UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ANDRES VELOZ, individually and on behalf of all others similarly situated, Plaintiff, v. **BYZFUNDER NY LLC**, Defendant.	Civil Action No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Andres Veloz ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to them and upon information and belief as to all other matters, and by and through undersigned counsel, hereby brings this Class Action Complaint against Defendant Byzfunder NY LLC ("Byzfunder" or "Defendant"), and alleges as follows:

INTRODUCTION

1. This class action arises out of the recent data breach ("Data Breach") that impacted Defendant and compromised Plaintiff and Class Members' personally identifiable information ("PII" or "Private Information").

2. Byzfunder is a for profit limited liability company with its principal place of business in New York, New York that provides funding and working capital to small and mid-sized businesses. In the regular course of its business, Byzfunder requires individuals who apply for or guarantee its financing products to provide sensitive PII so that Byzfunder can underwrite, fund, and service those accounts. Byzfunder knew that it was obligated to maintain reasonable and adequate security measures to secure, protect, and safeguard that PII against unauthorized access

and disclosure.

3. According to Byzfunder's own notice, on September 19, 2025 it detected suspicious activity within one of its software solutions. A subsequent investigation determined that certain files may have been accessed or acquired without authorization between September 1 and September 20, 2025. After conducting a review of affected files, Byzfunder determined on or about November 12, 2025 that Plaintiff's and Class Members' PII was contained in those files, and it began mailing data breach notices on or about November 19, 2025 (the "Data Breach").

4. The PII compromised in the Data Breach includes, at a minimum, full names and Social Security numbers. This information is highly sensitive and valuable to criminals because it can be used to commit identity theft and fraud. Plaintiff and Class Members have suffered a substantial and imminent risk of identity theft and other harm as a result of the Data Breach, and many have already experienced increased spam calls and emails, dark web alerts, and the need to take protective steps such as locking their credit profiles.

5. Plaintiff brings this action to seek redress for the harms caused by the Data Breach, including out of pocket costs and lost time spent responding to the incident, the continuing risk of identity theft, the loss of the benefit of the bargain with Byzfunder, and the present value of the credit monitoring and identity theft protection services needed to protect themselves going forward, as well as injunctive relief requiring Byzfunder to implement and maintain reasonable data security practices that meet industry standards.

6. Byzfunder owed a duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Byzfunder breached that duty by, among other things, failing to, or contracting with companies that failed to, implement and maintain reasonable security

procedures and practices to protect customers' PII from unauthorized access and disclosure. Every year, millions of Americans have their most valuable PII stolen and sold online because of data breaches. Despite dire warnings about the severe impact of data breaches on Americans across all economic strata, companies still fail to make the necessary investments in implementing important and adequate security measures to protect their customers' and employees' data.

7. Byzfunder required its customers to provide it with sensitive PII and failed to protect it. Byzfunder had an obligation to secure customers' PII by implementing reasonable and appropriate data security safeguards. This was part of the bargain between Byzfunder and Plaintiff and Class Members.

8. As a result of Byzfunder's failure to provide reasonable and adequate data security, Plaintiff's and the Class Members' unencrypted, non-redacted PII has been exposed to unauthorized third parties. Plaintiff and the Class are now at much higher risk of identity theft and cybercrimes of all kinds, especially considering the highly sensitive PII stolen here and the fact that the compromised PII is likely already being sold on the dark web. This risk constitutes a concrete injury suffered by Plaintiff and the Class as they no longer have control over their PII, which PII is now in the hands of third-party cybercriminals. This substantial and imminent risk of identity theft has been recognized by numerous courts as a concrete injury sufficient to establish standing.

9. Plaintiff and the Class will have to incur costs to pay a third-party credit and identity theft monitoring service for the rest of their lives as a direct result of the Data Breach.

10. Plaintiff brings this action on behalf of himself and those similarly situated to seek redress for the lifetime of harm they will now face, including, but not limited to, reimbursement of losses associated with identity theft and fraud, out-of-pocket costs incurred to mitigate the risk of future harm, compensation for time and effort spent responding to the Data Breach, the costs of

extending credit monitoring services and identity theft insurance, and injunctive relief requiring Byzfunder to ensure that it implements and maintains reasonable data security practices going forward.

THE PARTIES

11. Plaintiff Andres Veloz is a natural person and citizen of Texas who resides in San Antonio, Texas. He provided Byzfunder with his personal information, including his name and Social Security number, in connection with Byzfunder's financing services. On or about November 19, 2025, Byzfunder mailed Plaintiff a written "Notice of Data Security Incident" informing him that his name and Social Security number were contained in files that an unauthorized third party accessed between September 1 and September 20, 2025. Since the Data Breach, Plaintiff has experienced increased spam calls and emails, received a dark web alert from Experian indicating that his information was found on the dark web, and locked his credit profile in an effort to protect himself.

12. Defendant Byzfunder NY LLC is a for-profit New York limited liability company that provides capital for small and mid-sized businesses, with its principal place of business located in New York, New York.

JURISDICTION AND VENUE

13. This Court has personal jurisdiction over Defendant. Defendant is a New York limited liability company with its principal place of business in New York, New York, and it regularly conducts business there.

14. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d) because the amount in controversy exceeds $5,000,000 (exclusive of interest and costs), because there are more than 100 members in the proposed class, and at least one member of the class, including named Plaintiff, is a citizen of a state different from Defendant.

15. Venue is proper in this Court as a substantial part of the events, omissions, and acts giving rise to the claims herein, including the Data Breach itself, occurred within this district.

COMMON FACTUAL ALLEGATIONS

16. This is a class action brought by Plaintiff, individually and on behalf of all citizens who are similarly situated (i.e., the Class Members), seeking to redress Byzfunder's willful and reckless violations of their privacy rights. Plaintiff and the other Class Members were individuals who provided personal information to Byzfunder in connection with its financing services.

17. Between September 1, 2025 and September 20, 2025, an unauthorized third party accessed and obtained Plaintiff's and the Class Members' PII.

18. This action pertains to Byzfunder's unauthorized disclosures of the Plaintiff's PII that occurred during the Data Breach.

19. Byzfunder disclosed Plaintiff's and the other Class Members' PII to unauthorized persons as a direct and/or proximate result of Byzfunder's failure to safeguard and protect their PII.

20. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Byzfunder assumed legal and equitable duties and knew or should have known it was responsible for protecting the PII from unauthorized disclosures.

21. Despite recognizing its duty to do so, Byzfunder failed to implement security safeguards to protect Plaintiff's and the Class Members' PII.

22. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Byzfunder to keep their PII confidential and maintained securely, to use this information for business purposes only, to make only authorized disclosures of this information, and to ensure that its third-party vendors take similar steps.

1. The Data Breach

23. According to the written "Notice of Data Security Incident" that Byzfunder sent to Plaintiff and other victims on or about November 19, 2025, Byzfunder detected suspicious activity within one of its software solutions on September 19, 2025. Byzfunder states that it promptly initiated an investigation and engaged cybersecurity specialists. The investigation determined that certain files may have been accessed or acquired without authorization between September 1 and September 20, 2025. After undertaking a comprehensive review of the affected files, Byzfunder learned on or about November 12, 2025 that those files contained personal information relating to Plaintiff and other individuals.

24. The notice explains that the "potentially affected information may have included your name and Social Security number," and that Byzfunder is offering 12 months of identity theft protection through IDX, including credit and CyberScan monitoring, a 1,000,000 dollar insurance reimbursement policy, and fully managed identity theft recovery services, with an enrollment deadline of February 19, 2026.

25. The Data Breach was the direct result of Byzfunder's failure to implement and maintain reasonable and appropriate data security measures to protect the PII it collected and stored.

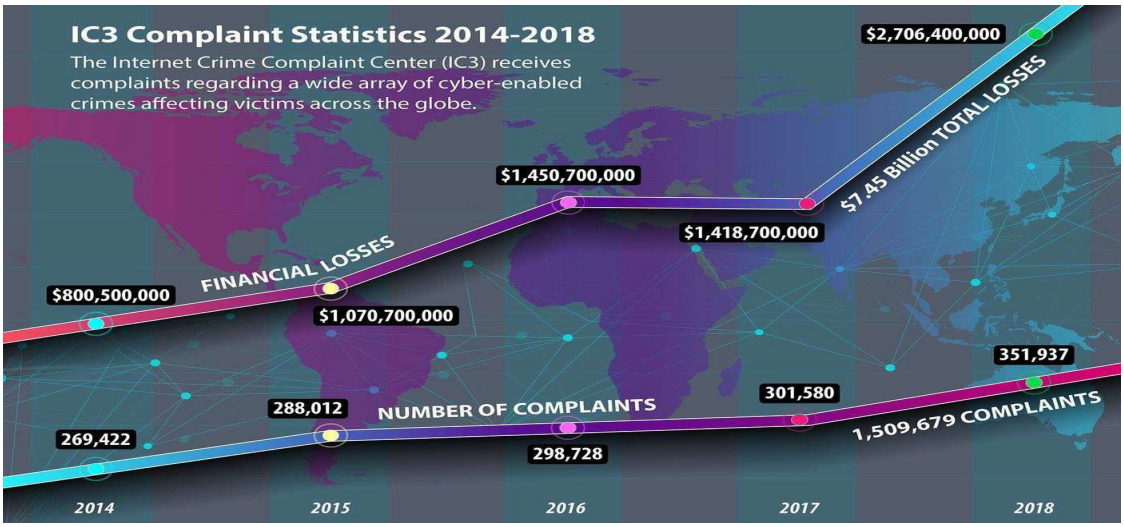
2. The Data Breach was Preventable

26. Had Byzfunder maintained industry-standard safeguards to monitor, assess, and update security controls and related system risks, Byzfunder could have safeguarded private data. Byzfunder's lack of security controls and the delayed implementation of enhanced security measures only after the Data Breach are inexcusable.

27. Byzfunder was at all times fully aware of its obligation to protect customers' PII and the risks associated with failing to do so. Byzfunder knew that information of the type

collected, maintained, and stored by Byzfunder is highly coveted and a frequent target of hackers.

28. This exposure, along with the fact that the compromised PII is already likely being sold on the dark web, is tremendously problematic. Cybercrime is rising at an alarming rate, as shown in the FBI's Internet Crime Complaint statistics chart shown below:



29. By 2013, it was being reported that nearly one out of four data breach notification recipients become a victim of identity fraud.[1]

30. Stolen PII is often trafficked on the dark web. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

31. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[2]

---

[1] Al Pascual, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, JAVELIN (Feb. 20, 2013), https://javelinstrategy.com/research/2013-identity-fraud-report-data-breaches-becoming-treasure-trove-fraudsters (last visited June 20, 2025).

[2] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Feb. 1, 2020), https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring.

32. In April 2023, NationsBenefits, "disclosed that thousands of its members had their personal information compromised in a late-January ransomware attack targeting Fortra's Anywhere platform, a file-transfer software that the firm was using. According to the news reports, the ransomware gang CLOP claimed responsibility for the attack, saying it took advantage of a previously known vulnerability."[3]

33. In mid-April 2023, "the second largest health insurer [Point32Health], in Massachusetts, suffered major technical outages resulting from a ransomware attack. The incident brought down the company's systems that it uses to service members and providers, resulting in some members having difficulty contacting their insurers."[4]

34. In May 2023, MCNA Insurance Company disclosed that "personal health information of nearly nine million customers was compromised in a cyber incident discovered in March. In a data breach notification letter filed with the Maine state attorney general's office dated May 26, the firm said that it detected unauthorized access to its systems on March 6, with some found to be infected with malicious code…According to MCNA, the hackers were successful in accessing patient personal information."[5]

35. In April 2020, ZDNet reported in an article titled, "Ransomware mentioned in 1,000+ SEC filings over the past year", that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news

[3] Mark Rosanes, *The insurance industry cyber crime report: recent attacks on insurance businesses*, INSURANCE BUSINESS (June 12, 2023),https://www.insurancebusinessmag.com/us/guides/the-insurance-industry-cyber-crime-report-recent-attacks-on-insurance-businesses-448429.aspx.
[4] *Id.*
[5] *Id.*

complaints as revenge against those who refuse to pay."[6]

36. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[7]

37. Another example is when the U.S. Department of Justice announced its seizure of AlphaBay in 2017. AlphaBay had more than 350,000 listings, many of which concerned stolen and fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. "As data breaches in the news continue to show, PII about employees, customers, and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[8]

38. The PII of consumers remains of high value to criminals, as evidenced by the price 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

---

[6] Catalin Cimpanu, *Ransomware mentioned in 1000 SEC filings over the past year*, ZDNET (April 30, 2020), https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/.

[7] Multi-State Information Sharing & Analysis Center, *Ransomware Guide*, UNITED STATES CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (Sept. 2020), https://www.cisa.gov/sites/default/files/2023-01/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.

[8] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018), https://web.archive.org/web/20210614051146/https://www.armor.com/resources/blog/stolen-piiramifications-identity-theft-fraud-dark-web/.

bank details have a price range of $50 to $200.[9] Experian reports that a solen credit or debit card number can sell for $5 to $110 on the dark web.[10] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[11]

39. Social Security numbers, for example, are among the worst kind of personal information 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:

> 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 assuming your identity can cause a lot of problems.[12]

40. What is 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, preventative action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraudulent activity to obtain a new number.

---

[9] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[10] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/?msockid=2bcba6b07db36c323b77b0a17cc26db2.

[11] *In the Dark*, VPNOVERVIEW, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Sept. 30, 2025).

[12] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION, Pub. No. 05-10064 (Oct. 2024), https://www.ssa.gov/pubs/EN-05-10064.pdf.

41. Even then, a new Social Security number may not be effective. According to July Ferguson of the Identity Theft Resource Center, "The 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."[13]

42. Because of this, the information comprised in the Data Breach here is significantly more harmful to lose than the loss of, for example, credit card information in a retailer payment card breach because victims can simply 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.

43. The PII compromised by the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[14]

44. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

45. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

---

[13] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[14] Tim Greene, *Anthem hack: Personal data stolen sells for 10x price of stolen credit card numbers*, NETWORK WORLD (Feb. 6, 2015), https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

46. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

47. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

48. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[15] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face, "substantial costs and inconveniences repairing damage to their credit records… [and their] good name."[16]

49. The exposure of Plaintiff's and Class Members' PII to cybercriminals will continue to cause substantial risk of future harm, including identity theft, that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off this highly sensitive information.

3. Byzfunder Failed to Comply with the Federal Trade Commission

50. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses

[15] *See* GOVERNMENT ACCOUNTABILITY OFFICE, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, GAO-07-737 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.
[16] *Id.*

that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[17]

51. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business,* which established guidelines for fundamental data security principals for business.[18] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted form the system; and have a response plan ready in the event of a breach.[19]

52. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[20]

53. Highlighting the importance of protecting against phishing and other types of data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice

---

[17] *See* FEDERAL TRADE COMMISSION, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[18] *See* FEDERAL TRADE COMMISSION, *Protecting Personal Information: A Guide for Business* (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[19] *Id.*

[20] FEDERAL TRADE COMMISSION, *supra* note 17.

prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

4. The Impact of Data Breach on Victims

54. Byzfunder's failure to keep Plaintiff's and Class Members' PII secure has severe ramifications. Given the highly sensitive nature of the PII exposed in the Data Breach, including Social Security numbers and names, hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future. As a result, Plaintiff has suffered injury and faces an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

55. The PII exposed in the Data Breach is highly coveted and valuable on underground markets. Identity thieves can use the PII to: (a) commit insurance fraud; (b) obtain a fraudulent driver's license or ID card in the victim's name; (c) obtain fraudulent government benefits; (d) file a fraudulent tax return using the victim's information; (e) commit medical and healthcare-related fraud; (f) access financial and investment accounts and records; (g) engage in mortgage fraud; and/or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

56. Further, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be victims of several cybercrimes stemming from a single data breach.

57. Given the exposure of PII from Byzfunder, victims of the Data Breach face a substantial and continuing risk of identity theft and fraud. Plaintiff and Class Members have also spent time and effort dealing with the fallout of the Data Breach, including reviewing financial

and insurance statements, checking credit reports, and monitoring for unauthorized activity.

58. It is no wonder, then, that identity theft exacts a severe emotional toll on its victims. The 2021 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 84% reported anxiety;
- 76% felt violated;
- 32% experienced financial related identity problems;
- 83% reported being turned down for credit or loans;
- 32% reported problems with family members as a result of the breach;
- 10% reported feeling suicidal.[21]

59. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48% reported sleep disturbances;
- 37.1% reported an inability to concentrate/lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1 reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[22]

[21] IDENTITY THEFT RESOURCE CENTER, *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces* (2021), https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf.
[22] *Id.*

60. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

61. The unauthorized disclosure of sensitive PII to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[23]

62. Consumers are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

63. As a result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and Class Members have and will continue to suffer economic loss and other actual harm

---

[23] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—that the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

for which they are entitled to damages, including, but not limited to, the following:

a. The unconsented disclosure of confidential information to a third party;

b. Unauthorized use of their PII without compensation;

c. Losing the value of the explicit and implicit promises of data security;

d. Losing the value of access to their PII permitted by Byzfunder without their permission;

e. Identity theft and fraud resulting from the theft of their PII;

f. Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

g. Anxiety, emotional distress, and loss of privacy;

h. The present value of ongoing credit monitoring and identity theft protection services necessitated by the Data Breach;

i. Unauthorized charges and loss of use of and access to their accounts;

j. Lowered credit scores resulting from credit inquiries following fraudulent activities;

k. Costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

l. The continued, imminent, and certainly impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or more unauthorized third parties.

64. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement. The Department of Justice's Bureau of Justice Statistics found that identity theft victims, "reported spending an average of about 7 hours

clearing up the issues" relating to identity theft or fraud.[24]

65. Plaintiff and Class Members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more to work with a provider that has better data security. Seventy percent of consumers would provide less personal information to organizations that suffered a data breach.[25]

66. Plaintiff and Class Members have a direct interest in Byzfunder's promises and duties to protect PII, i.e., that Byzfunder would *not increase* their risk of identity theft and fraud. Because Byzfunder failed to live up to its promises and duties in this respect, Plaintiff and Class Members seek the present value of ongoing identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by Byzfunder's wrongful conduct. Through this remedy, Plaintiff seeks to restore himself and Class Members as close to the same position as they would have occupied but for Byzfunder's wrongful conduct, namely its failure to adequately protect Plaintiff's and the Class Members' PII.

67. Plaintiff and Class Members further seek to recover the value of the unauthorized access to their PII permitted through Byzfunder's wrongful conduct. This measure of damages is analogous to the remedies for the unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PII is non-rivalrous—the unauthorized use by. Another does not diminish the rights- holder's ability to practice the patented

[24] E. Harrell, *Victims of Identity Theft, 2014*, U.S. DEPARTMENT OF JUSTICE (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.
[25] Richard Turner, *Beyond the Bottom Line: The Real Cost of Data Breaches*, FIREEYE (May 11, 2016), https://web.archive.org/web/20210422161745/https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html.

invention or use the trade-secret protected technology. Nevertheless, a Plaintiff may generally recover the reasonable use of the value of the IP—i.e., a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because: (a) Plaintiff and Class Members have a protectible property interest in their PII; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; (c) rental value is established with reference to market value, i.e., evidence regarding the value of similar transactions.

68. Plaintiff and Class Members have an interest in ensuring their PII is secured and not subject to further theft because Byzfunder continues to hold their PII.

CLASS ACTION ALLEGATIONS

69. Plaintiff brings this action on behalf of himself and the following proposed nationwide class (herein "the Class"), defined as follows:

> **National Class**
> All persons residing in the United States whose personally identifiable information was accessed and/or acquired by an unauthorized person as a result of the Data Breach, including all who were sent a notice of the Data Breach.

70. Excluded from the proposed Class are any officer or director of Byzfunder; any officer or director of any affiliate, parent, or subsidiary of Byzfunder; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

71. **Numerosity:** Members of the proposed Class are likely to number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class

is readily ascertainable from Byzfunder's own records.

72. **Commonality:** Common questions of law and fact exist as to the proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Byzfunder engaged in the wrongful conduct alleged herein;

b. Whether Byzfunder's inadequate data security measures was a cause of the Data Breach;

c. Whether Byzfunder owed a legal duty to Plaintiff and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII;

d. Whether Byzfunder negligently or recklessly breached legal duties owed to Plaintiff and the Class Members to exercise due care in collecting, storing, and safeguarding their PII;

e. Whether Plaintiff and the Class are at an increased risk for identity theft because of the Data Breach;

f. Whether Byzfunder failed to implement and maintain reasonable security procedures and practices for Plaintiff's and Class Members' PII;

g. Whether Plaintiff and the other Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

73. Byzfunder engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, individually, and on behalf of the other Class Members. Similar or identical statutory and common violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

74. **Typicality:** Plaintiff's claims are typical of the claims of the Members of the Class. All Class Members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Byzfunder's misconduct affected all Class Members in the same

manner.

75. **Adequacy of Representation:** Plaintiff is an adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

76. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Byzfunder, making it impracticable for Class Members to individually seek redress for Byzfunder's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

77. Plaintiff realleges all preceding paragraphs as if fully set forth herein.

78. Plaintiff brings this claim individually and on behalf of the Class.

79. Byzfunder owed a duty to Plaintiff and the Class to exercise reasonable care in

obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class Members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiff's and Class Members' PII in Byzfunder's possession was adequately secured and protected.

80. Byzfunder owed, and continues to owe, a duty to Plaintiff and the other Class Members to safeguard and protect their PII.

81. Byzfunder breached its duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiff's and the other Class Members' PII.

82. It was reasonably foreseeable that Byzfunder's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class Members' PII would result in an unauthorized third-party gaining access to such information for no lawful purpose.

83. As a direct result of Byzfunder's breach of its duties and the disclosure of Plaintiff's and Class Members' PII, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

84. By engaging in the negligent acts and omissions alleged herein, which permitted an unknown third party to access Byzfunder's systems containing the PII at issue, Byzfunder failed to meet the data security standards set forth under Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures, which Byzfunder has failed to do as discussed herein.

85. Byzfunder's failure to meet this standard of data security established under Section

5 of the FTC Act is evidence of negligence.

86. Neither Plaintiff nor other Class Members contributed to the Data Breach as described in this Complaint.

87. Byzfunder's wrongful actions and/or inaction and the resulting Data Breach (as described above) constituted (and continue to constitute) negligence at common law.

88. As a result of Byzfunder's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Byzfunder's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

89. Plaintiff realleges all preceding paragraphs as if fully set forth herein.

90. Plaintiff brings this claim individually and on behalf of the Class.

91. Byzfunder is engaged in "commerce" within the meaning of Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45.

92. Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce," which includes failing to implement and maintain reasonable data security measures to protect consumers' personally identifiable information from unauthorized access and

disclosure.

93. The Federal Trade Commission ("FTC") has issued numerous publications and brought many enforcement actions describing reasonable data security practices and identifying inadequate data security practices as "unfair" or "deceptive" under the FTC Act. These materials, along with widely recognized industry standards, put Byzfunder on notice of its duty to implement and maintain reasonable data security measures.

94. By failing to implement and maintain reasonable and appropriate data security measures to protect Plaintiff's and Class Members' PII from unauthorized access and disclosure, and by failing to timely detect and contain the Data Breach, Byzfunder violated Section 5 of the FTC Act and similar state consumer protection and data security statutes.

95. Plaintiff and Class Members are within the class of persons the FTC Act and similar state statutes are intended to protect, because they are individuals whose PII was collected, maintained, and used by Byzfunder in the course of offering and providing financing services.

96. The injuries that Plaintiff and Class Members have suffered, including the exposure of their PII to unauthorized third parties, the substantial and ongoing risk of identity theft and fraud, the time and expense of monitoring accounts and credit reports, and other harms alleged herein, are the type of injuries that the FTC Act and similar state laws were designed to prevent.

97. Byzfunder's violations of Section 5 of the FTC Act and similar state statutes constitute negligence per se.

98. Byzfunder's negligence per se was a direct and proximate cause of the Data Breach and the resulting injuries to Plaintiff and Class Members, including, but not limited to: (i) a substantially increased and imminent risk of identity theft and fraud; (ii) the compromise and potential misuse of their PII; (iii) out-of-pocket costs associated with the prevention, detection,

and mitigation of identity theft and fraud; (iv) loss of time and lost productivity; and (v) the present value of ongoing credit monitoring and identity theft protection services necessitated by the Data Breach.

99. Accordingly, Plaintiff and Class Members are entitled to damages and other relief in an amount to be proven at trial.

COUNT III
BREACH OF IMPLIED CONTRACT

100. Plaintiff realleges all preceding paragraphs as if fully set forth herein.

101. Plaintiff brings this claim individually and on behalf of the Class.

102. When Plaintiff and Class Members provided their PII to Byzfunder in connection with Byzfunder's financing services, they did so with the reasonable expectation and mutual understanding that Byzfunder would use their PII only for legitimate business purposes and would implement and maintain reasonable data security measures to safeguard their PII from unauthorized access and disclosure.

103. Byzfunder accepted and retained Plaintiff's and Class Members' PII, and in doing so accepted the obligations that flowed from that exchange. The circumstances surrounding the parties' interactions created an implied contract between Byzfunder, on the one hand, and Plaintiff and Class Members, on the other, pursuant to which Byzfunder agreed to reasonably safeguard and protect their PII.

104. This implied contract included, but was not limited to, Byzfunder's obligations to: (a) use the PII only for legitimate business purposes related to its financing services; (b) implement and maintain reasonable and appropriate data security measures consistent with applicable laws, regulations, and industry standards; and (c) promptly provide accurate and sufficient notice in the event of a security incident compromising the PII.

105. Byzfunder breached the implied contract by failing to implement and maintain reasonable and appropriate data security measures to safeguard Plaintiff's and Class Members' PII, and by failing to prevent, detect, or timely contain the Data Breach.

106. As a direct and proximate result of Byzfunder's breach of the implied contract, Plaintiff and Class Members suffered damages, including, but not limited to: (i) the loss of the benefit of their bargain with Byzfunder; (ii) the diminished value of the services they received, because part of the price paid and/or value conferred was for reasonable data security that they did not receive; (iii) the exposure of their PII to unauthorized third parties; (iv) the substantial and ongoing risk of identity theft and fraud; (v) out-of-pocket costs incurred to mitigate that risk; and (vi) the present value of ongoing credit monitoring and identity theft protection services necessitated by the Data Breach.

107. Plaintiff and Class Members are therefore entitled to damages and all other relief permitted by law as a result of Byzfunder's breach of implied contract.

COUNT IV
UNJUST ENRICHMENT

108. Plaintiff realleges all preceding paragraphs as if fully set forth herein.

109. Plaintiff brings this claim individually and on behalf of the Class.

110. Plaintiff and Class Members conferred a monetary benefit upon Byzfunder in the form of monies paid to Byzfunder in connection with its financing and merchant cash-advance services, with the understanding that Byzfunder would use a portion of those funds to implement and maintain reasonable data security.

111. Byzfunder accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Byzfunder also benefited from the receipt of Plaintiff's and Class Members' PII, as this was used to facilitate Byzfunder's financing transactions, account servicing, and

verification processes.

112. As a result of Byzfunder's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between its payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

113. Byzfunder should not be permitted to retain the money belonging to Plaintiff and the Class Members because Byzfunder failed to adequately implement the data privacy and security measures that Plaintiff and Class Members reasonably expected and that were otherwise mandated by federal, state, and local laws and industry standards.

114. Byzfunder should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enters judgment in their favor and against Byzfunder, as follows:

(a) Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Plaintiff's counsel as Lead Counsel for the Class;

(b) Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

(c) Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent Byzfunder from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

(d) Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

(e) Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

(f) Awarding Plaintiff and the Class such other favorable relief as allowable under law.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Class Action Complaint.

December 8, 2025

Respectfully submitted,

Martha A. Geer (NY Reg. No. 1917129)
BRYSON HARRIS SUCIU & DeMAY PLLC
900 W. Morgan Street
Raleigh, NC 27603
Telephone: (206) 623-7292
Email: mgeer@brysonpllc.com

/s/ Martha A. Geer
Martha A. Geer

and

J. Hunter Bryson (NC Bar No. 123599)*
BRYSON HARRIS SUCIU & DeMAY PLLC
11 Park Place, 3rd Floor
New York, NY 10007
Telephone: 919-539-2708
hbryson@brysonpllc.com
Secondary Email: rreinhart@brysonpllc.com

*Application for *pro hac vice* forthcoming

Attorneys for Plaintiffs