GOLDBERG SEGALLA

Death by a Thousand Paper Cuts: The Scourge That Is Business Email Compromise

March 9, 2022

James Vinocur

In June 2014, the CEO of Omaha-based Scoular Company sent a series of emails to his company's controller to let him know that the company was in negotiations to buy a Chinese company. The emails highlighted the sensitivity of the matter and ordered him not to speak about the deal "in order . . . not to infringe SEC regulations."[1] The CEO of the 120-year-old agricultural commodities company then gave the controller the email address for their contact at KPMG and directed the controller to email their contact to get the wire details necessary to effectuate the deal. The CEO even provided the controller with the KPMG contact's phone number so that he could verify the wire information. The controller did as asked and soon enough wired $17.2 million to a Chinese bank account to complete the deal. The only problem was that the CEO had never sent the emails, and the KPMG contact was part of the scam.

The Scoular Company had fallen victim to a business email compromise (BEC) scheme, a type of cyberattack that targets organizations of all sizes into wiring funds to unauthorized recipients. In the Scoular Company's case, the perpetrators had established email accounts that made it appear as if the emails were coming from the company's CEO. And, to add a sense of legitimacy to the scheme, the perpetrators had used a real KPMG employee's name—but had provided a fake KPMG email address and phone number that they controlled.[2]

Unfortunately, the Scoular Company was just one of the thousands of organizations that fall victim to this scheme every year. In 2014, the year that the Scoular Company was victimized, BEC schemes accounted for approximately $60 million in reported losses in the United States.[3] By 2020, that number had multiplied by a factor of 30, to over $1.8 billion.[4]

The first half of 2021 saw headlines dominated by ransomware attacks against school systems,[5] government,[6] health-care systems,[7] and critical supply lines.[8] And for good reason. The threat of ransomware is pervasive and the effects substantial. Ransomware attacks can lead to extended periods in which crucial systems cannot be accessed—including, in one case, with deadly effect—and the direct and indirect costs frequently exceed six figures.[9] The 2017 NotPetya attack alone caused over $10 billion in damages and brought both the Ukrainian government and corporate giants such as global shipping companies Maersk and FedEx to their knees.[10]

But if ransomware is a body blow, BEC is death by a thousand paper cuts. The average organization is almost eight times more likely to sustain a BEC attack than a ransomware attack, and that number is

probably low.[11] At its most basic, a BEC is a cyberattack in which a victim's email account is compromised for the purpose of inducing, or causing to be induced, a fraudulent transfer of funds. Typically, these attacks target individuals who have control of or access to their company's purse strings. Attackers will either gain access to internal email accounts or impersonate a counterparty in order to provide new, unauthorized bank account information. In many cases, the stolen money will then quickly be moved to secondary or tertiary bank accounts before being wired overseas, where the chances of recovering the funds are slim.

This article will endeavor to explain what BEC is, how it works, and who is behind it, as well as detail the myriad of legal and insurance issues that can arise as the result of a successful BEC attack. It will also give some thoughts on what trends might be seen next and how best to defend one's organization from this pervasive and persistent threat.

The Costs of BEC

According to the Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center (IC3) yearly report, losses attributable to BECs exceeded $1.8 billion in the United States in 2020—the largest amount in any fraud category that it monitors, and a full third of all losses attributable to cybercrime.[12] And the trend is going in the wrong direction—that $1.8 billion figure represents a nearly $100 million increase from 2019 and a more than $500 million increase from 2018. Equally important is that this $1.8 billion figure is based on only the 300,000 complaints that IC3 received, meaning that the true loss figure is likely much higher due to underreporting.[13] By way of comparison, the same report indicates that ransomware losses in 2020 amounted to only $29 million.[14] BECs are over 14 times as costly as corporate data breaches and cost on average nearly $100,000 in direct losses, while bigger losses routinely exceed $1 million.[15] AIG Insurance announced in 2019, for example, that BECs were its biggest single source of cyber insurance claims—bigger than both ransomware and data breaches.[16] Furthermore, BECs affect organizations of all sizes—over 74% of all American organizations reported falling victim to a successful phishing attack.[17] From a geographic perspective, California, Florida, New York, and Texas were the states that sustained the most, and costliest, attacks in 2020.[18]

Direct losses attributable to BECs do not paint the full picture, however. In addition to directly quantifiable financial losses, successful BEC attacks can incur substantial indirect costs, including legal costs, postattack remediation, and reputational damage. For instance, a successful BEC attack may lead to employees not being able to access certain accounts or platforms and may require costly postincident investigation, forensic analysis, and network/account remediation. (This is in addition to loss of employee productivity due to employee time spent reviewing possible attacks. One study indicated that this cost the average worker seven hours of productivity a year, up from four hours in 2015.[19]) Meanwhile, reputational damage may be hard to quantify but no less a reality. For example, while a "typical" BEC attack may only affect the two parties to a financial deal—thereby hurting one party's reputation vis-à-vis its counterparty—a BEC attack that leverages a network intrusion can also lead to the theft of confidential, sensitive, or proprietary information; these breaches almost always trigger data breach notification requirements, which may have the unintended consequence of damaging corporate relations and customer trust.

This threat has also been exacerbated by the COVID-19 pandemic, which led to the increased use of and reliance on email to communicate with colleagues and outside entities.[20] And, to add insult to injury, bad actors took advantage of government programs such as 2020's Paycheck Protection Program (PPP) to further perpetuate BECs. For example, as part of the administration of the loans, the Small Business Administration (SBA) published details for the more than 11 million PPP loans that were approved.[21] This information was then compiled in searchable databases, which include the recipient's name, address, loan amount, loan originator, number of jobs reported, etc.[22] Bad actors then used this information to more accurately impersonate individuals or target potential victims in BEC schemes.[23] The U.S. Attorney's Office for the District of Massachusetts highlighted the issue in January 2021, noting that perpetrators used the information to impersonate PPP lenders and request personal identifying information, including account information.[24]

How BEC Works

BECs don't come in a single shape or size. There are hundreds of variations on the execution of the underlying intrusion, the exfiltration of funds, and the laundering of stolen funds.

Intrusion. It's safe to say, however, that successful BEC attacks begin with the bad actor choosing the right target. Regardless of the industry, BEC attacks typically target an organization's finance department or those authorized to order wire transfers, such as corporate executives.[25] These individuals are targeted by combing through corporate profiles, lead generator databases, LinkedIn, and the like.

The bad actors then attempt to deceive authorized personnel into sending wire transfers by impersonating a trusted source. This deception can occur in many ways, including via the use of "spoofed" email addresses and/or unauthorized intrusion into an email account.

In the first scenario, bad actors impersonate a company or entity's name in an email domain, known as "spoofing." Nearly three-quarters of organizations that reported BEC schemes reported spoofing a known domain as the attack vector.[26] In this variation, attackers register a domain name similar to the real domain but change a letter or character that would only register with a careful reading. For instance, momsnycdeli.com may be changed to momnycdeli.com or to momsnydeli.com.

In the second scenario, bad actors gain access to an employee's email account by inducing the employee to open an attachment or click on a link that contains malware. The number of ruses used to get people to do this are limited only by one's imagination. Well-known brands such as UPS, Apple, PayPal, and Bank of America are routinely impersonated, requesting that the recipient click on a link to track a package or verify suspicious bank activity, for instance. Other ruses include links to "unsubscribe" the recipient from unwanted emails, to prevent impending deactivation of cloud-based services and products, or to warn of password expiration. Targets may also receive emails about familiar and oft-used programs such as Office 365 or Google, alerting them to the need for an urgent update. These impersonations pose a particular difficulty because they cannot simply be blocked by an organization's IT department given these programs' myriad of daily legitimate uses. Finally, bad actors will leverage the successful intrusion of one organization against another by combing through correspondence to impersonate trusted vendors and counterparties. These directed, targeted attacks, also called spear phishing, account for 69% of all BEC attacks.[27]

Bad actors are also keenly aware of current events and the time of year. For example, bad actors took advantage of the COVID-19 pandemic by including embedded links that purported to contain health alerts and were predicted to do the same during the 2021 end-of-year holiday period.[28]

Once this second phase has been completed, attackers will either impersonate a senior employee or person of authority and request that a wire transfer be initiated, or insert themselves into ongoing email correspondence between parties who are discussing a wire transfer. In the first variation, bad actors will highlight both the urgency of the request and the need for secrecy. Requests that arrive late on a Friday and that urge the execution of a transfer "before the end of business" are commonplace and leverage an employee's attempt to please a superior. In the latter scenario, bad actors monitor email correspondence about a business transaction or deal. Once the deal has been finalized and banking details have been shared, the bad actor will send an email impersonating the recipient bank account holder and provide "updated" bank account information. Regardless of method, the result is the same—the sending of money to the wrong account.

Exfiltration. In the majority of BECs, the bank account provided to the legitimate sender will be a U.S.-based account. The reasons for this are twofold: (1) to avoid raising the sender's suspicions, and (2) to avoid triggering banks' fraud-control mechanisms. In the first instance, bad actors are keenly aware that inserting account information for a foreign-based bank may raise suspicions. A Toledo-based printing company may not have any foreign-based vendors or do business abroad, for example, and therefore might be suspicious about sending funds to a Hong Kong–based bank account. Second, even modestly sized U.S. banks have fraud detection mechanisms in place that detect anomalous transactions. A sudden departure from payment transfer history and destination may cause the bank to seek verification from the sender before transferring the funds.

In turn, these U.S.-based bank accounts largely amount to brief waypoints, or "hops," before the stolen funds are sent overseas or to other accounts. These "first-hop" accounts therefore exist almost entirely for the purpose of facilitating fraud and obfuscating the path of the funds. Their owners, known as "money mules" or simply "mules," can largely be divided into two groups: complicit/knowing account holders and unwitting victim account holders.

Complicit account holders are aware that their accounts will be used for the purpose of facilitating this fraud, and they are either recruited for this very purpose or are part of the organizational hierarchy itself. These witting participants conduct a number of crucial steps in a successful BEC, including establishing bank accounts, initiating wire transfers, withdrawing cash, and/or purchasing merchandise to be shipped abroad.

The recruiters are typically U.S.-based as well and will attempt to recruit those around them (including acquaintances, friends, and family) and also via social media and the internet. The recruiters typically provide instructions on how to set up business bank accounts and what to say if questioned by bank officials. They may also advise which banks have weaker antifraud detection mechanisms in place.[29]

As one might expect, these complicit account holders are the lowest rung of the BEC food chain and only obtain modest financial rewards for their role. These account holders are also the easiest for law enforcement to identify and apprehend, given that they likely used legitimate identification to open up the bank account.

The second type of recipient account belongs to unwitting victims who have been fraudulently induced to establish the accounts. These individuals are themselves duped by way of a scam, the most notorious and pernicious of which is the so-called romance scam. Bad actors frequently use dating platforms to target individuals to create a romantic or trusting relationship that can later be leveraged. The "grooming" of this victim can take weeks if not months, and bad actors often prey on insecurities and vulnerabilities until a sense of trust and intimacy is established. Bad actors will often claim to be overseas (e.g., a businessman currently working in Hong Kong, a soldier posted in Iraq, an oil executive sent abroad to the Middle East) and eventually will explain that they need help receiving and sending certain funds. Being overseas is important both to explain why the romance scam victim and the perpetrator cannot meet and also to account for odd or infrequent messaging response times. The cover stories for why they need the victim to establish the bank account can range from an inability to open a bank account in time to receive an investor's transfer of funds or a sudden inheritance, to the need for an American-based bank in order to receive a bank loan.

Another popular scheme that takes advantage of unwitting victims is based on work-from-home positions. This particular scheme has skyrocketed during the pandemic, when large swaths of working Americans sought employment that allowed them to work from home, thereby revictimizing people already in precarious financial situations. The scam works by publishing job postings online on reputable job sites or on social media for what are typically low-level positions.[30] Applicants are told that their job will require them to receive and deposit checks or merchandise from vendors or clients, and to then forward the funds to designated accounts or foreign addresses.[31] These checks instead represent the fruits of a successful BEC attack and were created by another individual farther up the scheme's ladder. The types of scams that began on social media proliferated during the pandemic as more people were at home and had constant access to their electronic devices. The Federal Trade Commission (FTC) announced in October 2020 that while losses attributable to social media scams totaled $134 million in 2019, the first six months of 2020 alone (which really means the first three months of the pandemic in the United States) saw losses hit $117 million.

Unfortunately, these victims often bear the most immediate repercussions of these scams as financial institutions close even long-established bank accounts for fraud. In the event that an account is shut down, bad actors often try to persuade victims to open up additional accounts at multiple institutions, until they are again shut down for fraud or the victims realize that they are being duped.

Bad actors are increasingly turning to cryptocurrency as a means to exfiltrate and launder their stolen money. The annual IC3 report for 2020 indicated an increase in cryptocurrency conversion, particularly with regard to BECs.[32] There are several reasons for this. First, cryptocurrency is by design more difficult to trace than fiat currency. While the details of every single Bitcoin (to name but one of the many types of cryptocurrency) transaction are registered on a publicly accessible ledger known as the blockchain, the details themselves offer few clues as to the identity and location of the sender and recipient.[33] Second, cryptocurrency markets and exchanges are not as regulated as traditional fiat banks. While federal and local regulations tightly dictate what information banks and financial institutions must collect and maintain about their customers and their transactions, cryptocurrency regulations are far behind, particularly outside of the United States and Europe.

Recovery. Recovery of stolen funds due to a BEC is unlikely, particularly if outside the initial 72-hour window. As detailed above, stolen funds typically first move to a domestic bank account before being wired overseas to a foreign bank, or converted to cryptocurrency. Wire transfers' relatively quick turnaround makes recovery efforts difficult. Once a bank has accepted a wire transfer, there are only limited extenuating circumstances that will allow for its reversal—and they are almost only in the event that the bank, not the sender, made a mistake.[34]

However, canceling an in-process wire transfer is possible, thereby highlighting the importance of both catching the fraud and notifying the sender's financial institution in a timely manner. Financial institutions hold the levers that can reverse or cancel these transactions and are therefore best placed to freeze or claw back funds in transit. In addition, IC3 operates a Recovery Asset Team (RAT) to act as a liaison between victims, law enforcement, and financial institutions.

Who Is Behind BEC Attacks

The FBI coined the term "business email compromise" in approximately 2013 when it first began tracking the trend,[35] but the scheme can be understood as the natural evolution of the mass spamming campaigns that predated it. These campaigns began with what are now colloquially known as Nigerian prince or lottery schemes.[36] These email scams were notable for their amateurism—misspellings, grammatical mistakes, unbelievable stories—and were easy to spot and ignore.[37] The perpetrators quickly gained technical expertise, however, and now employ some of the significantly advanced techniques described above.

The reason that BECs are said to have evolved from these Nigerian prince schemes is that there is evidence to suggest that the main organizers of these BEC schemes are based in Western Africa. According to a report conducted by Agari, a cybersecurity firm that tracks BEC patterns, a full half of all BECs originate in Nigeria; however, nearly a quarter originate in the United States.[38] This is partially explained by the fact that American-based businesses are preferred targets for global BEC bad actors.[39] And, as detailed above, the exfiltration path typically sees one or more bank account hops within the United States. A whopping 80% of the hops' mules were within the United States, concentrated mostly in California, Florida, Georgia, New York, and Texas.[40]

Meanwhile, a study conducted of Nigerian cybercriminals engaged in BECs between 2014 and 2020 revealed that the "majority of the actors [are] well educated, having completed both secondary and university programs," demonstrating the need for technical expertise in order to execute the increasingly technically sophisticated nature of BECs in 2021.[41] Other demographics indicate that these actors tend to be in their late teens and twenties and are organized.[42]

The wide-flung geographic distribution of these bad actors is one of the reasons that they are, when compared to the breadth of fraud, infrequently criminally prosecuted. However, Nigerian authorities increasingly have played a meaningful role in dismantling these rings and working with international law enforcement partners.[43] As a result, there have been recent notable arrests, perhaps none more so than Ray Hushpuppi. In June 2020, the U.S. Attorney's Office for the Central District of California indicted and extradited Ramon Olorunwa Abbas, better known as "Ray Hushpuppi," for his role in laundering millions of dollars stolen in BEC schemes.[44] Abbas, a Nigerian national, was known for his

extravagant and BEC-funded lifestyle, which he frequently chronicled on his Instagram page.[45] He often posted photos of himself in designer clothes, standing beside luxury cars, and sitting in private planes—all of which the U.S. Department of Justice noted in the criminal complaint filed against him.[46] Abbas eventually pleaded guilty in July 2021 to charges that carried a sentence of up to 20 years.[47]

Insurance and Legal Issues and Considerations

Unfortunately, BEC schemes target organizations of all sizes and from all industries. No company or organization that relies upon email to conduct business is immune from these attacks. Organizations should therefore ensure that their insurance policies cover BEC attacks, and that they consider the myriad of postincident legal issues that may arise, some of which are discussed below. Given the relative novelty of BECs, it should not be surprising that courts have differed in their treatment of the insurance and legal issues that surround these attacks.

Insurance coverage. A successful BEC attack will generally fall under either a first-party cyber-incident insurance policy or a commercial crime insurance policy. Provisions and endorsements that may provide coverage for BEC attacks include computer fraud provisions and policy endorsements addressing fraudulent transfer of funds and social engineering fraud.

Coverage denials often are based upon instances where the spoofed emails used in a BEC attack "did not require access to [internal] computer system[s] . . . or input of fraudulent information,"[48] where the spoofed emails were not the direct cause of the fraudulent wire transfer,[49] and where the inclusion of a forged signature did not fall under a forgery or alteration provision.[50] Recognizing the benefit of independent, verbal verification of new wire details (further discussed below in how best to protect oneself from BECs), some policies' "fraudulent transfer of funds" (also known as "fraudulently induced transfers") provisions will also require that these conditions be met before coverage is extended.[51] In addition, insurers have denied coverage under a computer fraud provision when an employee's act of issuing the wire transfers was determined to be an "intervening act."[52] Other frequent coverage issues are premised upon whether the funds were transferred with the insureds' knowledge (i.e., denying coverage if the insureds knowingly sent transfers, even if they were duped) or whether the fraud happened within the "computer network" versus an "email account"—thereby implicitly drawing a line between BECs that include network intrusion and cases involving only spoofed emails.[53]

Courts have split on these various issues, but notably both the U.S. Court of Appeals for the Second Circuit and the U.S. Court of Appeals for the Sixth Circuit have held that damages arising from BEC attacks that used spoofed email addresses constitute "direct losses" under applicable computer fraud endorsements.[54] In turn, denials of coverage complaints usually fall under breach of contract and implied covenant of good faith and fair dealing claims.[55]

It can only be presumed that as the types of and means utilized to employ BEC attacks continue to evolve, so, too, will the coverage issues arising out of the submission of claims based on these attacks.

Legal issues. Outside of the insurance context, lawsuits born out of successful BEC attacks generally invoke breach of contract and negligence claims.

Breach of contract claims often arise after one party has refused to transfer money called for under the contract terms a second time on the grounds that the counterparty failed to exercise reasonable security in allowing the interception of email traffic, while the other party will claim failure to pay per the terms of the contract.[56] As a result of the relative novelty of BEC attacks specifically and phishing attacks generally, courts have struggled to find a consistent analytical framework within which to analyze these claims. A number of courts have sought to analogize the issue to the Uniform Commercial Code (UCC) and the "imposter rule."[57] Under this analysis, "the party who was in the best position to prevent the [fraud] by exercising reasonable care suffers the loss."[58] Courts in this context will examine the parties' use of ordinary care. But the degree to which each party deviated from those standards is typically left to fact finders at trial, given how fact specific this inquiry can be.[59] However, other courts have found the UCC analogy to be misplaced, relying solely on the terms of the underlying agreement to reach a decision.[60] Relatedly, courts typically will not entertain tort claims alongside breach of contract claims that arise out of the same conduct.[61]

To add to the scope of the problems presented, many organizations store personal/private information not in email accounts but on their networks. The increasing sophistication of all phishing attacks, including BECs, means that it is likely if not probable that bad actors will leverage their initial intrusion to search entire networked systems.[62] The COVID-19 pandemic and the growing work-from-home trend that has emerged as a by-product have only exacerbated this risk. A BEC may therefore qualify as a data breach if the affected email account is not siloed from the larger computer network. In that event, organizations may face lawsuits claiming negligence, invasion of privacy, breach of implied contract, breach of fiduciary duty, and claims based upon state data breach notification and consumer fraud laws.[63] Class action suits are not uncommon in the event of large-scale breaches.[64] In turn, these cases often turn on the question of whether the party that sustained the breach owed a duty of care to the plaintiff, and/or whether the private information custodian abided by industry security standards—the determination of which is fact specific.[65] Courts have conducted this fact-specific inquiry by examining whether there had been warnings and whether the defendant was aware of other publicized breaches, for example.[66] If these preliminary hurdles are overcome, the analysis typically shifts to whether the breach was the proximate cause of the claimed injuries. Significant to this phase of the analysis, potential harm and increased risk of harm are insufficient bases to prove damages, and proactive steps taken to mitigate risk do not amount to injury in fact.[67]

Loss considerations aside, successful BECs may also trigger both state and federal notification requirements; but, again, the determination as to whether they do so is largely fact specific. Currently, there is no federal data breach notification law. Instead, each state has its own version with varying (but largely overlapping) definitions of personal/private information, notification deadlines, and related requirements. The majority of these state data breach laws do not permit private actions, but they may lead to civil actions brought by state attorneys general.[68] A successful BEC attack may therefore require the analysis of several states' data breach laws to ensure compliance. These state regulations are intended to prevent the unauthorized access to, or theft of, customers' personal and private information, including, for example, Social Security numbers, names, and financial details.[69]

With respect to financial account information, the majority of these laws require notification only in the event that an account number is stolen in combination with the credentials needed to access

that account, such as a username and password.[70] Applied to BECs, state data breach notification requirements therefore may not apply if the only accessed data was the organization's own account information that was subsequently replaced by the bad actor. The initial analysis also will have to take into account whether the affected email account housed customers', vendors', or even employees' personal information and/or the credentials necessary to access relevant accounts. Even if the bad actor's goal was to steal money via a BEC, most states' breach notification laws are triggered if it is "reasonable to believe" that this information may have been accessed.

Additionally, federal regulations require notification if a publicly traded company and/or a financial institution falls victim to a BEC. The U.S. Securities and Exchange Commission's (SEC's) "Safeguards Rule" requires organizations to maintain appropriate cybersecurity measures to protect customer information.[71] As noted above, successful BECs increasingly leverage an initial email account intrusion to access personal customer information stored on a related network. The SEC has been increasingly active in this space, including by recently issuing six-figure penalties against offending entities.[72] The Gramm-Leach-Bliley Act (GLBA) of 1999 also imposes duties upon financial institutions to safeguard their customers' "nonpublic personal information,"[73] while the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) require institutions that maintain sensitive health information to enact safeguards to protect the data and to notify individuals affected by a data breach.[74] Thus, the impact of a BEC clearly implicates a need to conduct a multifaceted analysis regarding the requisite response.

What to Expect Next

It is likely that BEC attacks will gain sophistication and leverage developing technologies, as well as trade on our everyday cyber habits. Perpetrators have increasingly turned to SMS/text messages and social media instant messaging platforms to conduct their phishing campaigns. In 2020, 81% of U.S. organizations reported SMS/text-based phishing attacks, also known as "smishing."[75] Much like their email counterparts, these messages include links that purport to provide health advisories, delivery timetables, or fraud alerts, for example, but which aim to steal online account credentials or personal information. Perpetrators have turned to these methods not only because individuals increasingly use and rely on them but also because people are generally more attuned to the dangers of email phishing than of text message phishing.

Furthermore, it's safe to assume that bad actors will take advantage of emerging technologies such as synthetic media. More commonly known as "deepfakes," these hyperrealistic images, videos, and audio files purport to depict real people saying something that they never actually said. A deepfake video shared online could depict, for example, an authentic-looking President Biden announcing to the nation that he was forgiving all student loan debt. These files are generally created by manipulating existing video or audio examples of the person to create a new file that looks and sounds authentic.[76] There are, of course, legitimate applications for this technology, but the potential for misuse is great, despite its relative infancy. The European Parliament even issued a report in July 2021 entitled *Tackling Deepfakes in European Policy*, which addressed areas of potential concern, particularly within politics, and proposed regulations to mitigate the risk.[77]

The propagation of deepfakes is of particular concern in the context of BECs. As noted previously, BECs succeed in part because employees feel pressured or obliged to obey their superiors' orders, particularly when a sense of urgency is imposed. As a result, organizations are commonly advised to implement a secondary verification process, such as a phone call or face-to-face confirmation, before executing wire transfers. The rise of deepfakes therefore poses a significant threat to existing security protocols. This risk is exacerbated by the growing popularity of remote work and its emphasis on video meetings. It is not too far-fetched to believe that bad actors' BEC tool kits will soon include the harvesting of their targets' online videos from social media or other sources in order to impersonate business executives at either the request stage or the confirmation stage.[78] There is analogous precedence for this: between 2015 and 2016, individuals impersonated Jean-Yves Le Drian, the then French defense minister, in an elaborate scheme that netted over €50 million (approximately $55 million at the time).[79] In that case, the perpetrators had Skype chats with wealthy victims and impersonated Le Drian by wearing a silicone mask, set against an official-looking background. As frequently seen in BECs, the perpetrators also stressed the urgency of the request and the need for secrecy. Although that scam targeted over 150 victims, only a few actually sent funds—albeit in significant amounts—demonstrating that these schemes do not necessarily need to succeed in every instance in order to be profitable.[80] More recently, the United Arab Emirates requested official help from the U.S. government in a case where perpetrators had impersonated a company director's voice to authorize the fraudulent transfer of $35 million.[81] There is, therefore, good reason to believe that newer incarnations of BEC fraud will use deepfake technology to impersonate executives, thereby requiring implementation of new security safeguards.

Mitigation

Despite both the increasing frequency and sophistication of BEC attacks, there are a number of easily implemented steps that organizations can take to prevent and mitigate these attacks.

Employee education. Cybersecurity is primarily not a computer issue, but a human one. Organizations should strive to educate their employees on how to spot phishing and social engineering, how BECs work, and what the potential fallout can be.

Multifactor authentication (MFA). Organizations should implement MFA to require additional entries rather than just the use of a password to access email accounts. Microsoft has stated that MFA-enabled accounts account for less than 0.1% of all account compromises.[82]

Independent verification. Employees charged with effectuating, facilitating, or sending wire transfers and other financial remittances should obtain verbal confirmation from relevant parties that (1) outgoing wire transfers are authorized both in amounts and destination and (2) bank account information is correct. This confirmation should be obtained via trusted, previously used lines of communication. Employees should be empowered to seek this confirmation from superiors, especially if the timing is suspicious or if they have been told that the matter is time sensitive.

Email management. Emails that arrive from outside the organization should include a banner warning the reader to be mindful of clicking on links, opening attachments, or responding to unknown senders. These banners should be brightly colored and attached to the top of any incoming email from outside

the organization. Furthermore, notifications should be implemented to detect the creation of automatic forwarding rules in email accounts. Many BECs involve the implementation of rules that automatically forward and/or delete incoming emails that mention "invoices" or "wire," for instance.

Password management. If security is limited to only password usage, passwords should be complex (i.e., using a range of letters, numbers, and characters) and changed on a regular basis. In addition, passwords should be unique to the account and not reused from another account. "Password fatigue" leads to repeated usage of the same password over a number of online accounts.

Endnotes

1. Maria Korolov, *Omaha's Scoular Co. Loses $17 Million after Spearphishing Attack,* CSO Online (Feb. 13, 2015), https://www.csoonline.com/article/2884339/omahas-scoular-co-loses-17-million-after-spearphishing-attack.html.

2. *Id.*; Chris Johnston, *Company Loses $17M in Email Scam*, Guardian (Feb. 5, 2015), https://www.theguardian.com/technology/2015/feb/05/company-loses-17m-in-email-scam.

3. Fed. Bureau of Investigation (FBI) Internet Crime Complaint Ctr. (IC3), 2016 Internet Crime Report (2016), https://www.ic3.gov/Media/PDF/AnnualReport/2016_IC3Report.pdf.

4. FBI IC3, 2020 Internet Crime Report (2020) [hereinafter 2020 Internet Crime Report], https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

5. *See* Layne Dowdall, *Buffalo Schools Still Reeling from Ransomware Attack*, WGRZ (May 11, 2021), https://www.wgrz.com/article/news/local/buffalo-schools-still-reeling-from-ransomware-attack/71-854e9915-4ec4-45af-a746-d38b25320e3c.

6. *See Tulsa System Shutdown Alters "Backside Operations," Ransomware Attack Still Being Investigated*, 2 News Okla. (May 11, 2021), https://www.kjrh.com/news/local-news/tulsa-system-shutdown-alters-backside-operations-ransomware-attack-still-being-investigated.

7. *See* Shira Ovide, *Don't Ignore Ransomware. It's Bad*, N.Y. Times (Apr. 29, 2021), https://www.nytimes.com/2021/04/29/technology/ransomware-attacks-prevention.html.

8. *See* Christina Wilkie, *Colonial Pipeline Paid $5 Million Ransom One Day after Cyberattack*, *CEO Tells Senate*, CNBC (June 8, 2021), https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html.

9. *See* Kevin Poulson et al., *A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death*, Wall St. J. (Sept. 30, 2021), https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116; *see also Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands*, Coveware (Feb. 1, 2021), https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020.

10. *See* Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

11. 2020 Internet Crime Report, *supra* note 4, at 19. It should also be noted that the IC3 report separates out other forms of fraud that are frequently used in BEC attacks, such as romance scams and spoofing, leading to the likelihood that the true number of BEC attacks is higher.

12. *Id.* at 20. For the same reason that the number of BEC attacks is probably much higher, the true cost of BECs is likely much higher. Crane Hassold, senior director of threat research at Agari, a leading email integrity protection company, stated that the 2020 IC3 report's statement that BECs account for "37% of all losses [was] an outrageous figure. Given the

fact that 'spoofing' is likely a subset of BEC, the total loss is close to $2.1 billion." Graham Cluley, *64 Times Worse Than Ransomware? FBI Statistics Underline the Horrific Cost of Business Email Compromise*, Tripwire (Mar. 18, 2021), https://www.tripwire.com/state-of-security/featured/fbi-statistics-underline-orrific-cost-of-business-email-compromise.

13. 2020 Internet Crime Report, *supra* note 4, at 20. As the report notes, this figure is likely very low. It does not include reports made directly to local FBI offices, nor did all IC3 complaints include dollar figures. Finally, the figure does not include estimates for lost business and ancillary costs.

14. This is not to say that ransomware isn't devastating—ransomware losses have been forecasted to top $20 billion globally. *See, e.g.*, Steve Morgan, *Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) by 2021*, Cybercrime Mag. (Oct. 21, 2019), https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021.

15. 2020 Internet Crime Report, *supra* note 4, at 20–21; Ponemon Inst., The 2021 Cost of Phishing Study (2021), https://www.proofpoint.com/sites/default/files/analyst-reports/pfpt-us-ar-ponemon-2021-cost-of-phishing-study.pdf.

16. Am. Int'l Grp. UK Ltd., Cyber Claims: GDPR and Business Email Compromise Drive Greater Frequencies (2019), https://www.aig.co.uk/content/dam/aig/emea/regional-assets/documents/aig-cyber-claims-2019.pdf.

17. Proofpoint, 2021 State of the Phish (2021), https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2021.pdf.

18. 2020 Internet Crime Report, *supra* note 4, at 24.

19. Proofpoint, *supra* note 17, at 2.

20. *See, e.g.*, Coalition, Coalition Cyber Insurance Claims Report (2020), https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2020-09-Coalition-Cyber-Insurance-Claims-Report-2020.pdf (documenting a 35% rise in BECs since the beginning of the pandemic).

21. *PPP FOIA*, U.S. Small Bus. Admin., https://data.sba.gov/dataset/ppp-foia (last updated Jan. 3, 2022).

22. *See, e.g.*, *Paycheck Protection Program Data*, FederalPay, https://www.federalpay.org/paycheck-protection-program (last visited Feb. 1, 2022); *see also Tracking PPP: Search Every Company Approved for Federal Loans*, ProPublica, https://projects.propublica.org/coronavirus/bailouts (last updated Nov. 30, 2021).

23. Press Release, U.S. Small Bus. Admin., SBA Loan Applicants Beware of Email Phishing Scams (Aug. 13, 2020), https://www.sba.gov/about-sba/sba-newsroom/press-releases-media-advisories/sba-loan-applicants-beware-email-phishing-scams; Sergiu Gatlan, *Phishing Campaign Lures US Businesses with Fake PPP Loans*, BleepingComputer (Feb. 1, 2021), https://www.bleepingcomputer.com/news/security/phishing-campaign-lures-us-businesses-with-fake-ppp-loans; *see also* FinCEN, FIN-2020-A003, Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19) (2020), https://www.fincen.gov/sites/default/files/advisory/2020-07-07/Advisory_%20Imposter_and_Money_Mule_COVID_19_508_FINAL.pdf.

24. Seth Orkand, *DOJ Warns of Business Email Compromise Scheme Targeted at PPP Loan Recipients*, Robinson & Cole LLP (Jan. 19, 2021), https://www.dataprivacyandsecurityinsider.com/2021/01/doj-warns-of-business-email-compromise-scheme-targeted-at-ppp-loan-recipients.

25. Cybersecurity Insiders, 2021 Business Email Compromise Report (2021), https://info.greathorn.com/hubfs/Reports/2021-Business-Email-Compromise-Report-GreatHorn.pdf.

26. *Id.*

27. *Id.*

28. *See* Proofpoint, *supra* note 17; *see also* Press Release, Fed. Bureau of Investigation, FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic (Apr. 6, 2020), https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic.

29. *See, e.g.*, Press Release, Manhattan Dist. Att'y's Off., D.A. Vance, NYPD Take Down $2.8 Million Business Email Compromise Scam, Offer Prevention Tips and Tools (May 30, 2019), https://web.archive.org/web/20210414054915/https://www.manhattanda.org/d-a-vance-nypd-take-down-2-8-million-business-email-compromise-scam-offer-prevention-tips-and-tools. The author was responsible for the prosecution of this matter.

30. Emma Fletcher, *Scams Starting on Social Media Proliferate in Early 2020*, Fed. Trade Comm'n (Oct. 21, 2020), https://www.ftc.gov/news-events/blogs/data-spotlight/2020/10/scams-starting-social-media-proliferate-early-2020.

31. Nathaniel Popper, *A Job That Isn't Hard to Get in a Pandemic: Swindlers' Unwitting Helper*, N.Y. Times (Sept. 15, 2020), https://www.nytimes.com/2020/09/15/technology/money-mules-fraud-pandemic.html.

32. 2020 Internet Crime Report, *supra* note 4, at 10.

33. There is a growing industry of firms that offer cryptocurrency tracing capabilities. These companies, including Chainalysis, Elliptic, and TRM Labs, to name but a few, rely on proprietary algorithms to both trace transactions across the blockchain and to assign recipient addresses to known exchanges, businesses, markets, and nation-states, if possible. In turn, investigators can obtain account information from established exchanges and businesses that have know-your-customer (KYC) requirements under applicable law. However, there are entire markets and exchanges devoted to avoiding these KYC requirements.

34. Panna Kemenes, *Can a Wire Transfer Be Reversed?*, Wise (Mar. 30, 2021), https://wise.com/us/blog/can-a-wire-transfer-be-reversed; *see also* Zack Needles, *BofA Denies Liability for Wire Transfer after Law Firm "Took the Bait" in Phishing Scam*, Law.com (June 29, 2018), https://www.law.com/thelegalintelligencer/2018/06/29/bofa-denies-liability-for-wire-transfer-after-law-firm-took-the-bait-in-phishing-scam. The lawsuit was dismissed in its entirety on November 13, 2018.

35. *Business E-Mail Compromise—An Emerging Global Threat*, Fed. Bureau of Investigation (Aug. 28, 2015), https://www.fbi.gov/news/stories/business-e-mail-compromise.

36. *See id.*; *see also* Agari Data, Inc., The Geography of BEC: The Global Reach of the World's Top Cyber Threat (2020), https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-geography-of-bec.pdf; Peter Renals, *SilverTerrier—Nigerian Business Email Compromise*, Unit 42 (Oct. 7, 2021), https://unit42.paloaltonetworks.com/silverterrier-nigerian-business-email-compromise.

37. *See, e.g.*, Brian Krebs, *Spy Service Exposes Nigerian "Yahoo Boys,"* Krebs on Sec. (Sept. 9, 2013), https://krebsonsecurity.com/2013/09/spy-service-exposes-nigerian-yahoo-boys.

38. These statistics are based on an analysis of over 9,000 engagements between May 2019 and July 2020, with the majority of BECs found in just five states: California, Florida, Georgia, New York, and Texas. Agari, The Geography of BEC, *supra* note 36, at 2.

39. Agari Data, Inc., Exaggerated Lion: How an African Cybercrime Group Leveraged G Suite and a Check Mule Network to Build a Prolific BEC Operation (2020), https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-exaggerated-lion.pdf.

40. *See* Agari, The Geography of BEC, *supra* note 36, at 2, 9.

41. Renals, *supra* note 36.

42. *Id.*; *see also* Agari Data, Inc., Scattered Canary: The Evolution and Inner Workings of a West African Cybercriminal Startup Turned BEC Enterprise (2019), https://agari.com/cyber-intelligence-research/whitepapers/scattered-canary.pdf; Agari Data, Inc., Silent Starling: BEC to VEC—The Emergence of Vendor Email Compromise (2019), https://www.agari.com/cyber-intelligence-research/whitepapers/silent-starling.pdf.

43. For a more detailed look, the Nigerian Economic and Financial Crimes Commission (EFCC) maintains an active Twitter account that documents recent law enforcement efforts in this sphere. *See* EFCC Nigeria (@officialEFCC), Twitter, https://twitter.com/officialefcc (last visited Feb. 1, 2022).

44. Press Release, U.S. Att'y's Off. Cent. Dist. of Cal., Nigerian National Brought to U.S. to Face Charges of Conspiring to Launder Hundreds of Millions of Dollars from Cybercrime Schemes (July 3, 2020), https://www.justice.gov/usao-cdca/pr/nigerian-national-brought-us-face-charges-conspiring-launder-hundreds-millions-dollars.

45. Hushpuppi, Instagram, https://www.instagram.com/hushpuppi (last visited Feb. 1, 2022).

46. Criminal Complaint by Telephone or Other Reliable Electronic Means, *United States v. Abbas,* No. 2:20-mj-02992 (C.D. Cal. June 25, 2020), https://www.justice.gov/usao-cdca/press-release/file/1292066/download.

47. Abbas had not yet been sentenced as of October 7, 2021.

48. *Medidata Sols., Inc. v. Fed. Ins. Co.,* 268 F. Supp. 3d 471, 476 (S.D.N.Y. 2017). Courts have split on this question. *See Medidata Sols., Inc. v. Fed. Ins. Co.,* 729 F. App'x 117 (2d Cir. 2018) (affirming the district court's holding that a BEC was the direct cause of loss and therefore triggered the insurance policy's computer fraud provision); *see also Childrens Place, Inc. v. Great Am. Ins. Co.,* No. 18-11963, 2019 U.S. Dist. LEXIS 70109 (D.N.J. Apr. 25, 2019) (relying in part on *Medidata* and finding that the policy's computer fraud provision similarly applied, but declining to decide on the insurer's direct causation argument as premature); *cf. Sanderina, LLC v. Great Am. Ins. Co.,* No. 2:18-cv-00772, 2019 U.S. Dist. LEXIS 154760 (D. Nev. Sept. 11, 2019) (finding that a spoofed email sent to a company employee from what appeared to be the company's owner did not constitute an "entry into" the computer system); *Taylor & Lieberman v. Fed. Ins. Co.,* 681 F. App'x 627 (9th Cir. 2017).

49. *See Apache Corp. v. Great Am. Ins. Co.,* 662 F. App'x 252 (5th Cir. 2016) (ruling for the insurer where a number of additional steps were taken to perpetuate the fraud, including multiple phone calls and the invitation of the spoofed emails).

50. *See Ryeco, LLC v. Selective Ins. Co.,* No. 20-3182, 2021 U.S. Dist. LEXIS 91186 (E.D. Pa. May 13, 2021).

51. *See Childrens Place*, 2019 U.S. Dist. LEXIS 70109, at *13–14.

52. *Virtu Fin. Inc. v. Axis Ins. Co.,* No. 20-CV-6293, 2021 U.S. Dist. LEXIS 163875, at *3 (S.D.N.Y. Aug. 30, 2021).

53. *See Taylor & Lieberman*, 681 F. App'x at 629; *see also Miss. Silicon Holdings, L.L.C. v. Axis Ins. Co.,* 843 F. App'x 581, 584–85 (5th Cir. 2021).

54. *See Medidata Sols., Inc. v. Fed. Ins. Co.,* 729 F. App'x 117, 119 (2d Cir. 2018); *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.,* 895 F.3d 455, 463 (6th Cir. 2018).

55. *See, e.g.*, *Virtu*, 2021 U.S. Dist. LEXIS 163875, at *5; *Medidata*, 729 F. App'x at 117; *Miss. Silicon*, 843 F. App'x at 583.

56. *See, e.g., Arrow Truck Sales, Inc. v. Top Quality Truck & Equip., Inc.,* No. 8:14-cv-2052, 2015 U.S. Dist. LEXIS 108823 (M.D. Fla. Aug. 18, 2015).

57. *See id.* at *15; *J.F. Nut Co. v. San Saba Pecan Exps. Corp.*, No. 1:17-cv-00405, 2018 U.S. Dist. LEXIS 226743, at *9 (W.D. Tex. 2018); Be*au Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc.,* 759 F. App'x 348, 353 (6th Cir. 2018); *Jetcrete N. Am. LP v. Austin Truck & Equip., Ltd.,* 484 F. Supp. 3d 915, 919 (D. Nev. 2020).

58. *Arrow*, 2015 U.S. Dist. LEXIS 108823, at *15; *Jetcrete*, 484 F. Supp. 3d at 919.

59. *See, e.g.*, *Arrow*, 2015 U.S. Dist. LEXIS 108823, at *15; *Beau Townsend*, 759 F. App'x at 359; *Bile v. RREMC, LLC,* No. 3:15-cv-051, 2016 U.S. Dist. LEXIS 113874 (E.D. Va. Aug. 24, 2016).

60. *See Peeples v. Carolina Container, LLC,* No. 4:19-cv-21, 2021 U.S. Dist. LEXIS 176076, at *16–21 (N.D. Ga. Sept. 16, 2021) (hesitating to apply the UCC's framework in a breach of contract claim due to BEC matter, while finding that the terms of the agreement itself dictated liability); *2 Hail, Inc. v. Beaver Builders, LLC,* No. 2016CV32847, 2017 Colo. Dist. LEXIS 1294 (Nov. 29, 2017) (declining to impose a UCC-inspired legal analysis framework and finding for the party who did not receive the expected wire transfer).

61. *See, e.g., Deutsche Bank Nat'l Tr. Co. v. Buck,* No. 3:17-cv-833, 2019 U.S. Dist. LEXIS 54774 (D. Va. Mar. 29, 2019); *Curry v. Schletter Inc.,* No. 1:17-cv-0001, 2018 U.S. Dist. LEXIS 49442 (W.D.N.C. Mar. 26, 2018).

62. *A BEC Scam Leads to a Healthcare Data Breach*, Panda Sec. (Feb. 17, 2020), https://www.pandasecurity.com/en/mediacenter/news/bec-scam-medical-center.

63. *See, e.g., McGlenn v. Driveline Retail Merch., Inc.,* No. 18-cv-2097, 2021 U.S. Dist. LEXIS 179775 (C.D. Ill. Sept. 21, 2021) (holding that neither a duty to safeguard nor a fiduciary duty existed under state law).

64. *See, e.g.*, *In re* Experian Data Breach Litig., No. 8:15-cv-01592, 2019 U.S. Dist. LEXIS 81243 (C.D. Cal. 2019); *In re* Home Depot, Inc., Customer Data Sec. Breach Litig., No. 1:14-MD-2583, 2016 U.S. Dist. LEXIS 65111 (N.D. Ga. May 17, 2016).

65. *See, e.g.*, *Experian*, 2019 U.S. Dist. LEXIS 81243; *Home Depot*, 2016 U.S. Dist. LEXIS 65111.

66. *See, e.g.*, *Experian*, 2019 U.S. Dist. LEXIS 81243; *Home Depot*, 2016 U.S. Dist. LEXIS 65111; *In re* Arby's Rest. Grp. Litig., No. 1:17-CV-0514, 2018 U.S. Dist. LEXIS 131140, at *22 (N.D. Ga. Mar. 5, 2018).

67. *See McGlenn*, 2021 U.S. Dist. LEXIS 179775, at *25–26; *Pena v. Brit. Airways, PLC (UK),* 849 F. App'x 13, 14 (2d Cir. 2021); *McMorris v. Carlos Lopez & Assocs., LLC,* 995 F.3d 295, 303 (2d Cir. 2021).

68. *See, e.g.*, California Consumer Privacy Act (CCPA), Cal. Civ. Code. § 1798.150(a)(1); New York SHIELD Act, N.Y. Gen. Bus. Law § 899-aa(6)(a); *see also* Press Release, N.Y. State Att'y Gen., Attorney General James Gets Dunkin' to Fill Holes in Security, Reimburse Hacked Customers (Sept. 15, 2020), https://ag.ny.gov/press-release/2020/attorney-general-james-gets-dunkin-fill-holes-security-reimburse-hacked-customers.

69. *See, e.g.*, *Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act")*, N.Y. Att'y Gen., https://ag.ny.gov/internet/data-breach (last visited Feb. 1, 2022); *Data Security Breach Reporting*, State of Cal. Dep't of Just., https://oag.ca.gov/privacy/databreach/reporting (last visited Feb. 1, 2022).

70. *See, e.g.*, Ohio Rev. Code Ann. § 1349.19(A)(7)(a)(iii); Tex. Bus. & Com. Code Ann. § 521.002(a)(2)(A).

71. *See* Safeguards Rule, 17 C.F.R. § 248.30(a) (Rule 30(a) of Regulation S-P).

72. Press Release, U.S. Sec. & Exch. Comm'n, SEC Announces Three Actions Charging Deficient Cybersecurity Procedures (Aug. 30, 2021), https://www.sec.gov/news/press-release/2021-169.

73. 15 U.S.C. §§ 6801, 6809(4).

74. 42 U.S.C. § 17932.

75. Proofpoint, *supra* note 17.

76. The website thispersondoesnotexist.com, for instance, displays daily a picture of a hyperrealistic but nonexistent person who was stitched together digitally using publicly available photos on the internet.

77. Eur. Parliamentary Rsch. Serv., Tackling Deepfakes in European Policy (2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf.

78. *Deepfakes: The Future of Phishing*, Egress (June 28, 2021), https://www.egress.com/en-us/blog/deepfakes-future-of-phishing.

79. *See* Aurelien Breeden, *Defense Minister Was on the Line, Asking for Millions to Aid France. Or Was He?*, N.Y. Times (Feb. 4, 2020), https://www.nytimes.com/2020/02/04/world/europe/france-Jean-Yves-Le-Drian-fraud.html; Hugh Schofield, *The Fake French Minister in a Silicone Mask Who Stole Millions*, Guardian, June 20, 2019.

80. Aurelien Breeden, *Paris Court Convicts 6 in $50 Million Fake-Identity Scheme*, N.Y. Times (Mar. 11, 2020), https://www.nytimes.com/2020/03/11/world/europe/france-identity-fraud-le-drian.html.

81. Thomas Brewster, *Fraudsters Cloned Company Director's Voice in $35 Million Bank Heist, Police Find*, Forbes (Oct. 14, 2021), https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions.

82. Melanie Maynes, *One Simple Action You Can Take to Prevent 99.9 Percent of Attacks on Your Accounts*, Microsoft (Aug. 20, 2019), https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks.