43. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….
- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[1]

44. To prevent and detect cyber-attacks attacks Defendant could and should have

[1] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at:* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Nov. 11, 2021).

implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> **Secure internet-facing assets**
>
> - Apply latest security updates
> - Use threat and vulnerability management
> - Perform regular audit; remove privileged credentials;
>
> **Thoroughly investigate and remediate alerts**
>
> - Prioritize and treat commodity malware infections as potential full compromise;
>
> **Include IT Pros in security discussions**
>
> - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
>
> **Build credential hygiene**
>
> - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;
>
> **Apply principle of least-privilege**
>
> - Monitor for adversarial activities
> - Hunt for brute force attempts
> - Monitor for cleanup of Event Logs
> - Analyze logon events;
>
> **Harden infrastructure**
>
> - Use Windows Defender Firewall
> - Enable tamper protection
> - Enable cloud-delivered protection
> - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[2]

[2] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 11, 2021).

45. Upon information and belief, Defendant also transmitted and stored unencrypted PII in employee emails, a grossly negligent act.

46. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyber-attacks.

47. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent what appears to be an email phishing attack (which is the most common and easily thwarted form of cyberattack), resulting in the Data Breach and the exposure of the PII of an undisclosed amount of current and former consumers, including Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members

48. Defendant acquired, collected, and stored the PII of Plaintiff and Class Members.

49. Defendant retains and stores this information, and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to perform its tax and business services.

50. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

51. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

52. Defendant could have prevented this Data Breach by instituting policies and practices not to transmit or store unencrypted PII in employee email account, or by properly

securing and encrypting the emails, files and file servers containing the PII of Plaintiff and Class Members.

53. Defendant's policies on its website include promises and legal obligations to maintain and protect PII, demonstrating an understanding of the importance of securing PII. In fact, GWLM's website unequivocally states that:

> Security is very important to us. We don't just consider security on our end, we think about yours as well.
>
> We send all sensitive documentation through Citrix ShareFile to ensure the information is sent to your securely. We also encourage our clients to do the same when sending files to use.[3]

54. Defendant also has adopted a Privacy Policy that details specific privacy obligations and promises to its customers, including Plaintiff and Class Members.[4]

55. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

56. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

This Email Phishing Attack Was Completely Foreseeable.

57. While Defendant has been purposefully vague about the mechanism of this cyberattack, upon information and belief, this Data Breach occurred as the result of a targeted email phishing attack. The targeted email phishing attack against Defendant was completely foreseeable.

58. According to Verizon, over 90% of all cybersecurity attacks that result in a data

[3] https://www.gwlmcpa.com/custom7.php (last accessed March 22, 2022)
[4] https://www.gwlmcpa.com/privacy.php (last accessed March 22, 2022)

breach start with a phishing attack.[5]

59. "Phishing is a cyber-attack that uses disguised email as a weapon. In simple terms, phishing is a method of obtaining personal information using deceptive e-mails and websites. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment."[6] The fake link will typically mimic a familiar website and require the input of credentials. Once input, the credentials are then used to gain unauthorized access into a system.

60. Phishing attacks are among the oldest, most common, and well known form of cyberattack. "It's one of the oldest types of cyberattacks, dating back to the 1990s" and one that every organization with an internet presence is aware."[7] It remains the "simplest kind of cyberattack and, at the same time, the most dangerous and effective."[8]

61. Phishing attacks are well understood by the cyber-protection community and are generally preventable with the implementation of a variety of proactive measures such as

---

[5] *Verizon Says Phishing Drives 90% of Cybersecurity Breaches*, Graphus (Jan. 21, 2020), https://www.graphus.ai/verizon-says-phishing-still-drives-90-of-cybersecurity-breaches/.

[6] Josh Fruhlinger, *What is Phishing? How This Cyber-Attack Works and How to Prevent It*, CSO Online (Sept. 4, 2020), https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

[7] *What is phishing? How this cyber attack works and how to prevent it*, CSO Online, February 20, 2020, https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html (last visited October 28, 2020).

[8] *Phishing*, Malwarebytes, https://www.malwarebytes.com/phishing/ (last visited October 28, 2020).

sandboxing inbound e-mail[9], inspecting and analyzing web traffic, penetration testing[10], and employee education, among others.

62. As a sophisticated commercial entity that collects and stores a plethora of PII, an email phishing attack, and the potential harms arising therefrom, was reasonably foreseeable to Defendant.

Defendant Knew or Should Have Known of the Risk Because the Accounting Sector is Particularly Susceptible to Cyber Attacks

63. Defendant knew and understood unprotected or exposed PII in the custody of accounting firms such as Defendant is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access, as accounting firms maintain highly sensitive PII, including Social Security numbers and financial information.

64. Moreover, it has been well-reported that the banking/credit/financial services industry is one of the most "at-risk" industries when it comes to cybersecurity attacks.[11] Attacks against the financial sector increased 238% globally from the beginning of February 2020 to the end of April, with some 80% of financial institutions reporting an increase in cyberattacks, according to cyber security firm VMware.

---

[9] Sandboxing is an automated process whereby e-mail with attachments and links are segregated to an isolated test environment, or a "sandbox," wherein a suspicious file or URL may be executed safely.

[10] Penetration testing is the practice of testing a computer system, network, or web application to find security vulnerabilities that an attacker could exploit. The main objective of penetration testing is to identify security weaknesses. Penetration testing can also be used to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incident. The primary goal of a penetration test is to identify weak spots in an organization's security posture, as well as measure the compliance of its security policy, test the staff's awareness of security issues and determine whether -- and how -- the organization would be subject to security disasters. *See* https://searchsecurity.techtarget.com/definition/penetration-testing (last visited October 28, 2020).

[11] *See, e.g.,* https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/financial-services-risk-cyber.html.

Value of Personally Identifiable Information

65. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[12] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[13]

66. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, Personal Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16]

67. Social Security numbers, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

---

[12] 17 C.F.R. § 248.201 (2013).
[13] *Id*.
[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Jan. 19, 2022).
[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Jan 19, 2022).
[16] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Jan. 19, 2022).

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[17]

68. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

69. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[18]

70. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number, addresses, and financial information.

71. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information,

---

[17] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 19, 2022).

[18] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Jan. 19, 2022).

personally identifiable information and Social Security numbers are worth more than 10x on the black market."[19]

72. Among other forms of fraud, identity thieves may use Social Security numbers to obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

73. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[20]

74. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you.
>
> Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[21]

75. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless

---

[19] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Nov. 11, 2021).

[20] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed July 20, 2021).

[21] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?"* (October 24, 2018) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last accessed July 20, 2021).

piece of information to lose if it happens in isolation."[22] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[23]

76. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[24]

77. The fraudulent activity resulting from the Data Breach may not come to light for years.

78. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

79. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, driver's license numbers, and financial account information, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached,

---

[22] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed July 20, 2021).
[23] *Id.*
[24] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed July 20, 2021).

[25] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 19, 2022).