To support the previous recommendations, companies should engage in active monitoring to identify patterns and trends regarding fraudulent activity. For example, at least one Cryptocurrency Company has noticed a recent rise in "romance" attacks. These are attacks in which a scammer creates an online profile–often on a dating application–and pretends to have a romantic interest in potential victims. Over time, the scammer gains trust from the victim, who is duped into sending money for fabricated expenses, such as medical bills, travel costs, or customs fees to retrieve impounded items. In 2019, 25,000 people reported being romance scam victims, losing approximately $201 million, up 40% from 2018.[56] Because Cryptocurrency Companies are monitoring for scams, they are well-positioned to respond when patterns emerge. For example, once the Cryptocurrency Company became aware of the serious threat romance scams posed to their customers, they took solid action steps such as blocking fraudulent addresses and coordinating with regulators and law enforcement. Also, they are in the process of circulating guidance to their customers, identifying how to spot and avoid them. It is this type of vigilance and commitment to educating customers that can prevent consumers from losing money. Sharing Information with Other Cryptocurrency Companies To ensure that all companies have relevant information, the Department encourages Cryptocurrency Companies to share information about fraud and cybercrime. This can be valuable at any time but is particularly important during crisis. Cryptocurrency Companies should also participate in information sharing groups, such as the Financial Services Information Sharing and Analysis Center ("FS-ISAC"). Information sharing will help ensure all players in the space have up-to-date knowledge about attacks and how others are acting to stop them. Cybersecurity Best Practices Could Have Mitigated Twitter's Risks As demonstrated by the Twitter Hack, cybersecurity flaws can have serious consequences. The practices described below can help protect consumers and industry from similar hacks and would have substantially reduced the likelihood of the Twitter Hack. Leadership Given the importance of cybersecurity, the tone needs to be set from the top. Leadership is critical, and an executive-level leader should be responsible for cybersecurity. The Department's cybersecurity regulation requires companies to have a CISO, and for good reason.[57] A CISO should have sufficient independence to press for improved cybersecurity protocols, and having a CISO is important for getting buy-in on cybersecurity measures from senior management and across the organization. And a lack of a CISO sends the message that cybersecurity is not a top priority from senior leadership. Access Management and Authentication Twitter's access management and authentication failed to prevent unsophisticated hackers from getting to the powerful internal tools. Access controls are security techniques or measures that restrict who can access or use a resource. Consistent with best practices, the Department's cybersecurity regulation requires that each user should have access to systems and applications only to the extent necessary for their job.[58] Access should be recertified regularly, to account for changes in roles and responsibilities. While Twitter did have some access controls in place, they were not enough to prevent the Twitter Hack. Twitter did limit access to the internal tools, but over 1,000 Twitter employees still had access to them for job functions and duties such as Twitter user account maintenance and support, content review, and responses to reports of Twitter Rules violations. Immediately after the Twitter Hack, however, Twitter further limited the number of employees with access to the internal tools, even though it caused a slowdown of some job functions.[59] Authentication requirements should also be calibrated to match the risk. For instance, for high-risk applications and functions like Twitter's internal tools, authentication requirements should be stricter. Access to critical functions should require MFA. Another possible control for high-risk functions is to require certification or approval by a second employee before the action can be taken. An approval requirement can limit the damage if an attacker compromises one employee's access. MFA is critical, but not all MFA methods are created equal. Twitter used application-based MFA, which sent a request for authentication to an employee's smart phone. This is a common form of MFA, but it can be circumvented. During the Twitter Hack, the Hackers got past MFA by convincing the Twitter employees to authenticate the application-based MFA during the login. The most secure form of MFA is a physical security key, or hardware MFA, involving a USB key that is plugged into a computer to authenticate users. This type of hardware MFA would have stopped the Hackers, and Twitter is now implementing it in place of application-based MFA. Employee Education and Training The Hackers succeeded by fooling Twitter employees with a social engineering attack. Such attacks can be aimed at employees in any part of an organization, and the first line of defense is to ensure that all employees are aware of threats, including social engineering techniques aimed at exploiting the new normal of remote working. This is why the Department's cybersecurity regulation requires regular cybersecurity awareness training for all employees.[60] In addition to training with metrics for success, organizations should also conduct regular phishing and vishing exercises to test the organization's ability to respond to such attacks. Organizations should further establish uniform standards of communications and educate employees about them. For example, the Federal Financial Institutions Examinations Council, which sets regulatory standards for testing the safety and soundness of financial institutions, recommends best practices to educate customers about cybersecurity hygiene when accessing products and services online. These principles also apply to employees, especially when they are accessing employer VPNs or using their own devices rather than employer-issued equipment: Explain in plain terms how the entity will contact employees about suspicious account activity (e.g., the entity will not ask the employee to provide his or her log-in credentials over the phone or via e-mail); Recommend controls and prudent practices that employees should implement when using the institution's remote access services; Recommend technical and business controls that can be implemented to mitigate the risks from fraud schemes; and Provide a method to contact the institution if employees notice suspicious account activity.[61] Security Monitoring [62]In addition to ensuring the right people have the right access at the right time, the best practice is to always log and monitor their usage. Security information and event management ("SIEM") systems not only log usage, but they also collect, aggregate, analyze, and correlate information from discrete systems and applications and use that information to identify anomalous activity, including insider threats and malicious actors. If Twitter had a robust security monitoring program, it would have been able to detect the anomalous activity in near real-time and respond quickly (or proactively terminate sessions based on risk). Security teams should use a SIEM system to monitor network activity and follow up on threat alerts. Regardless of the log management method, institutions should develop processes to collect, aggregate, analyze, and correlate security information. DFS's cybersecurity regulation sets forth a framework for audit trails necessary to reconstruct financial transactions and detect and respond to cybersecurity incidents.[63] Policies should define retention periods for security and operational logs. Institutions maintain event logs to understand an incident or cyber event. Monitoring those event logs for anomalies and comparing that information with other sources of information broadens the institution's ability to understand trends, quickly react to threats, and improve reporting. Akin to other critical industries, public oversight of social media is needed. While there are various proposals to improve public oversight of large social media companies or technology companies more broadly, they primarily focus on the issues of antitrust/competition or content moderation.[64] As the Twitter Hack demonstrates, cybersecurity weaknesses at a large social media company can have widespread consequences. There are well-documented instances of our adversaries hacking traditional media, social media, and other institutions to spread disinformation.[65] We need a comprehensive cybersecurity regulation and an appropriate regulator for large social media companies. The stakes are too high to leave to the private sector alone. Cybersecurity Regulation for Large Social Media Companies The Department's cybersecurity regulation for the financial services industry established an effective regulatory approach and is a good model here. This regulation, which was the first of its kind, requires a comprehensive, risk-based cybersecurity program. The regulation requires companies to assess their security risks, and then develop policies for data governance, access controls, system monitoring, third party security, and incident response and recovery. It also requires notification of compliance from covered entities, and notification to the Department of certain cyberattacks. As previously noted, the regulation has served as a model for other regulators, including the FTC, multiple states, the NAIC, and the CSBS. While there are some regulatory requirements for social media companies that touch on data security, these are much less comprehensive and stringent. The most comprehensive is New York's SHIELD (Stop Hacks and Improve Electronic Data Security) Act, enacted in 2019. The SHIELD Act protects New Yorkers by imposing enhanced data breach notifications requirements and mandating "reasonable" cybersecurity safeguards. But, as it is intended to apply to all companies doing business in New York, the SHIELD Act's requirements are general and do not specify substantive controls or a comprehensive program. Given the criticality of Twitter and other major social media companies, more oversight should be required. An effective cybersecurity regulation here should go even further than the Department's regulation. The Department's regulation, which was drafted with substantial industry input, was carefully designed to be flexible enough to apply to the thousands of companies regulated by the Department, from global corporations to small businesses. By contrast, a regulation for major social media companies could be applied to a handful of large, complex, and technologically sophisticated corporations with a global footprint. A cybersecurity regulation for large social media companies should be both more detailed and require more security in high-risk areas. In light of the issues exposed by the Twitter Hack, regulatory guidance is necessary to ensure large social media companies have proper controls in place to appropriately mitigate ever-evolving risks. A New Regulator is Needed Social media companies currently have no dedicated regulator. They are subject to the same general oversight applicable to other companies. For instance, the SEC's regulations for all public companies apply to public social media companies, and antitrust and related laws and regulations enforced by the Department of Justice and the FTC apply to social media companies as they do to all companies. Social media companies are also subject to generally applicable laws, such as the California Consumer Privacy Act and the New York SHIELD Act. The European Union's General Data Protection Regulation, which regulates the storage and use of personal data, also applies to social media entities doing business in Europe. But there are no regulators that have the authority to uniformly regulate social media platforms that operate over the internet, and to address the cybersecurity concerns identified in this Report. That regulatory vacuum must be filled. A useful starting point is to create a "systemically important" designation for large social media companies, like the designation for critically important bank and non-bank financial institutions. In the wake of the 2007-08 financial crisis, Congress established a new regulatory framework for financial institutions that posed a systemic threat to the financial system of the United States. An institution could be designated as a Systemically Important Financial Institution ("SIFI") "where the failure of or a disruption to the functioning of a financial market utility or the conduct of a payment, clearing, or settlement activity could create, or increase, the risk of significant liquidity or credit problems spreading among financial institutions or markets and thereby threaten the stability of the financial system of the United States."[66] The risks posed by social media to our consumers, economy, and democracy are no less grave than the risks posed by large financial institutions. The scale and reach of these companies, combined with the ability of adversarial actors who can manipulate these systems, require a similarly bold and assertive regulatory approach. The designation of an institution as a SIFI is made by the Financial Stability Oversight Council ("FSOC"), which Congress established to "identify risks to the financial stability of the United States" and to provide enhanced supervision of SIFIs.[67] The FSOC also "monitors regulatory gaps and overlaps to identify emerging sources of systemic risk."[68] In determining whether a financial institution is systemically important, the FSOC considers numerous factors including: the effect that a failure or disruption to an institution would have on financial markets and the broader financial system;[69] the nature of the institution's transactions and relationships; the nature, concentration, interconnectedness, and mix of the institution's activities; and the degree to which the institution is regulated.[70] An analogue to the FSOC should be established to identify systemically important social media companies. This new Oversight Council should evaluate the reach and impact of social media companies, as well as the society-wide consequences of a social media platform's misuse, to determine which companies they should designate as systemically important. Once designated, those companies should be subject to enhanced regulation, such as through the provision of "stress tests" to evaluate the social media companies' susceptibility to key threats, including cyberattacks and election interference. Finally, the success of such oversight will depend on the establishment of an expert agency to oversee designated social media companies. Systemically important financial companies designated by the FSOC are overseen by the Federal Reserve Board, which has a long-established and deep expertise in banking and financial market stability. A regulator for systemically important social media would likewise need deep expertise in areas such as technology, cybersecurity, and disinformation. This expert regulator could take various forms; it could be a completely new agency or could reside within an established agency or at an existing regulator. Our public institutions must evolve to keep up with new types of systemically important systems such as social media. The need for a new regulatory framework is clear. [66] 12 U.S.C. § 5462(9). [69] 12 U.S.C. § 5463(a)(2)(D). [70] Stupak, supra note 67. The Twitter Hack brought a social media giant to its knees. The David to this Goliath was a group of unsophisticated cyber crooks who exploited social media to create widespread disruption for hundreds of millions of users. The election weeks away puts a spotlight on the need to improve cybersecurity to prevent misuse of social media platforms. Social media companies have evolved into an indispensable means of communications: more than half of Americans use social media to get news, and connect with colleagues, family, and friends. This evolution calls for a regulatory regime that reflects social media as critical infrastructure. The swift and effective response of DFS-regulated Cryptocurrency Companies illustrates how effective regulation can foster innovation and growth, while also protecting consumers. After the Hackers took control of the Twitter accounts of the Cryptocurrency Companies, the Companies reacted within minutes to block transactions between customers' and the Hackers' bitcoin addresses. This swift action blocked over 6,000 attempted transfers worth approximately $1.5 million to the Hackers' bitcoin addresses. These actions were made possible because the Cryptocurrency Companies had robust programs around cybersecurity, fraud-prevention, and anti-money laundering programs–as required by DFS regulations. As the Department has shown, a balance can be struck between encouraging innovation and promulgating regulation to protect consumers. In contrast, the large and globally influential social media companies essentially regulate themselves. There is no dedicated state or federal regulator empowered to ensure adequate cybersecurity practices to prevent fraud, disinformation, and other systemic threats to social media giants. An analogue to the Financial Stability Oversight Council should be established to designate systemically important social media companies, and a regulator with appropriate expertise should be tasked with monitoring and supervising the cybersecurity of these companies. The Twitter Hack demonstrates, more than anything, the risk to society when systemically important institutions are left to regulate themselves. Protecting systemically important social media against misuse is crucial for all of us–consumers, voters, government, and industry. The time for government action is now. Acknowledgement: This report includes research and/or contributions from Joanne Berman, Jonathan Blattmachr, Debra Brookes, Shirin Emami, Robert Francis, Marcia Henry, Justin Herring, Matthew Homer, Katherine Lemire, Sasha Mathew, Chris Mulvihill, and Richard Weber.