IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JEONG-SU KIM, HUE-SOUNG JUN, and JONG MIN LEE on behalf of themselves and all others similarly situated, Plaintiffs, v. McDONALD'S USA, LLC, a Delaware limited liability company, and McDONALD'S CORPORATION, a Delaware corporation, Defendants.	Civil Action No.: JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Jeong-Su Kim, Hue-Soung Jun, and Jong Min Lee, individually and on behalf of all others similarly situated, bring this action against Defendants McDonald's USA, LLC and McDonald's Corporation (collectively, "McDonald's" or "Defendants") seeking statutory damages and injunctive relief for the Class defined below. Plaintiffs make the following allegations upon information and belief except as to their own actions.

NATURE OF THE ACTION

1. This class action arises out of the April 15, 2021, data hack and data breach ("Data Breach") of McDonald's that the company announced in June of 2021, whereby delivery customers' ("Customers") addresses, phone numbers, and e-mail addresses ("Personal Information") were stolen by attackers. Plaintiffs provided this data to Defendants with the

expectation that Defendants would manage, maintain, and secure this data in full compliance with all applicable laws and regulations. They did not. As a result of the Data Breach, Plaintiffs and thousands of other Class Members suffered losses in the form of the value of their time, anxiety, mental and emotional distress reasonably incurred to investigate, remedy, prevent, or mitigate the effects of the attack. Additionally, Plaintiffs' and Class Members' Personal Information, which was entrusted to Defendants, its officials, and agents, was compromised and unlawfully accessed as a result of the Data Breach.

2. Plaintiffs bring this class action lawsuit on behalf of themselves and those similarly situated, in order to: (1) seek redress for Defendants' inadequate safeguarding of Class Members' Personal Information, which Defendants collected and maintained; (2) remedy Defendants' failure to provide Plaintiffs and Class Members timely notice that their Personal Information had been subject to the unauthorized access and acquiring by an unknown third-party; and (3) obtain all other relief from Defendants' unlawful conduct relating to the Data Breach.

3. Defendants maintained the Personal Information in a reckless manner, including by failing to safeguard Personal Information against cyberattacks and by not securing and/or encrypting the files containing this data. In particular, the Plaintiffs' Personal Information was maintained in a non-encrypted file on Defendants' servers in a condition vulnerable to cyberattacks. Despite the lack of encryption of the files containing the Personal Information, Defendants failed to take steps necessary to secure the Personal Information from potential cyberattacks and other risks.

4. Furthermore, Defendants and their employees: (a) failed to properly monitor their network and server that contained the Personal Information, (b) failed to implement appropriate steps to ensure that the Personal Information was secured, and (c) failed to implement and/or

execute appropriate policies to notify Plaintiffs and Class Members promptly when the Data Breach occurred. In fact, in the e-mailed notice of the Data Breach, Defendants state that they inspected their "vulnerable" servers and implemented security measures. Had these changes been in place prior to the attack, this incident would not have happened, and Plaintiffs' and Class Members' Personal Information would not have been hacked or wrongfully obtained by cybercriminals.

5. Defendants have yet to provide any information to Plaintiffs and Class Members about the identities of those who accessed and wrongfully obtained the Personal Information. Nor have they provided any confirmation that the wrongfully-obtained Personal Information is no longer in the cybercriminals' hands.

6. Cybercriminals, data thieves, and hackers are also able to register for almost all website subscriptions, exposing the owner of the e-mail address to countless spam and/or unwanted advertising e-mails. In addition to spam e-mails, Plaintiffs and Class Members are also exposed to unwanted solicitations and phishing attempts.[1]

7. Given the fact that the hacked phone numbers are tied to Plaintiffs' and Class Members' names and addresses, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of phishing scams.

8. Plaintiffs and all other Class Members, at their own cost, must now and in the future expend time and effort to closely monitor their accounts to guard against phishing scams and identity theft.

[1] As used herein, the term "phishing" refers to the fraudulent practice of sending e-mails purporting to be from reputable companies or individuals in order to induce recipients to reveal personal information, such as passwords and credit card numbers.

9. In addition, Plaintiffs and those similarly situated have expended time and effort contacting Defendants to understand the extent of the Data Breach, remove and deregister their account information with Defendants, monitor their e-mail addresses to remove or prevent unwanted e-mails, and/or remove and deregister their account information with websites accessed by cybercriminals.

10. Defendants' conduct has directly and proximately caused economic and non-economic damages, invasion of privacy, and deprivation of the exclusive use and control of individuals' own personal information. Furthermore, Defendants' conduct has affected Plaintiffs' and Class Members' ability to fully protect themselves from fraud.

11. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly-situated individuals, whose Personal Information was accessed during the Data Breach.

12. Plaintiffs seek relief including, but not limited to, statutory damages and injunctive relief including improvements to Defendants' data security systems.

13. Accordingly, Plaintiffs bring this action against Defendants seeking redress for their unlawful conduct, and asserting claims for: (a) violations of The Consumer Fraud And Deceptive Business Practices Act ("Consumer Fraud Act") (815 Illinois Compiled Statutes 505/1 *et seq.*); (b) violations of The Uniform Deceptive Trade Practices Act ("UDTPA") (815 Illinois Compiled Statutes 510/1 *et seq.*); and (c) Korea's Personal Information Protection Act ("PIPA").

PARTIES

14. Plaintiff Jeong-Su Kim is, and at all times relevant hereto was resident in the Republic of Korea ("Korea"). Mr. Kim has been a customer of Defendants. Mr. Kim, at all relevant times, maintained a McDonald's account using his Personal Information in order to place

McDonald's delivery orders. After various news outlets reported the Data Breach, Mr. Kim learned that his Personal Information had been stolen and that Defendants failed to adequately safeguard and protect his Personal Information. In response, Mr. Kim took several actions, including but not limited to, contacting the McDonald's Customer Service Center about the exponential increase in the number of unwanted spam e-mails from foreign companies he had been receiving since the Data Breach. In response to Mr. Kim, on July 29, 2021, McDonald's stated that when it became aware of the unauthorized access to its servers, McDonald's assessed and strengthened its "weak" security measures.

15. Plaintiff Hue-Soung Jun is, and at all times relevant hereto was resident in Korea. Mr. Jun has been a customer of Defendants. Mr. Jun, at all relevant times, registered for a McDonald's account using his Personal Information in order to place McDonald's delivery orders. After various news outlets reported the Data Breach, Mr. Jun learned that his Personal Information had been stolen and that Defendants failed to adequately safeguard and protect his Personal Information. Since the Data Breach, Mr. Jun has been receiving constant notifications of unauthorized e-mail log-in attempts in Japan. Furthermore, even though Mr. Jun's McDelivery account was to be deleted after not being in use for over one year pursuant to McDonald's Privacy Policy discussed below, McDonald's informed Mr. Jun that due to a "serious internal error [within McDonald's], his personal information was leaked" during the Data Breach. For this reason, Mr. Jun was forced to spend time preparing and filing a police report regarding the Data Breach, as well as deal with the unauthorized log-in attempts.

16. Plaintiff Jong Min Lee is, and at all times relevant hereto was resident in Korea. Mr. Lee has been a customer of Defendants. Mr. Lee, at all relevant times, registered for a McDonald's account using his Personal Information in order to place McDonald's delivery orders.

After various news outlets reported the Data Breach, Mr. Lee learned that his Personal Information had been stolen and that Defendants failed to adequately safeguard and protect his Personal Information. After the reported Data Breach, on August 13, 2021, Mr. Lee was subjected to attempted extortion (to which he had never been exposed prior to the Data Breach), in which Mr. Lee was requested to pay $1,700 by clicking and accessing a provided web link in exchange for deleting copies of Mr. Lee's personal files that the scammer claimed to have obtained by hacking a website with which Mr. Lee registered.

17. Defendant McDonald's USA, LLC is a citizen of Illinois. Defendant is a Delaware limited liability corporation with its principal place of business located at 110 North Carpenter Street, Chicago, Illinois. According to McDonald's USA, LLC's website, its executive leadership team comprises of Christopher J. Kempczinski, the Chief Executive Officer; Joe Erlinger, the President; Spero Droulias, Chief Financial Officer; Bill Garrett, Senior Vice President of U.S. Operations; Morgan Flatley, Chief Marketing and Digital Customer Experience Officer; Tiffanie Boyd, Senior Vice President and Chief People Officer; Mason Smoot, Senior Vice President and Chief Restaurant Officer; Angela Steele, General Counsel; Whitney McGinnis, Chief Information Officer and Vice President; Marion Gross, Senior Vice President and Chief Supply Chain Officer, North America; and Skye Anderson, West Zone President. Mr. Kempczinski, Mr. Erlinger, Mr. Droulias, Mr. Garrett, Ms. Flatley, Mr. Smoot, Ms. Steele, Ms. McGinnis, Ms. Gross, and Ms. Anderson are all citizens of Illinois. Ms. Boyd states in her McDonald's bio that while she currently resides in Minnesota, she and her family plan on relocating to Chicago. McDonald's USA, LLC is a wholly-owned subsidiary of McDonald's Corporation. On information and belief, McDonald's USA, LLC, in conjunction with McDonald's Corporation, manages, maintains, and provides

cybersecurity for the Personal Information of its Korean customers. Defendant regularly transacts business in the State of Illinois and the Northern District of Illinois, including Chicago.

18. Defendant McDonald's Corporation is a citizen of Illinois. Defendant is a publicly traded Delaware corporation with its principal place of business located at 110 North Carpenter Street, Chicago, Illinois. McDonald's Corporation manages, maintains, and provides cybersecurity for the Personal Information of its Korean customers. Defendant regularly transacts business in the State of Illinois and the Northern District of Illinois, including Chicago.

JURISDICTION AND VENUE

19. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000 and Plaintiffs, and other members of the proposed Class, are citizens of states other than Illinois or a foreign nation.

20. This Court has personal jurisdiction over this action because Defendants have sufficient contacts with this District by virtue of establishing their headquarters here, and further, they have purposefully availed themselves of the privilege of doing business in this District such that they could foresee litigation being brought in this District.

21. This Court also has original jurisdiction over this action pursuant to 28 U.S.C. § 1332(a), because the matter in controversy exceeds the sum or value of $75,000, exclusive of interests or costs, and is between "citizens of a State and citizens or subjects of a foreign State." 28 U.S.C. § 1332(a). The Court also has supplemental jurisdiction over the state law claim alleged herein pursuant to 28 U.S.C. § 1367.

22. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District. Defendants

are headquartered in this District, physical evidence relating to the Data Breach. Including documents and electronic data, will be found in this district, relevant employees and officers of Defendants are found in this District.

FACTUAL ALLEGATIONS

23. On June 11, 2021, the *Wall Street Journal* ("WSJ") reported that McDonald's Corporation announced that "hackers stole some data from its systems in markets including the U.S., South Korea, and Taiwan, . . . [including but not limited to] customer emails, phone numbers and addresses for delivery customers in South Korea and Taiwan."

24. In the WSJ article, Defendants stated that "the unauthorized access was cut off *a week after* it was identified[.]" (emphasis added).

25. Furthermore, the WSJ article reported that the Data Breach was "another example of cybercriminals infiltrating high-profile global companies" such as McDonald's.

26. On June 13, 2021, McDonald's published in Korea its Data Breach Public Notice on its web page ("Public Notice").

27. According to that Notice, a "file" containing McDelivery customers' e-mail addresses, phone numbers, and physical addresses were breached and obtained by unauthorized individuals. The Notice also states that Defendants inspected their "vulnerable" servers and implemented security measures after learning of the Data Breach. In addition, the Notice informed the public that McDonald's does not request credit card or other financial information through phone or e-mail. The Notice asked the public to be particularly cautious of voice phishing attempts and/or e-mail solicitation from entities impersonating McDonald's. It also notifies the public of a website that each affected customer can access to confirm that their Personal Information was breached in this Data Breach incident.

28. On June 19, 2021, McDonald's distributed a Data Breach E-mail Notice ("E-mail Notice") to individual customers affected by the Data Breach. This E-mail Notice included an almost identical message as the Public Notice to its affected customers, but McDonald's additionally apologizes to its affected customers for the delay in identifying and addressing the issues arising from the Data Breach after it was notified of the Data Breach incident.

29. Affected customers include many foreigners—U.S. citizens included—who visit Korea, register an account with McDelivery, and use the McDelivery mobile app and/or the website to order food for delivery. U.S. citizens residing in Korea include tens of thousands of members of the U.S. armed forces and their families, English language teachers, employees temporarily assigned to work in Korea, and other ex-patriots. More than a million Americans visited Korea in 2019. [2]

30. As more information was disclosed, it became apparent that the Data Breach also extended to customers and employees in Taiwan, as well as to the United States. McDonald's also notified some employees in South Africa and Russia of possible unauthorized access to their information.

31. Cybersecurity experts' reaction to the news of the Data Breach was swift.

32. One article stated that:

---

[2] *See Number of foreign tourists to hit record high in 2019*, https://www.koreatimes.co.kr/www/culture/2019/12/141_280829.html (last accessed August 27, 2021). *See, e.g., How do you enter an address for McDelivery?*, https://www.reddit.com/r/korea/comments/9b8bkl/how_do_you_enter_an_address_for_mcdelivery/ (last accessed August 20, 2021); *What apps do you frequently use in your daily life in Korea?*, https://www.reddit.com/r/Living_in_Korea/comments/jlis5e/what_apps_do_you_frequently_use_in_your_daily/ (last accessed August 20, 2021); *Could anyone help me translate mcdelivery.co.kr so I can order to my house?*, https://www.reddit.com/r/korea/comments/1orn0s/could_anyone_help_me_translate_mcdeliverycokr_so/ (last accessed August 20, 2021); *Having a typical foreigner quarantine crisis! Please help*, https://www.reddit.com/r/korea/comments/ihbc7i/having_a_typical_foreigner_quarantine_crisis/ (last accessed August 20, 2021).

> Ed Bishop, co-founder & CTO, Tessian, says, "Hackers will be quick to exploit the business contact details exposed in this breach, either simply selling the data or using the information to send convincing phishing, smishing or vishing attacks to victims of the breach. For example, cybercriminals could send phishing emails to individuals whose contact details were breached, asking them to click a link to update their username and password in the wake of the incident, in order to harvest credentials and gain access to data and systems. In a more advanced attack, the cybercriminal could use the knowledge that the contact has a business email relationship with McDonald's and impersonate the brand to create further legitimacy to the attack. With people's phone numbers being exposed too, cybercriminals could make their social engineering campaigns even more convincing by following up their email with a voice phishing — vishing — call."
>
> Bishop adds, "The warning for all McDonald's employees and franchisees, then, is to watch out for phishing emails and verify any requests for payments or information with the supposed source via another means of communication before complying with the request. No matter how urgent the message appears, always take a minute to check its legitimacy."
>
> ****
>
> Richard Blech, CEO, XSOC CORP., says, "This breach like so many of the others, is just plainly unacceptable given the universal awareness now about these cyber-attacks. What this says about the state of US infrastructure is that many of the large US enterprises have clearly not taken the necessary measures to stop these types of breaches. I would expect that we are going to find that there was human error involved somewhere in this McDonald's breach. And human error is usually the number one culprit. This is where large enterprises and government entities are significantly lacking in their efforts to ensure that they have, across the board, trained all staff and employees of, what should be a required job function, of the best practices and rules of conduct when operating within the network or infrastructure. Additionally, and this is the most surprising, is that there are a plethora of tools and resources to 'white hat' hack/test an environment to find all areas of exposure, even where human error could occur and then enterprises would be in position to better prevent breaches and not be put in the position to only reacting, after the fact."

33. Paul Bischoff, a Privacy Advocate at Comparitech, echoed these concerns:

> "McDonald's customers in Taiwan and South Korea who have given the company their contact information at any point should be on the lookout for phishing emails. Scammers will send emails and texts posing as McDonald's or a related company, using personal data from the breach to personalize messages and make them more convincing. These messages will most likely instruct victims to click on a malicious link that either downloads malware or goes to a fake website. The website will ask victims for their login or payment information, which is then stolen by the attackers."

34. McDonald's attempted to defend its conduct by asserting that it did a good job of discovering the Data Breach. One cybersecurity publication ridiculed this argument:

> "If McDonald's cybersecurity efforts were truly substantial, however, it wouldn't be reporting a data breach. Claiming that discovering a data breach is representative of good cybersecurity is certainly an interesting spin. There's no suggestion that ransomware was involved, but three different countries and different sorts of data stolen may suggest multiple attacks were involved.
>
> The recent cyberbreach at McDonald's is another example showing that every organization is a software organization," Jonathan Knudsen, technical evangelist at electronic design automation firm Synopsys Inc. (https://www.synopsys.com/), told SiliconANGLE.
>
> "Fast food? Oil pipeline? Global shipping? Every organization in every industry depends on software for critical business functions." As a result, he added, every organization in every industry must embrace a proactive approach to cybersecurity. "Without a security mindset in all parts of the organization, the risk of disaster is high," he said.
>
> Kate Kuehn, senior vice president of application relationship management company vArmour Networks Inc. (https://www.varmour.com/), noted that the data breach is a stark reminder that all organizations need to assume they have already been breached and adopt a zero-trust (https://siliconangle.com/2020/02/23/trust-nothing-breaches-mount-radical-approach-cybersecurity-gains-favor/) model of defense.
>
> "It's not a question of if, but when, organizations will need to respond/contain an incident, and real-time visibility and application relationship management is critical to attempt success." Kuehn said.

> John McClurg, senior vice president and chief information security officer at intelligent security firm BlackBerry Ltd. (https://www.blackberry.com/us/en), said the McDonald's breach also highlights the need for a "prevention-first" approach.
>
> "As diverse industries from gaming to the supply chain to local transportation face an unparalleled rise in cyberattacks, which are incredibly costly and are damaging reputations amongst consumers, humans and technology must work hand-in-hand to stay one step ahead to secure and protect critical data for the long term," McClurg said. "Implementing prevention-first AI-driven technology can enable organizations to stop data breaches and ransomware attacks before they execute."

35. Likewise, Jamie Akhtar, the COO and Co-Founder of CyberSmart, said of the Data Breach:

> "This recent data breach of McDonald's shows how critical it is for organisations to recognise that security is a matter of when, not if, and we should all take steps to implement a secure baseline - recognition really is the first step.
>
> Fortunately, there is no need to re-invent the wheel of your own security program. Start by aligning with the UK Government's guidelines. Think of it as an ongoing program rather than a project as well. Security should be embedded within the culture, and although most businesses are not likely to suffer highly sophisticated attacks, it's important to keep updated as the landscape shifts. For example, phishing has become increasingly popular and will likely impact employees and franchisees of McDonald's in the coming months now that their contact information is out in the open. The benefit of a holistic approach to cyber is not only that you can worry less but the next time a customer asks about your security, you can answer with confidence you're on top of it."

36. As a result of Defendants' failure to properly safeguard and protect the "file" containing Plaintiffs' and the Class Members' Personal Information, cybercriminals were able to access, obtain, and use their Personal Information without authorization, invading Plaintiffs' and the Class Members' privacy.

37. Furthermore, due to Defendants' failure to properly safeguard and protect their Personal Information, Plaintiffs and Class Members have had to and will continue to expend a significant amount of time and mental aggravation to protect their identities and other Personal Information by changing their phone numbers, contacting McDonald's to understand the extent of the privacy invasion, contacting McDonald's to remove records of their McDelivery accounts online and off-line, investigating websites from which they received spam e-mails in order to review whether their e-mail addresses were used to enroll in unwanted advertising e-mails, contacting websites to unsubscribe or deregister from their mailing list or website registrations, and monitoring calls and e-mails for phishing scams.

38. This recent incident was not the first time that McDonald's has suffered a data breach; it has a history of failing to maintain the privacy of personal data on its servers. Defendants experienced a similar if not identical failure to safeguard McDelivery users' Personal Information almost four years ago, in 2017. Due to Defendants' poor security measures, more than 2.2 million McDelivery users' personal information in India was breached.

39. According to one BBC.com article, "a poorly configured server gave anyone access to the names, emails, home addresses and phone numbers of users."

40. *Cybersecurity Insiders* also reported the 2017 McDonald's data breach and stated that "the leak could prove disastrous if cyber crooks use the data to access financial details of users, including their credit card info and e-wallet details."

41. Furthermore, a cybersecurity firm called Fallible which broke the news of the 2017 McDonald's data breach to the media announced that despite reporting that "McDelivery is leaking personal data for more than 2.2 million of its users" to McDonald's on February 4, 2017, it still had not received any response from McDonald's on March 18, 2017, the day Fallible disclosed

the data breach to the public. Fallible also noted in its announcement that despite its report, McDelivery users were still vulnerable over a month and a half after Fallible's report to McDonald's.

42. Also in 2017, it was reported that McDonald's Canada's career site exposed the personal data of 95,000 applicants seeking jobs at the restaurant since 2014. Applicants' names, home and e-mail addresses, telephone numbers, employment histories and other "standard application information" were stolen.

43. As of August 2021, McDonald's security measures continue to remain lackluster. According to an UpGuard security ratings report, which generates a rating based on billions of data points each day, McDonald's rating is at B (741/850).

44. The costs and harms associated with such data breaches are immense. The FBI's Internet Crime Complaint Center reported that people lost $57 million to phishing schemes in one recent year.

45. Phishing scams are also prevalent in Korea, where Plaintiffs, and many of the Class Members reside. According to a November 16, 2020 article by the *Korea Herald*, eight members of a voice phishing ring were arrested for stealing around two billion won ($1.8 million) from approximately 200 South Koreans. As the article explained, "[t]he accused allegedly used customer information . . . such as name . . . and telephone number, and fooled customers into downloading a spy application developed by the hacker in an attempt to steal more information from them. They then then posed as bank or insurance firm employees and had victims send money to them."

46. Text messages to phone numbers are also used in phishing scams. According to another article in the *Korea Times* article, tens of thousands of people who fell victim to a voice

phishing scam clicked on a link that they received through a text message. The article also quotes the city government's department warning potential victims that clicking on such innocuous seeming links can allow hackers to access one's phone.

47. According to the Federal Trade Commission, "[p]hishing emails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store. Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice
- want you to click on a link to make a payment
- say you're eligible to register for a government refund
- offer a coupon for free stuff[.]"

48. The FTC's warning echoes the potential phishing scams to which Plaintiffs and the Class Members are at risk of being subject, as described by McDonald's in their Public Notice and the E-mail Notice. Plaintiffs and Class Members now have to spend time and effort to ensure that the Data Breach does not cause them further injury.

49. As a direct and/or proximate result of the McDonald's Data Breach, the criminal(s) and/or their customers now have Plaintiffs' and Class Members' Personal Information.

50. On August 13, 2021, shortly after the Data Breach, Plaintiff Lee received a phishing e-mail. The e-mail titled, "Your Smartphone," informs Mr. Lee that "a website with [his] account . . . was hacked." Then the e-mail states that as a result of this successful hacking attack, the author was able to "access Mr. Lee's password" and use the password to "extract Mr. Lee's cloud storage."

51. The e-mail also informs Mr. Lee that the author was able to download "personal photos, video files, conversations, documents, e-mails, contact information, search history, notes, social media records, and deleted files."

52. The author then states that they "found interesting photos and videos (as Mr. Lee must know what they mean) and assume that Mr. Lee's friends and colleagues would not simply think the photos and videos are 'interesting.'"

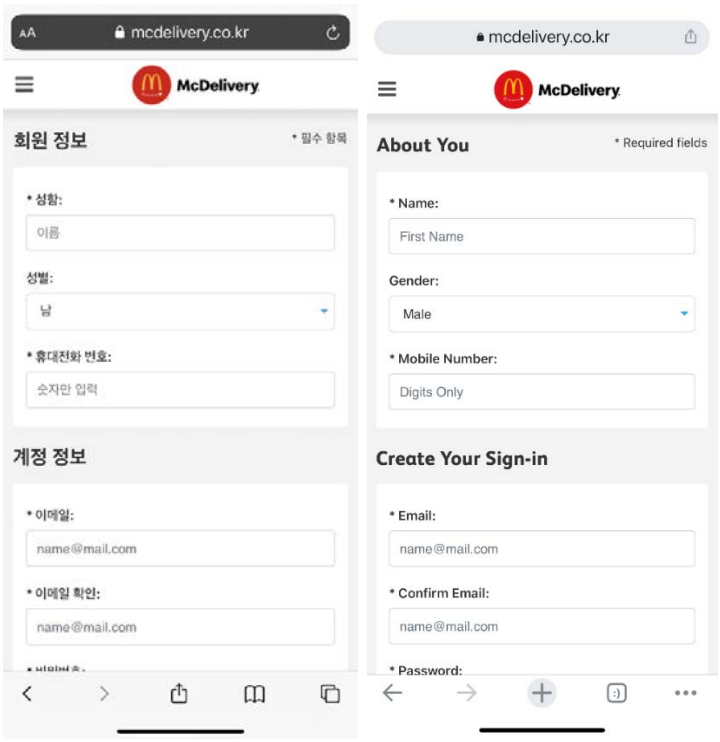
53. The author's threat continues by asking Mr. Lee to imagine what could happen if the hacked files—which according to the author are "very personal and inappropriate"—were leaked.

54. The author then provides a "solution" to Mr. Lee by asking Mr. Lee to wire a fee totaling $1,700 by clicking on a provided link within two days. According to the author, only then will they delete the files.

55. The author also alerts Mr. Lee to change his password.

56. Plaintiffs and Class Members registered for a McDelivery account to place an order for delivery of food while present in Korea through the McDonald's delivery mobile app or the McDonald's delivery website before the date of the Data Breach.

57. In order to place a delivery order through McDonald's delivery mobile app or McDonald's web site, Plaintiffs and Class Members were required to enter their addresses, e-mail addresses and cell phone numbers. Class Members can also store their credit card information or other payment information that allows for a faster and easier check-out if they choose to create an account via the website. Credit card information or other payment information that allows for a faster and easier check-out is stored if the McDelivery app is used.



58. As part of the registration process, customers are also required to agree to three of McDonald's terms and conditions, including its privacy policies.

59. As demonstrated above, the McDelivery registration process is available in both Korean and in English, catering to both Koreans and non-Koreans including U.S. citizens living in or visiting Korea.

60. In McDonald's Korean privacy policy, McDonald's notifies the customer that some of McDonald's customers' Personal Information—name, phone number, e-mail, address, and password—are sent to McDonald's Corporation and Amazon Web Services ("AWS"). In this privacy policy, McDonald's also states that cases where McDonald's customers' Personal Information is transmitted to McDonald's Corporation, the Personal Information is encrypted and secured.

61. Despite McDonald's representation that the Personal Information is encrypted and secured prior to being sent oversees to McDonald's Corporation in Illinois, during a phone call, a

McDonald's senior customer representative informed Plaintiff Kim that she was unable to confirm that his Personal Information was encrypted or secured when it was transferred to McDonald's Corporation's servers.

62. A Korean citizen affected by the Data Breach published a blog post about the effects of the Data Breach. In this blog post, the author posted screen shots of his inbox after the Data Breach that shows part of the thirty e-mails he received from Wish.com, a website of which the author did not know and had not previously visited.

63. In this blog, the author goes on to discuss the time he spent searching online for Wish.com and his discovery that the author's hacked e-mail address was used to create an account on Wish.com.

64. The author also noted that the country was set to Ukraine, and the currency was set to Ukrainian hryvnia (UAH).

65. After confirming that the author's hacked e-mail was used to create an account on Wish.com, the author then had to navigate Wish.com's website in order to deactivate the account.

66. Defendants' wrongful actions and/or inaction here directly and/or proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' Personal Information without their knowledge, authorization, and/or consent. As a further direct and/or proximate result of Defendants' wrongful actions and/or inaction, Plaintiffs and Class Members have suffered, and will continue to suffer, damages including, without limitation, lost time and expenses monitoring for phishing scams, removing accounts registered under the exposed e-mail addresses, removing unwanted spam e-mails from unfamiliar websites, and communicating with McDonald's to remedy the stolen Personal Information. All of this has caused Plaintiffs and Members of the Class anxiety, emotional distress, loss of privacy, and other harm.

67. To date, Defendants have not offered Plaintiffs and Class Members any compensation or direct personal protection from the Data Breach, including, for example, means to prevent phishing scams and/or identity theft insurance.

68. The Korean Personal Information Protection Act ("PIPA") explains that "[t]he purpose of this act is to protect the freedom and rights of individuals, and further, to realize the dignity and value of the individuals, by prescribing the processing and protection of personal information." A copy of an English version of PIPA is attached as Appendix A.

69. According to Article 2 of PIPA, the term "personal information" means any of the following information relating to a living individual: "(a) [i]nformation that identifies a particular individual by his or her full name, . . . (b) [i]nformation which, even if it by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual. In such cases, whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as [the] likelihood that the other information can be procured; . . .."

70. Under PIPA, the term "personal information controller" means "a public institution, legal person, organization, individual, etc. that processes personal information directly or indirectly to operate the personal information files as part of its activities[.]"

71. Article 34 of PIPA states that "[a] personal information controller shall notify data subjects of the following matters without delay when the personal information controller becomes aware their personal information has been divulged: 1. Particulars of the personal information divulged; 2. When and how personal information has been divulged; 3. Any information about how the data subjects can minimize the risk of damage from divulgence, etc.; 4. Countermeasures taken by the personal information controller and remedial procedure; 5. Help desk and contact

points for the data subjects to report damage." Despite the express requirements of Article 34, Defendants failed to notify Plaintiffs and Class Members "without delay . . . [p]articulars of the personal information divulged; [and w]hen and how personal information has been divulged[.]"

72. Defendants represented in their Public Notice and E-mail Notice that only the customers' phone numbers, addresses, and e-mail addresses were stolen by the hackers.

73. In the Public Notice and in the E-mail Notice, McDonald's simply states that it "recently" became aware of an unauthorized access to a "file" that contained the Personal Information.

74. Also, despite the fact that the Data Breach took place around April 15, 2021 as reported by the company, McDonald's did not notify its customers until approximately June 13, 2021, almost two months after the hacker's unauthorized access had been discovered. Even in its Public Notice and E-Mail Notice, McDonald's conceded and apologized for the "delay."

75. Furthermore, Article 39(3) of PIPA states that "[w]here a data subject suffers damage out of loss, theft, divulgence, forgery, alteration, or damage of his or her own personal information, caused by wrongful intent or negligence of a personal information controller, the Court may determine the amount of compensation for damage not exceeding three times such damage[.]"

76. Article 21 requires that "[a] personal information controller shall destroy personal information without delay when the personal information becomes unnecessary owing to the expiry of the retention period, attainment of the purpose of processing the personal information[.]"

77. According to Section 3 of McDonald's Privacy Policy, McDonald's promises its McDelivery users that it destroys and will destroy any and all Personal Information of users who do not use McDelivery for over a year.

78. Despite Article 21 of PIPA and Section 3 of McDonald's Privacy Policy, McDonald's failed to destroy Plaintiff Mr. Jun's Personal Information and even conceded to Mr. Jun that even though Mr. Jun's Personal Information was to be destroyed by McDonald's after over one year of non-use, Mr. Jun's Personal Information remained in McDonald's system and was subjected to the Data Breach due to a "serious internal error."

79. As a result of Defendants' breach of security (and negligence resulting in the breach) concerning the Personal Information of Plaintiffs and the Class, Plaintiffs and the Class suffered injury in fact. Further, with the prevalence and dangers of phishing scams recognized globally, monetary damages are imminent and likely. Defendants' wrongful actions and/or inaction here directly and/or proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' Personal Information without their knowledge, authorization, and/or consent. As a further direct and/or proximate result of Defendants' wrongful actions and/or inaction, Plaintiffs and Class Members have suffered, and will continue to suffer, damages including, without limitation, lost time, anxiety, emotional distress, loss of privacy, and other harm.

CLASS ACTION ALLEGATIONS

80. Plaintiffs repeat and reallege the allegations set forth above and incorporates them by reference.

81. Plaintiffs bring this action on their own behalf and on behalf of all other persons similarly situated pursuant to Fed. R. Civ. P. 23. The Class which Plaintiffs seek to represent is:

> All persons, regardless of where they reside, who registered for a McDelivery account to place an order for delivery of food while present in Korea through the McDonald's delivery mobile app or the McDonald's delivery website and whose Personal Information was

compromised in the April 15, 2021 Data Breach as announced by the company.

Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assignees of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

82. **Numerosity**. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of tens of thousands of persons whose data was compromised in the Data Breach. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the parties and the Court.

83. The rights of each Class Member were violated in a virtually identical manner as a result of Defendants' willful, reckless, and/or negligent actions and/or inaction.

84. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or improperly disclosed Plaintiff's and Class Members' Personal Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their Personal Information;

f. Whether Defendants breached their duty to Class Members to safeguard their Personal Information;

g. Whether computer hackers obtained Class Members' Personal Information in the Data Breach;

h. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

i. Whether Defendants' conduct was negligent or otherwise inconsistent with applicable laws and regulations;

j. Whether Defendants' conduct as described herein caused injury to Plaintiffs and the Class Members;

k. Whether Defendants failed to provide notice of the Data Breach in a timely manner, and

l. Whether Plaintiffs and Class Members are entitled to damages and/or injunctive relief.

85. **Typicality**. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

86. **Adequacy of Representation**. Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

87. **Predominance**. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members in that all the Plaintiffs' and Class Members' data was stored on the same server and unlawfully obtained in the same way. The common issues arising from Defendants' conduct affecting Class Members, as described herein, predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

88. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

89. The Class Members are ascertainable and can be ascertained and identified from, among other things, Defendants' records.

90. Defendants acted or refused to act on grounds generally applicable to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

FIRST CLAIM FOR RELIEF
VIOLATION OF THE CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT (CONSUMER FRAUD ACT)
(815 ILLINOIS COMPILED STATUTES 505/1 *et seq.*)
(On Behalf of Plaintiffs and All Class Members)

91. Plaintiffs re-allege and incorporate by reference the preceding paragraphs, as if fully set forth herein.

92. The Illinois Consumer Fraud and Deceptive Business Practices Act ("Consumer Fraud Act"), 815 ILCS 505/1 *et seq*. declares unlawful "any . . . false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, . . . in the conduct of any trade or commerce . . . whether any person has in fact been misled, deceived or damaged thereby."

93. In the Privacy Policy, Defendants represented to Plaintiffs and the Class Members that their Personal Information would be encrypted and/or securely maintained with McDonald's Corporation.

94. By requiring Plaintiffs and Class Members to agree to Defendants' Privacy Policy, Defendants intended Plaintiffs and the Class Members to rely on it. The Privacy Policy represented that Plaintiffs' and Class Members' Personal Information would be encrypted and/or secured by Defendants. Plaintiffs and Class Members were required to agree to Defendants' Privacy Policy in order to place food delivery orders through the McDelivery mobile app or the website.

95. Plaintiffs and Class Members relied on Defendants to encrypt and/or secure their Personal Information per the Privacy Policy.

96. Based upon a Class Member's phone conversation with a senior customer representative at McDonald's, Plaintiffs and the Class Members believe that McDonald's failed to encrypt Plaintiffs' and the Class Members' Personal Information or safeguard it, despite McDonald's express representation in the Privacy Policy.

97. Further, in the Privacy Policy, Defendants represent to its users that the users' Personal Information would be destroyed after one year of non-use.

98. Because Plaintiff Jun's account with McDelivery was inactive for over one-year, McDonald's was required to destroy his Personal Information pursuant to the Privacy Policy.

99. However, after the Data Breach, McDonald's informed Plaintiff Jun that McDonald's failed to destroy his Personal Information despite McDonald's representation in the Privacy Policy. McDonald's conceded to Plaintiff Jun that due to a "serious internal error [within McDonald's] his personal information was leaked" during the Data Breach.

100. Plaintiffs and Class Members were (and continue to be) damaged as a direct and/or proximate result of Defendants' misrepresentation that Plaintiffs' and Class Members' Personal Information would be encrypted and maintained securely in the form of, *inter alia*, time spent contacting McDonald's to assess the extent of the Data Breach, time spent changing passwords to hacked e-mail addresses, time spent removing accounts registered on unwanted and unfamiliar websites, time spent monitoring and removing unwanted phishing scam e-mails and text messages, anxiety, emotional distress, loss of privacy, and other harm, for which they are entitled to compensation.

101. Plaintiffs and Class Members are therefore entitled to obtain actual damages and all other relief permissible under 815 ILCS 505/10a.

SECOND CLAIM FOR RELIEF
VIOLATION OF THE UNIFORM DECEPTIVE TRADE PRACTICES ACT ("UDTPA")
(815 ILLINOIS COMPILED STATUTES 510/1 *et seq.*)
(On Behalf of Plaintiffs and All Class Members)

102. Plaintiffs re-allege and incorporate by reference the preceding paragraphs, as if fully set forth herein.

103. Under the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS 510/1 Section 2(a)(12), "[a] person engages in a deceptive trade practice when, in the course of his or her business, . . . the person . . . engages in any [] conduct which similarly creates a likelihood of confusion or misunderstanding."

104. In the Privacy Policy, Defendants represented to Plaintiffs and the Class Members that their Personal Information would be encrypted and/or securely maintained with McDonald's Corporation.

105. Based upon a Class Member's phone conversation with a senior customer representative at McDonald's, Plaintiffs and the Class Members believe that McDonald's failed to encrypt Plaintiffs' and the Class Members' Personal Information or safeguard it, despite McDonald's express representation in the Privacy Policy.

106. Further, in the Privacy Policy, Defendants represent to its users that the users' Personal Information would be destroyed after one year of non-use.

107. Because Plaintiff Jun's account with McDelivery was inactive for over one-year, McDonald's was required to destroy his Personal Information pursuant to the Privacy Policy.

108. However, after the Data Breach, McDonald's informed Plaintiff Jun that McDonald's failed to destroy his Personal Information despite McDonald's representation in the Privacy Policy. McDonald's conceded to Plaintiff Jun that due to a "serious internal error [within McDonald's] his personal information was leaked" during the Data Breach.

109. This incident was not the first time that McDonald's has suffered a data breach; it has a history of failing to maintain the privacy of personal data on its servers. Defendants experienced a similar if not identical failure to safeguard McDelivery users' Personal Information almost four years ago, in 2017. Due to Defendants' poor security measures, more than 2.2 million McDelivery users' personal information in India was breached.

110. Also in 2017, it was reported that McDonald's Canada's career site exposed the personal data of 95,000 applicants seeking jobs at the restaurant since 2014. Applicants' names, home and e-mail addresses, telephone numbers, employment histories and other "standard application information" were stolen.

111. As detailed above, Defendants have a history of repeatedly engaging "in a deceptive trade practice when, in the course of [their] business, . . . [they] . . . engage[] in [] conduct which similarly creates a likelihood of confusion or misunderstanding."

112. Defendants' security measures continue to remain lackluster. According to an UpGuard security ratings report from August 2021, which generates a rating based on billions of data points each day, McDonald's rating is at B (741/850).

113. According to Defendants, 68 million people are "fed daily" through more than 38,000 McDonald's locations.

114. Millions of Defendants' consumers and their Personal Information remain at risk of being stolen and damaged in the future by Defendants' conducts which continue to create a likelihood of future injury.

115. Plaintiffs and Class Members were (and continue to be) damaged as a direct and/or proximate result of Defendants' misrepresentation that Plaintiffs' and Class Members' Personal Information would be encrypted and maintained securely in the form of, *inter alia*, time spent

contacting McDonald's to assess the extent of the Data Breach, time spent changing passwords to hacked e-mail addresses, time spent removing accounts registered on unwanted and unfamiliar websites, time spent monitoring and removing unwanted phishing scam e-mails and text messages, anxiety, emotional distress, loss of privacy, and other harm, for which they are entitled to compensation.

116. Plaintiffs and Class Members are therefore entitled to injunctive relief, attorneys' fees and costs, and all other relief permissible under 815 ILCS 510/3.

THIRD CLAIM FOR RELIEF
THE PERSONAL INFORMATION PROTECTION ACT
(On Behalf of Plaintiffs and All Class Members)

117. Plaintiffs re-allege and incorporate by reference the preceding paragraphs, as if fully set forth herein.

118. Plaintiffs brings this claim under South Korea's Personal Information Protection Act ("PIPA"), on behalf of themselves and the Class.

119. PIPA aims to protect personal data from unnecessary collection, unauthorized use or disclosure, and abuse.

120. According to Article 2 of PIPA, the term "personal information" means any of the following information relating to a living individual: "(a) [i]nformation that identifies a particular individual by his or her full name, . . . (b) [i]nformation which, even if it by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual. In such cases, whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as [the] likelihood that the other information can be procured; . . .."

121. Under PIPA, the term "personal information controller" means "a public institution, legal person, organization, individual, etc. that processes personal information directly or indirectly to operate the personal information files as part of its activities[.]"

122. Defendants, an entity that processes personal information directly and/or indirectly to operate the personal information files as part of its McDelivery service, are "personal information controller(s)" as defined in Article 2 of PIPA.

123. Under Article 29 of PIPA, Defendants, as personal information controllers, had a specific duty to "take such technical, managerial, and physical measures . . . that are necessary to ensure safety as prescribed by Presidential Decree so that the personal information may not be lost, stolen, divulged, forged, altered, or damaged."

124. By and through their conduct as described herein, Defendants failed to uphold the specific duty to implement security measures to ensure safety of Personal Information, as required by PIPA.

125. Article 34 of PIPA also required Defendants to: (a) notify "without delay" those affected by the Data Breach of several details about the Data Breach, including but not limited to "1. [p]articulars of the personal information divulged; [and] 2. [w]hen and how personal information has been divulged[.]"

126. Defendants knew or should have known at the time they learned of the Data Breach that failure to provide notice of the breach to Plaintiffs and the Class "without delay" was unlawful.

127. Article 30 of PIPA requires that "[e]very personal information controller [to] establish a personal information processing policy including . . . [o]utsourcing personal information processing[.]"

128. Further, for any and all information transferred overseas, Article 39-12 of PIPA states that the information controller "shall obtain users' consent if intending to provide (including accessing), outsource the processing of, or store (hereinafter referred to as 'transfer' []) users' personal information overseas[.]"

129. Additionally, for any and all information transferred overseas, Article 17 of PIPA states that the personal information controller "may provide . . . the personal information of a data subject to a third party . . . [w]here the consent is obtained from the data subject[.]" And when a personal information controller obtains a data subject's consent to provide the personal information to a third party, the personal information controller "shall inform a data subject" when any of the following is modified: "1. The recipient of personal information; 2. The purpose for which the recipient of personal information uses such information; 3. Particulars of personal information to be provided; 4. The period during which the recipient retains and uses personal information; [and] 5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent."

130. Defendants, however, failed to disclose in its Korean version of the Privacy Policy that the customers' Personal Information was transferred to (1) Facebook Inc., ("Facebook") (2) Applied Predictive Technologies, Inc., ("APT") and (3) Tasseologic, Inc. ("Tasseologic"). Thus, Defendants needed Plaintiffs' and the Class Members' consent to transfer Plaintiffs' and Class Members' Personal Information to Facebook, APT, and Tasseologic, rather than just to McDonald's Corporation and Amazon Web Services per the Korean Privacy Policy. But McDonald's failed to obtain such consent prior to the transfer in violation of Articles 17, 30, and 39-12 of PIPA.

131. In the English version of the Privacy Policy, Defendants also do not disclose that the customers' Personal Information is transferred to McDonald's Corporation or to Amazon Web Services. McDonald's never obtained the consent of customers who reviewed and agreed to the English version of the Privacy Policy prior to modifying the list of transferees of the customers' Personal Information in violation of Articles 17, 30, and 39-12 of PIPA.

132. Further, despite Defendants' retaining their users' Personal Information for over one-year even with non-use (contrary to Defendants' representation in the Privacy Policy), Defendants failed to inform their customers that their accounts were not deleted after one-year of non-use, in violation of Article 17(2) and 21(1) of PIPA.

133. Article 64 of PIPA allows any of the following corrective measures to be ordered when "there has been infringement with respect to personal information, and failure to take action is likely to cause damage that is difficult to remedy . . . : 1. To suspend infringement with respect to personal information; 2. To temporarily suspend personal information processing; [and] 3. Other measures necessary to protect personal information and to prevent personal information infringement."

134. Moreover, Article 39-2(1) of PIPA provides that "a data subject, who suffers damage out of loss, theft, divulgence, forgery, alteration, or damage of his or her own personal information, caused by wrongful intent or negligence of a personal information controller, may claim a reasonable amount of damages not exceeding three million won (approximately USD $2500.00 at the current exchange rate)." It further states that "[i]n such cases, the said personal information controller may not be released from the responsibility for compensation if it fails to prove non-existence of his or her wrongful intent or negligence."

135. Also, Article 39-2(2) provides that in such cases, "the Court may determine a reasonable amount of damages not exceeding the amount provided for in [Article 39-2(1)] taking into account all arguments in the proceedings and the results of examining evidence."

136. The harmful impact upon members of the Class and Plaintiffs resulting from Defendants' conduct as described herein far outweighs any justifications proffered by Defendants.

137. As a direct and proximate result of Defendants' violations of PIPA, Plaintiffs and the Class have suffered actual harm as described above and prayed for below in an amount according to proof at trial. As a result of Defendants' conduct, Plaintiffs and the Class seek damages, including statutory damages, and all other relief permissible under PIPA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class;

b) For equitable relief compelling Defendants, among other things (1) to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, (2) to disclose with specificity how and when the Data Breach occurred, and (3) to create and disclose data retention and transmission policies that are accurate and truthful, and otherwise comply with all applicable legal standards;

c) For an Order requiring Defendants to pay for phishing scam monitoring and identity theft protection services for Plaintiffs and the Class;

d) For an award of damages, including statutory damages and statutory penalties, in an amount to be determined, as allowable by law; and

e) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury, pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, of all issues triable.

Dated: October 5, 2021

Respectfully submitted,

By: /s/ *Shannon M. McNulty*

Shannon M. McNulty
CLIFFORD LAW OFFICES, P.C.
120 North LaSalle Street
36th Floor
Chicago, IL 60602
Tel: (312) 899-9090
Fax: (312) 251-1160
smm@CliffordLaw.com

Christopher L. Lebsock*
Michael P. Lehmann*
HAUSFELD LLP
600 Montgomery St. #3200
San Francisco, CA 94111
Tel: (415) 633-1908
Fax: (415) 358-4980
clebsock@hausfeld.com
mlehmann@hausfeld.com

James J. Pizzirusso*
Jane I. Shin*
HAUSFELD LLP
888 16th Street, N.W.
Suite 300
Washington, DC 20006
Tel: (202) 540-7200
Fax: (202) 540-7201
jpizzirusso@hausfeld.com
jshin@hausfeld.com

Young-Ki Rhee*
We The People Law Group
6F Jin-Yang Bldg., 47 Kyonggidae-ro
Seodaemun-gu, Seoul, South Korea 03752
Tel: +82-2-2285-0062
Fax: +82-2-2285-0071
ykrhee@wethepeople.co.kr

Amy E. Keller
Dicello Levitt Gutzler
Ten North Dearborn Street
Sixth Floor
Chicago, Illinois 60602
Tel: (312) 214-7900
akeller@dicellolevitt.com

**Pro hac vice to be sought*