

1 M. Anderson Berry (SBN 262879)
2 Gregory Haroutunian (SBN 330263)
3 **CLAYEO C. ARNOLD,**
4 **A PROFESSIONAL LAW CORP.**
5 865 Howe Avenue
6 Sacramento, CA 95825
7 Telephone: (916) 239-4778
8 Facsimile: (916) 924-1829
9 aberry@justice4you.com
10 gharoutunian@justice4you.com

11 John A. Yanchunis
12 (*Pro Hac Vice*)
13 Ryan D. Maxey
14 (*Pro Hac Vice*)
15 **MORGAN & MORGAN**
16 **COMPLEX LITIGATION GROUP**
17 201 N. Franklin St., 7th Floor
18 Tampa, FL 33602
19 Telephone: (813) 223-5505
20 Facsimile: (813) 223-5402
21 jyanchunis@ForThePeople.com
22 rmaxey@ForThePeople.com

23 *Attorneys for Plaintiff*

24 **THE UNITED STATES DISTRICT COURT**
25 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**
26 **SAN FRANCISCO DIVISION**

27 KAMAL BITMOUNI, on behalf of himself
28 and all others similarly situated,

Plaintiff,

vs.

PAYSAFE PAYMENT PROCESSING
SOLUTIONS LLC, a Delaware limited
liability company,

Defendant.

Case No.: 3:21-cv-00641-JCS

SECOND AMENDED CLASS ACTION
COMPLAINT

DEMAND FOR JURY TRIAL

1 Plaintiff Kamal Bitmouni (“Plaintiff”), individually and on behalf of all others similarly
2 situated (“Class Members”), brings this Second Amended Class Action Complaint against Paysafe
3 Payment Processing Solutions LLC (“Defendant”), and alleges, upon personal knowledge as to his
4 own actions and his counsels’ investigations, and upon information and belief as to all other
5 matters, as follows:

6 I. INTRODUCTION

7 1. Plaintiff brings this class action against Defendant for its failure to properly secure
8 and safeguard Plaintiff’s and Class Members’ PII, including without limitation, names, contact
9 details, Social Security numbers, and bank account information (collectively, “personal
10 identifiable information” or “PII”). Plaintiff also alleges Defendant failed to provide timely,
11 accurate, and adequate notice to Class Members that their PII had been lost and precisely what
12 types of information was unencrypted and in the possession of unknown third parties.

13 2. On or before November 6, 2020, Defendant obtained possession of some or all of
14 Plaintiff’s and Class Members’ PII through unknown means and for purposes not yet known.

15 3. On or before November 6, 2020, Defendant shared some or all of the PII of Plaintiff
16 and Class Members with one or more of its affiliates. Again, the reason or purpose for sharing this
17 information is not yet known, although what is known is that information about consumers has
18 become a valuable resource upon which businesses generate other business and/or profit.

19 4. In sharing some or all of the PII of Plaintiff and Class Members with one or more
20 of its affiliates, Defendant had a duty to ensure that the shared PII was and would be properly
21 secured.

22 5. On or before November 6, 2020, Defendant’s affiliate, Paysafe Group Holdings
23 Limited (“PGHL”), now known as PI UK HOLDCO 1 LIMITED, discovered a potential
24 compromise of a website used by part of its U.S. business (the “Data Breach”).

25 6. On or before December 3, 2020, PGHL determined that suspicious activity on the
26 website from May 13, 2018 to November 24, 2020 may have compromised information held on
27 the website.

1 7. On or around December 16, 2020, PGHL notified Plaintiff that his PII, including
2 his name, contact details, Social Security number, and bank account information, may have been
3 accessed during the Data Breach.¹

4 8. On or around January 12, 2021, PGHL notified the Maine Attorney General that
5 the PII of 91,706 individuals may have been accessed during the Data Breach.²

6 9. Maine law requires an information broker or any other person “who maintains
7 computerized data that includes personal information” to notify Maine residents of “a breach of
8 the security of the system.” Me. Re. Stat. Ann. tit. 10, § 1348.1.

9 10. Maine law also requires that notice be provided to the Department of Professional
10 and Financial Regulation or the Attorney General. *Id.* § 1348.5.

11 11. In notifying Maine residents and the Maine Attorney General of the Data Breach,
12 PGHL indicated that it, alone or with others, maintained Plaintiff’s and Class Members’ PII at the
13 time of the Data Breach.

14 12. In order for PGHL to have maintained Plaintiff’s and Class Members’ PII at the
15 time of the Data Breach, it obtained some or all of the PII, directly or indirectly, from Defendant.

16 13. In order for any other affiliates of PGHL to have maintained Plaintiff’s and Class
17 Members’ PII at the time of the Data Breach, such affiliates obtained the PII, directly or indirectly,
18 from Defendant.

19 14. By obtaining, collecting, using, and deriving a benefit from Plaintiff’s and Class
20 Members’ PII, Defendant assumed legal and equitable duties to those individuals. Defendant,
21 through its affiliate PGHL, admits that the unencrypted PII exposed to “unauthorized activity”
22 included names, contact details, Social Security numbers, and bank account information.

23 15. The exposed PII of Plaintiff and Class Members can be sold on the dark web.
24

25 ¹ Exhibit 1 (Redacted “Notice of Data Breach” provided to Plaintiff by Paysafe, dated December
26 16, 2020.)

27 ² Exhibit 2 (Screenshot of the Maine Attorney General “Data Breach Notifications” website for
28 Paysafe; also available at: <https://apps.web.maine.gov/online/aevviewer/ME/40/19dd2b37-106a-4a4f-aa0e-76cf4008ec45.shtml> (last accessed March 30, 2022).)

1 Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff
2 and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of
3 Social Security numbers.

4 16. This PII was compromised due to Defendant's negligent and/or careless acts and
5 omissions and the failure to protect PII of Plaintiff and Class Members. In addition to Defendant's
6 failure to prevent the Data Breach, after discovering the breach, Defendant, through its affiliate
7 PGHL, waited over a month to report it to the states' Attorneys General and affected individuals.

8 17. As a result of this delayed response, Plaintiff and Class Members had no idea their
9 PII had been compromised, and that they are and continue to be at significant risk to identity theft
10 and various other forms of personal, social, and financial harm. The risk will remain for their
11 respective lifetimes.

12 18. Plaintiff brings this action on behalf of all persons whose PII was compromised as
13 a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members;
14 (ii) warn Plaintiff and Class Members of its inadequate information security practices; (iii)
15 effectively secure hardware containing protected PII using reasonable and effective security
16 procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and
17 violates federal and state statutes; and (iv) ensure that any affiliates of Defendant that directly or
18 indirectly acquired some or all of the PII from Defendant did (i), (ii), and (iii).

19 19. Plaintiff and Class Members have suffered cognizable injuries as a result of
20 Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket
21 expenses associated with the prevention, detection, and recovery from identity theft, tax fraud,
22 and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to
23 mitigate the actual consequences of the Data Breach, including but not limited to lost time, and
24 significantly (iv) the continued and certainly an increased risk to their PII, which: (a) remains
25 unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain
26 backed up in Defendant's possession and is subject to further unauthorized disclosures so long as
27 Defendant fail to undertake appropriate and adequate measures to protect the PII. Moreover,

1 Plaintiff and Class Members are at a present and increased risk of identity theft as a result of
2 Defendant's conduct and failures as herein pled.

3 20. Defendant disregarded the rights of Plaintiff and Class Members by intentionally,
4 willfully, recklessly, or negligently failing to take and implement adequate and reasonable
5 measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take
6 available steps to prevent an unauthorized disclosure of data, and failing to follow applicable,
7 required and appropriate protocols, policies and procedures regarding the encryption of data, even
8 for internal use. As the result, the PII of Plaintiff and Class Members was compromised through
9 disclosure to an unknown and unauthorized third party. While a digital copy of the PII of Plaintiff
10 and Class Members was taken, Plaintiff and Class Members have a continuing interest in ensuring
11 that their information which remains in Defendant's possession is and remains safe, and they
12 should be entitled to injunctive and other equitable relief to ensure that their information is
13 protected.

14 **II. PARTIES**

15 21. Plaintiff Kamal Bitmouni is a Citizen of California residing in Chino Hills,
16 California. Mr. Bitmouni received Defendant's *Notice of Data Breach*, dated December 16, 2020,
17 on or about that date.

18 22. Defendant Paysafe Payment Processing Solutions LLC is a limited liability
19 company organized under the laws of Delaware with a principal office in California at 30721
20 Russel Ranch Road, Suite 200, Westlake Village, California.

21 23. Defendant's sole member is Paysafe Holdings (US) Corp, a Delaware corporation.

22 24. The true names and capacities of persons or entities, whether individual, corporate,
23 associate, or otherwise, who may be responsible for some of the claims alleged herein are currently
24 unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true
25 names and capacities of such other responsible parties when their identities become known.

26 25. All of Plaintiff's claims stated herein are asserted against Defendant and any of its
27 owners, predecessors, successors, subsidiaries, agents and/or assigns.

1 **III. JURISDICTION AND VENUE**

2 26. This Court has subject matter and diversity jurisdiction over this action under 28
3 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum
4 or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the
5 proposed class, and at least one Class Member, including Plaintiff (a citizen of California) and one
6 or more of the 485 Maine residents who PGHL represented may have had their personal
7 information impacted during the Data Breach,³ is a citizen of a State different from Defendant,
8 which is a citizen of Delaware.⁴

9 27. The Northern District of California has personal jurisdiction over Defendant named
10 in this action because Defendant is organized under the laws of California and conducts substantial
11 business in California and this District through itself and/or its subsidiaries.

12 28. Venue is proper in this District under 28 U.S.C. §1391(b) because California has
13 more than one judicial district and Defendant’s contacts in this District would be sufficient to
14 subject it to personal jurisdiction if this District were a separate State.

15 **IV. FACTUAL ALLEGATIONS**

16 ***Background***

17 29. Defendant services thousands of businesses in accepting and processing credit and
18 debit payments.

19 30. Prior to the Data Breach, Defendant acquired the PII of some or all of Plaintiff and
20 Class Members through unknown means.

21 31. Defendant had a duty to adopt reasonable measures to protect Plaintiff’s and Class
22 Members’ PII from involuntary disclosure to third parties and ensure that any affiliates with which
23

24 ³ Exhibit 3 (“Security Incident Notification,” dated December 16, 2020, provided to Maine
25 Attorney General by Paysafe).

26 ⁴ As a limited liability company, Defendant is “a citizen of every state of which its
27 owners/members are citizens.” *Johnson v. Columbia Props. Anchorage, LP*, 437 F.3d 894, 899
(9th Cir. 2006). Defendant is a citizen of Delaware because its sole member is a Delaware
28 corporation, Paysafe Holdings (US) Corp.

1 Defendant directly or indirectly shared the PII also adopted reasonable measures to protect it.

2 ***The Data Breach***

3 32. Beginning on or about December 16, 2020, Defendant sent Plaintiff and Class
4 Members a *Notice of Data Breach*.⁵ Defendant informed the recipients of the notice that:

5
6 We are writing to inform you of a cybersecurity incident that may
7 have affected personal information related to you. You provided the
8 information to Merchant Services* in the course of enrolling for a
9 merchant account.

10 **WHAT HAPPENED** On November 6, 2020, through Merchant
11 Services'* internal cybersecurity program, we discovered a
12 potential compromise of a website used by part of our U.S. business.
13 We promptly initiated an investigation to determine the nature and
14 potential impact of the vulnerability. In the course of doing so, we
15 identified suspicious activity indicating that an unauthorized actor
16 submitted automated queries to the website. We created a secure
17 environment to test the queries, using available logs and other
18 information to assess potential impact. By November 19, 2020, we
19 determined that a subset of the queries identified might have
20 involved data held on the website. We analyzed logs and other
21 information available to assess whether those queries could have
22 returned information to unauthorized actors, and we engaged
23 external forensics experts to assist. By December 3, 2020, we
24 determined that some queries may have compromised certain
25 information held on the website, although the evidence is not
26 conclusive. At this time, we have identified evidence of suspicious
27 activity on the website between May 13, 2018, and November 24,
28 2020. We have notified law enforcement. Although we are not
aware of any evidence confirming that the activity resulted in
unauthorized actors acquiring or misusing your personal
information, we are providing this notice out of an abundance of
caution so that you can take steps to protect yourself.

29 **WHAT INFORMATION WAS INVOLVED** The information
30 about you that may have been accessed includes your name, contact
31 details, Social Security number, and bank account information. The
32 website did not hold customer transaction data, consumer data, or
33 payment card information. The website impacted is separate from
34 Merchant Services'* core processing and operating systems. The
35 website was part of a legacy system used internally and by a small
36 group of former Chi Payment agents, a group acquired in an

37 ⁵ See Exhibits 1 and 3.

1 acquisition of iPayment in 2018, and contains certain data of a
2 limited subset of merchants and agents.⁶

3 33. On or about December 16, 2020, Defendant began notifying various state Attorneys
4 General, including Maine's Attorney General, signed by "Merchant Services."⁷

5 34. Defendant admitted in the *Notice of Data Breach* and the letters to the Attorneys
6 General that one or more unauthorized third persons submitted automated queries to Defendant's
7 website and that some of these queries could have returned information to unauthorized actors,
8 including the names, contact details, Social Security numbers, and bank account information of
9 Plaintiff and Class Members.

10 35. In response to the Data Breach, Defendant claims that it "took steps to prevent
11 further unauthorized access and have closed the website. We continue to invest in cybersecurity,
12 including enhancing our website scanning practices and vulnerability detection program.
13 Additionally, we have arranged for you to obtain credit monitoring and identity monitoring
14 services at no cost to you for two years through Kroll, a leading provider of credit monitoring and
15 identity monitoring services."⁸

16 36. Plaintiff's and Class Members' unencrypted information may end up for sale on the
17 dark web, or simply fall into the hands of companies that will use the detailed PII for targeted
18 marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can
19 easily access the PII of Plaintiff and Class Members.

20 37. Defendant did not use reasonable security procedures and practices appropriate to
21 the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class
22 Members, causing Plaintiff's and Class Members' PII to be exposed.

23 ***Defendant Acquires, Collects and Stores Plaintiff's and Class Members' PII.***

24 38. Defendant acquired, collected, and stored Plaintiff's and Class Members' PII.

25 39. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Defendant

26 ⁶ Ex. 3, p. 3.

27 ⁷ Ex. 3, p. 4.

28 ⁸ Ex. 3, p. 3.

1 assumed legal and equitable duties and knew or should have known that it was responsible for
2 protecting Plaintiff's and Class Members' PII from disclosure and for ensuring that any affiliates
3 with which it shared the PII would also protect the PII from disclosure.

4 40. Plaintiff and the Class Members have taken reasonable steps to maintain the
5 confidentiality of their PII.

6 ***Securing PII and Preventing Breaches***

7 41. Defendant could have prevented this Data Breach by properly securing and
8 encrypting Plaintiff's and Class Members' PII and ensuring any affiliates with which it directly or
9 indirectly shared the PII also properly secured it. Or Defendant could have destroyed the data,
10 especially old data that Defendant had no legal duty to retain.

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

13 43. Despite the prevalence of public announcements of data breach and data security
14 compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the
15 proposed Class from being compromised.

16 44. The Federal Trade Commission ("FTC") defines identity theft as "a fraud
17 committed or attempted using the identifying information of another person without authority."⁹
18 The FTC describes "identifying information" as "any name or number that may be used, alone or
19 in conjunction with any other information, to identify a specific person," including, among other
20 things, "[n]ame, Social Security number, date of birth, official State or government issued driver's
21 license or identification number, alien registration number, government passport number,
22 employer or taxpayer identification number."¹⁰

23 45. The ramifications of Defendant's failure to keep Plaintiff's and Class Members' PII
24 are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent
25 use of that information and damage to victims may continue for years.

27 ⁹ 17 C.F.R. § 248.201 (2013).

28 ¹⁰ *Id.*

1 ***Value of Personal Identifiable Information***

2 46. The PII of individuals remains of high value to criminals, as evidenced by the prices
3 they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity
4 credentials. For example, personal information can be sold at a price ranging from \$40 to \$200,
5 and bank details have a price range of \$50 to \$200.¹¹ Experian reports that a stolen credit or debit
6 card number can sell for \$5 to \$110 on the dark web.¹² Criminals can also purchase access to entire
7 company data breaches from \$900 to \$4,500.¹³

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

13 A dishonest person who has your Social Security number can use it
14 to get other personal information about you. Identity thieves can use
15 your number and your good credit to apply for more credit in your
16 name. Then, they use the credit cards and don't pay the bills, it
17 damages your credit. You may not find out that someone is using
18 your number until you're turned down for credit, or you begin to get
19 calls from unknown creditors demanding payment for items you
20 never bought. Someone illegally using your Social Security number
21 and assuming your identity can cause a lot of problems.¹⁴

22 48. What is more, it is no easy task to change or cancel a stolen Social Security number.

23 ¹¹ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct.
24 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed March 30, 2022).

25 ¹² *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec.
26 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed March 30, 2022).

27 ¹³ *In the Dark*, VPNOverview, 2019, available at:
28 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed March 30, 2022).

¹⁴ Social Security Administration, *Identity Theft and Your Social Security Number*, available at:
<https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed March 30, 2022).

1 An individual cannot obtain a new Social Security number without significant paperwork and
2 evidence of actual misuse. In other words, preventive action to defend against the possibility of
3 misuse of a Social Security number is not permitted; an individual must show evidence of actual,
4 ongoing fraud activity to obtain a new number.

5 49. Even then, a new Social Security number may not be effective. According to Julie
6 Ferguson of the Identity Theft Resource Center, “The credit bureaus and banks are able to link the
7 new number very quickly to the old number, so all of that old bad information is quickly inherited
8 into the new Social Security number.”¹⁵

9 50. Based on the foregoing, the information compromised in the Data Breach is
10 significantly more valuable than the loss of, for example, credit card information in a retailer data
11 breach, because, there, victims can cancel or close credit and debit card accounts. The information
12 compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to
13 change—Social Security number, driver’s license number or government-issued identification
14 number, name, and date of birth.

15 51. This data demands a much higher price on the black market. Martin Walter, senior
16 director at cybersecurity firm RedSeal, explained, “Compared to credit card information,
17 personally identifiable information and Social Security numbers are worth more than 10x on the
18 black market.”¹⁶

19 52. Among other forms of fraud, identity thieves may obtain driver’s licenses,
20 government benefits, medical services, and housing or even give false information to police.

21 53. The PII of Plaintiff and Class Members was taken by hackers to engage in identity
22 theft or and or to sell it to others criminals who will purchase the PII for that purpose. The
23

24 ¹⁵ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR
25 (Feb. 9, 2015), available at: [http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-
s-hackers-has-millionsworrying-about-identity-theft](http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft) (last accessed March 30, 2022).

26 ¹⁶ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card
27 Numbers*, IT World, (Feb. 6, 2015), available at:
28 [https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-
price-of-stolen-credit-card-numbers.html](https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html) (last accessed March 30, 2022).

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

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

5 [L]aw enforcement officials told us that in some cases, stolen data
6 may be held for up to a year or more before being used to commit
7 identity theft. Further, once stolen data have been sold or posted on
8 the Web, fraudulent use of that information may continue for years.
As a result, studies that attempt to measure the harm resulting from
data breaches cannot necessarily rule out all future harm.¹⁷

9
10 55. At all relevant times, Defendant knew, or reasonably should have known, of the
11 importance of safeguarding Plaintiff’s and Class Members’ PII, including Social Security numbers
12 and dates of birth, and of the foreseeable consequences that would occur if Defendant’s or its
13 affiliate’s data security system was breached, including, specifically, the significant costs that
14 would be imposed on Plaintiff and Class Members as a result of a breach.

15 56. Plaintiff and Class Members now face years of constant surveillance of their
16 financial and personal records, monitoring, and loss of rights. The Class is incurring and will
17 continue to incur such damages in addition to any fraudulent use of their PII.

18 57. Defendant was, or should have been, fully aware of the unique type and the
19 significant volume of data on Defendant’s or its affiliate’s network, amounting to potentially tens
20 of thousands of individuals’ detailed, personal information and thus, the significant number of
21 individuals who would be harmed by the exposure of the unencrypted data.

22 58. To date, Defendant’s affiliate, PGHL, has offered Plaintiff and Class Members only
23 two years of identity theft protection services through a single credit monitoring and identity
24 monitoring service, Kroll. The offered service is inadequate to protect Plaintiff and Class Members
25 from the threats they face for years to come, particularly in light of the PII at issue here.

26 59. The injuries to Plaintiff and Class Members were directly and proximately caused

27 ¹⁷ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:
28 <http://www.gao.gov/new.items/d07737.pdf> (last accessed March 30, 2022).

1 by Defendant’s failure to implement, maintain, and ensure adequate data security measures for the
2 PII of Plaintiff and Class Members.

3 ***Plaintiff Kamal Bitmouni’s Experience***

4 60. Mr. Bitmouni received the Notice of Data Breach, dated December 16, 2020, on or
5 about that date.

6 61. On or about December 5, 2020, Plaintiff attempted to log into his personal checking
7 account and discovered that he was denied access. He then contacted his bank and discovered that
8 unknown, unauthorized third-parties had used Mr. Bitmouni’s PII, including but not limited to his
9 name, bank account information, and Social Security number, to access his checking account in
10 an attempt to divert Mr. Bitmouni’s funds and had requested an access code for the account from
11 a device Plaintiff did not have access to or own.

12 62. Upon regaining access to his account, Plaintiff discovered that these unknown,
13 unauthorized third parties had been in the process of diverting his funds from this account when
14 he discovered their actions.

15 63. As part of this attempt to divert his funds, these unknown, unauthorized third parties
16 stopped payments on a number of Plaintiff’s scheduled payments, including a rental payment of
17 \$1,600.

18 64. Plaintiff had to exhaust more than eight hours communicating with his bank,
19 landlord, and others to discover what happened and to attempt to resolve the fraud.

20 65. The delays caused by these “stopped payments” resulted in Plaintiff’s rent being
21 approximately forty-five (45) days late, as it took that many days for the bank to resolve the
22 fraudulent activity.

23 66. As a result of the Data Breach notice and the unauthorized access to his checking
24 account, Mr. Bitmouni spent time dealing with the consequences of the Data Breach, which
25 includes time spent communicating with his bank to stop the fraudulent transfers, verifying the
26 legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance
27

1 options, signing up and routinely monitoring the credit monitoring offered by Defendant, and self-
2 monitoring his accounts. This time has been lost forever and cannot be recaptured.

3 67. The credit monitoring service provided by Defendant to Mr. Bitmouni warned him
4 on or about January 13, 2021, that his PII is potentially exposed on the dark web.

5 68. Additionally, Mr. Bitmouni is very careful about sharing his PII. He has never
6 knowingly transmitted unencrypted PII over the internet or any other unsecured source.

7 69. Mr. Bitmouni stores any documents containing his PII in a safe and secure location
8 or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for
9 his various online accounts.

10 70. Mr. Bitmouni suffered actual injury in the form of damages to and diminution in
11 the value of his PII—a form of intangible property that Mr. Bitmouni entrusted to Defendant for
12 its services to accept payment card payments, which was compromised in and as a result of the
13 Data Breach.

14 71. Mr. Bitmouni suffered lost time, annoyance, interference, and inconvenience as a
15 result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

16 72. Mr. Bitmouni has suffered imminent and impending injury arising from the
17 substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially
18 his Social Security number, in combination with his name and bank account information, being
19 placed in the hands of unauthorized third-parties and possibly criminals.

20 73. Mr. Bitmouni has a continuing interest in ensuring that his PII, which, upon
21 information and belief, remains backed up in Defendant's possession, is protected and safeguarded
22 from future breaches.

23 **V. CLASS ALLEGATIONS**

24 74. Plaintiff brings this nationwide class action on behalf of himself and on behalf of
25 all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules
26 of Civil Procedure.

27 75. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

1 All individuals who are residents of the United States and whose PII
2 was or may have been accessed during the cybersecurity incident
3 referenced in the Notice of Data Breach dated December 16, 2020
4 that Merchant Services (including CHI Payments, iPayment, and
Paysafe) sent to Plaintiff (the “Nationwide Class”).

5 76. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the
6 Nationwide Class, Plaintiff Kamal Bitmouni asserts claims on behalf of a separate statewide
7 subclass, defined as follows:

8 All individuals who are residents of California and whose PII was
9 or may have been accessed during the cybersecurity incident
10 referenced in the Notice of Data Breach dated December 16, 2020
11 that Merchant Services (including CHI Payments, iPayment, and
Paysafe) sent to Plaintiff (the “California Class”).

12 77. Excluded from the Classes are the following individuals and/or entities: Defendant
13 and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which
14 Defendant has a controlling interest; all individuals who make a timely election to be excluded
15 from this proceeding using the correct protocol for opting out; any and all federal, state or local
16 governments, including but not limited to their departments, agencies, divisions, bureaus, boards,
17 sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this
18 litigation, as well as their immediate family members.

19 78. Plaintiff reserves the right to modify or amend the definition of the proposed classes
20 before the Court determines whether certification is appropriate.

21 79. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the “Class”) are so
22 numerous that joinder of all members is impracticable. Defendant’s affiliate PGHL has identified
23 tens of thousands of individuals whose PII may have been improperly accessed in the Data Breach,
24 and the Class is apparently identifiable within Defendant’s records. PGHL advised Maine’s
25 Attorney General that the Data Breach affected 91,706 individuals.

26 80. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact
27 common to the Classes exist and predominate over any questions affecting only individual Class
28

1 Members. These include:

- 2 a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and
3 Class Members;
- 4 b. Whether Defendant had a duty not to disclose the PII of Plaintiff and Class Members
5 to unauthorized third parties;
- 6 c. Whether Defendant had a duty not to use the PII of Plaintiff and Class Members for
7 non-business purposes;
- 8 d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class
9 Members and ensure its affiliates adequately safeguarded the PII;
- 10 e. Whether and when Defendant actually learned of the Data Breach;
- 11 f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and
12 Class Members that their PII had been compromised;
- 13 g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class
14 Members that their PII had been compromised;
- 15 h. Whether Defendant failed to implement and maintain reasonable security procedures
16 and practices appropriate to the nature and scope of the information compromised in
17 the Data Breach and ensure its affiliates did the same;
- 18 i. Whether Defendant adequately addressed and fixed the vulnerabilities which
19 permitted the Data Breach to occur and ensured its affiliates did the same;
- 20 j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to
21 safeguard the PII of Plaintiff and Class Members;
- 22 k. Whether Plaintiff and Class Members are entitled to actual, consequential, nominal,
23 and/or statutory damages as a result of Defendant's wrongful conduct;
- 24 l. Whether Plaintiff and Class Members are entitled to restitution as a result of
25 Defendant's wrongful conduct; and
- 26 m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the
27 imminent and currently ongoing harm faced as a result of the Data Breach.

1 include, but are not limited to:

- 2 a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise
3 due care in collecting, storing, using, and safeguarding their PII and ensure its
4 affiliates with which it directly or indirectly shared the PII did the same;
- 5 b. Whether Defendant breached a legal duty to Plaintiff and Class Members to
6 exercise due care in collecting, storing, using, and safeguarding their PII and
7 ensure its affiliates with which it directly or indirectly shared the PII did the
8 same;
- 9 c. Whether Defendant failed to comply with its own policies and applicable laws,
10 regulations, and industry standards relating to data security and ensure its
11 affiliates with which it directly or indirectly shared the PII did the same;
- 12 d. Whether Defendant adequately and accurately informed Plaintiff and Class
13 Members that their PII had been compromised;
- 14 e. Whether Defendant failed to implement and maintain reasonable security
15 procedures and practices appropriate to the nature and scope of the information
16 compromised in the Data Breach and failed to ensure its affiliates with which it
17 directly or indirectly shared the PII did the same;
- 18 f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing
19 to safeguard the PII of Plaintiff and Class Members and failing to ensure its
20 affiliates with which it directly or indirectly shared the PII did the same; and,
- 21 g. Whether Class Members are entitled to actual, consequential, nominal, and/or
22 statutory damages and/or injunctive relief as a result of Defendant's wrongful
23 conduct.

24 **COUNT I**
25 **Negligence**

26 **(On Behalf of Plaintiff and the Nationwide Class)**

27 91. Plaintiff and Class Members re-allege and incorporate by reference herein all of the
28 allegations contained in paragraphs 1 through 90.

1 92. Plaintiff acquired and stored the PII of Plaintiff and Class Members and shared the
2 PII, directly or indirectly, with its affiliates.

3 93. Defendant has full knowledge of the sensitivity of the PII and the types of harm
4 that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

5 94. Defendant knew or reasonably should have known that the failure of Defendant or
6 its affiliates to exercise due care in the collecting, storing, and using of Plaintiff's and Class
7 Members' PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the
8 harm occurred through the criminal acts of a third party.

9 95. Defendant had a duty to exercise reasonable care in safeguarding, securing, and
10 protecting such information from being compromised, lost, stolen, misused, and/or disclosed to
11 unauthorized parties, including ensuring its affiliates did the same. This duty includes, among
12 other things, designing, maintaining, and testing Defendant's security protocols to ensure that
13 Plaintiff's and Class Members' information in Defendant's possession was adequately secured and
14 ensuring its affiliates with which it directly or indirectly shared the PII did the same.

15 96. Defendant also had a duty to exercise appropriate clearinghouse practices to remove
16 Plaintiff's and Class Members' PII it was no longer required to retain pursuant to regulations and
17 ensure its affiliates with which it directly or indirectly shared the PII did the same.

18 97. Defendant also had a duty to have procedures in place to detect and prevent the
19 improper access and misuse of Plaintiff's and Class Members' PII and ensure its affiliates with
20 which it directly or indirectly shared the PII did the same.

21 98. Defendant was subject to an "independent duty," untethered to any contract
22 between Defendant and Plaintiff or Class Members.

23 99. A breach of security, unauthorized access, and resulting injury to Plaintiff and the
24 Class Members was reasonably foreseeable, particularly in light of Defendant's and its affiliates'
25 inadequate security practices.

26 100. Plaintiff and Class Members were the foreseeable and probable victims of any
27 inadequate security practices and procedures. Defendant knew or should have known of the

1 inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of
2 providing adequate security of that PII, the necessity for encrypting PII stored on Defendant's
3 systems, and the need to ensure its affiliates with which it directly or indirectly shared the PII did
4 the same.

5 101. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class
6 Members. Defendant's misconduct included, but was not limited to, their failure to take the steps
7 and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also
8 included its decision not to comply with industry standards for the safekeeping of Plaintiff's and
9 Class Members' PII, including basic encryption techniques freely available to Defendant, and its
10 failure to ensure its affiliates with which it directly or indirectly shared the PII did the same.

11 102. Plaintiff and the Class Members had no ability to protect their PII that was in, and
12 possibly remains in, Defendant's or its affiliates' possession.

13 103. Defendant was in a position to protect against the harm suffered by Plaintiff and
14 Class Members as a result of the Data Breach.

15 104. Defendant had and continues to have a duty to adequately disclose that the PII of
16 Plaintiff and Class Members within Defendant's possession might have been compromised, how
17 it was compromised, and precisely the types of data that were compromised and when. Such notice
18 was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and
19 repair any identity theft and the fraudulent use of their PII by third parties.

20 105. Defendant had a duty to employ proper procedures to prevent the unauthorized
21 dissemination of the PII of Plaintiff and Class Members and ensure its affiliates with which it
22 directly or indirectly shared the PII did the same.

23 106. Defendant has admitted that the PII of Plaintiff and Class Members was wrongfully
24 lost and disclosed to unauthorized third persons as a result of the Data Breach.

25 107. Defendant, through its actions and/or omissions, unlawfully breached its duties to
26 Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable
27 care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII

1 was within Defendant's possession or control and failing to ensure its affiliates with which it
2 directly or indirectly shared the PII did the same.

3 108. Defendant improperly and inadequately safeguarded the PII of Plaintiff and Class
4 Members in deviation of standard industry rules, regulations, and practices at the time of the Data
5 Breach and failed to ensure its affiliates with which it directly or indirectly shared the PII did the
6 same

7 109. Defendant failed to heed industry warnings and alerts to provide adequate
8 safeguards to protect Plaintiff's and Class Members' PII in the face of increased risk of theft and
9 failed to ensure its affiliates with which it directly or indirectly shared the PII did the same.

10 110. Defendant, through its actions and/or omissions, unlawfully breached its duty to
11 Plaintiff and Class Members by failing to have appropriate procedures in place to detect and
12 prevent dissemination of Plaintiff's and Class Members' PII and failing to ensure its affiliates with
13 which it directly or indirectly shared the PII did the same.

14 111. Defendant breached its duty to exercise appropriate clearinghouse practices by
15 failing to remove Plaintiff's and Class Members' PII it was no longer required to retain pursuant
16 to regulations and failing to ensure its affiliates with which it directly or indirectly shared the PII
17 did the same.

18 112. Defendant, through its actions and/or omissions, unlawfully breached its duty to
19 adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data
20 Breach and failed to ensure its affiliates with which it directly or indirectly shared the PII did the
21 same.

22 113. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and
23 Class Members, the PII of Plaintiff and Class Members would not have been compromised.

24 114. There is a close causal connection between Defendant's failure to implement
25 security measures to protect the PII of Plaintiff and Class Members, and ensure its affiliates with
26 which it directly or indirectly shared the PII did the same, and the harm suffered or risk of imminent
27 harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' PII was lost and accessed

1 as the proximate result of Defendant’s failure to exercise reasonable care in safeguarding such PII
2 by adopting, implementing, and maintaining appropriate security measures and failure to ensure
3 its affiliates with which it directly or indirectly shared the PII did the same.

4 115. Additionally, Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting
5 commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by
6 businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC
7 publications and orders described above also form part of the basis of Defendant’s duty in this
8 regard.

9 116. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures
10 to protect PII and not complying with applicable industry standards, as described in detail herein,
11 and failing to ensure its affiliated with which it directly or indirectly shared the PII did the same.
12 Defendant’s conduct was particularly unreasonable given the nature and amount of PII it obtained,
13 stored, and directly or indirectly shared with its affiliates and the foreseeable consequences of the
14 immense damages that would result to Plaintiff and Class Members.

15 117. Defendant’s violation of Section 5 of the FTC Act constitutes negligence *per se*.

16 118. Plaintiff and Class Members are within the class of persons that the FTC Act was
17 intended to protect.

18 119. The harm that occurred as a result of the Data Breach is the type of harm the FTC
19 Act was intended to guard against. The FTC has pursued enforcement actions against businesses,
20 which, as a result of its failure to employ reasonable data security measures and avoid unfair and
21 deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

22 120. As a direct and proximate result of Defendant’s negligence and negligence *per se*,
23 Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i)
24 actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise,
25 publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention,
26 detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost
27 opportunity costs associated with effort expended and the loss of productivity addressing and
28

1 attempting to mitigate the present and continuing consequences of the Data Breach, including but
2 not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud
3 and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued
4 risk to their PII, which remain in Defendant's and its affiliate's possession and is subject to further
5 unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate
6 measures to protect Plaintiff's and Class Members' PII in its continued possession; and (viii)
7 present and continuing costs in terms of time, effort, and money that will be expended to prevent,
8 detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the
9 remainder of the lives of Plaintiff and Class Members.

10 121. As a direct and proximate result of Defendant's negligence and negligence *per se*,
11 Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or
12 harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic
13 and non-economic losses.

14 122. Additionally, as a direct and proximate result of Defendant's negligence and
15 negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks
16 of exposure of their PII, which remain in Defendant's possession and is subject to further
17 unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate
18 measures to protect the PII in its continued possession.

19 123. As a direct and proximate result of Defendant's negligence and negligence *per se*,
20 Plaintiff and Class Members are entitled to recover actual, consequential, and nominal damages.

21 **COUNT II**
22 **Invasion of Privacy**
23 **(On Behalf of Plaintiff and the Nationwide Class)**

24 124. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein
25 all of the allegations contained in paragraphs 1 through 90.

26 125. Plaintiff and the Nationwide Class had a legitimate expectation of privacy to their
27 PII and were entitled to the protection of this information against disclosure to unauthorized third
28

1 parties.

2 126. Defendant owed a duty to Plaintiff and the Nationwide Class to keep their PII
3 confidential.

4 127. Defendant failed to protect and directly or indirectly through its affiliates released
5 to unknown and unauthorized third parties the PII of Plaintiff and the Nationwide Class.

6 128. Defendant allowed unauthorized and unknown third parties access to and
7 examination of the PII of Plaintiff and the Nationwide Class the Nationwide Class, by way of
8 Defendant's failure to protect the PII and failure to ensure its affiliates with which it directly or
9 indirectly shared the PII did the same.

10 129. The unauthorized release to, custody of, and examination by unauthorized third
11 parties of the PII of Plaintiff and the Nationwide Class is highly offensive to a reasonable person.

12 130. The intrusion was into a place or thing, which was private and is entitled to be
13 private.

14 131. The Data Breach at the hands of Defendant constitutes an intentional interference
15 with Plaintiff's and the Nationwide Class's interest in solitude or seclusion, either as to their
16 persons or as to their private affairs or concerns, of a kind that would be highly offensive to a
17 reasonable person.

18 132. Defendant acted with a knowing state of mind when it permitted the Data Breach
19 to occur because it was with actual knowledge that its or its affiliates' information security
20 practices were inadequate and insufficient.

21 133. Because Defendant acted with this knowing state of mind, it had notice and knew
22 the inadequate and insufficient information security practices would cause injury and harm to
23 Plaintiff and the Nationwide Class.

24 134. As a proximate result of the above acts and omissions of Defendant, the PII of
25 Plaintiff and the Nationwide Class was disclosed to third parties without authorization, causing
26 Plaintiff and the Nationwide Class to suffer damages.

1 135. Unless and until enjoined, and restrained by order of this Court, Defendant's
2 wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the
3 Nationwide Class in that the PII maintained by Defendant can be viewed, distributed, and used by
4 unauthorized persons for years to come. Plaintiff and the Nationwide Class have no adequate
5 remedy at law for the injuries in that a judgment for monetary damages will not end the invasion
6 of privacy for Plaintiff and the Nationwide Class.

7 136. As a direct and proximate result of Defendant's invasion of privacy, Plaintiff and
8 the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

9 **COUNT III**
10 **Violation of California's Unfair Competition Law**
11 **(Cal. Bus. & Prof. Code § 17200, *et seq.*)**
12 **(On Behalf of Plaintiff and the Nationwide Class)**

13 137. Plaintiff and Class Members re-allege and incorporate by reference herein all of the
14 allegations contained in paragraphs 1 through 90.

15 138. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair
16 business practices within the meaning of California's Unfair Competition Law ("UCL"), Business
17 and Professions Code § 17200, *et seq.*

18 139. Defendant stored the PII of Plaintiff and Class Members in its computer systems
19 and directly or indirectly shared the PII with its affiliates, which stored the PII in their computer
20 systems.

21 140. Defendant knew or should have known it and its affiliates did not employ
22 reasonable, industry standard, and appropriate security measures that complied with federal
23 regulations and that would have kept Plaintiff's and Class Members' PII secure and prevented the
24 loss or misuse of that PII.

25 141. Defendant did not disclose at any time that Plaintiff's and Class Members' PII was
26 vulnerable to hackers because Defendant's and its affiliates' data security measures were
27 inadequate and outdated, and Defendant and its affiliates were the only ones in possession of that
28 material information, which Defendant had a duty to disclose.

1 to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiffs
2 and Class Members, directly causing the harms alleged below.

3 **148. Defendant engaged in unfair business practices under the “tethering test.”**

4 Defendant’s actions and omissions, as described in detail above, violated fundamental public
5 policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 (“The
6 Legislature declares that . . . all individuals have a right of privacy in information pertaining to
7 them The increasing use of computers . . . has greatly magnified the potential risk to
8 individual privacy that can occur from the maintenance of personal information.”); Cal. Civ. Code
9 § 1798.81.5(a) (“It is the intent of the Legislature to ensure that personal information about
10 California residents is protected.”); Cal. Bus. & Prof. Code § 22578 (“It is the intent of the
11 Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide
12 concern.”). Defendant’s acts and omissions thus amount to a violation of the law.

13 **149. Defendant engaged in unfair business practices under the “FTC test.”** The

14 harm caused by Defendant’s actions and omissions, as described in detail above, is substantial in
15 that it affects thousands of Class Members and has caused those persons to suffer actual harms.
16 Such harms include a substantial risk of identity theft, disclosure of Plaintiff’s and Class Members’
17 PII to third parties without their consent, diminution in value of their PII, consequential out of
18 pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other
19 expenses relating to identity theft losses or protective measures. This harm continues given the
20 fact that Plaintiff’s and Class Members’ PII remains in Defendant’s and its affiliates’ possession,
21 without adequate protection, and is also in the hands of those who obtained it without their consent.
22 Defendant’s actions and omissions violated Section 5(a) of the Federal Trade Commission Act.
23 *See* 15 U.S.C. § 45(n) (defining “unfair acts or practices” as those that “cause[] or [are] likely to
24 cause substantial injury to consumers which [are] not reasonably avoidable by consumers
25 themselves and not outweighed by countervailing benefits to consumers or to competition”); *see*
26 *also, e.g., In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016)

1 (failure to employ reasonable and appropriate measures to secure personal information collected
2 violated § 5(a) of FTC Act).

3 150. Plaintiff and Class Members suffered injury in fact and lost money or property as
4 the result of Defendant’s unfair business practices. Plaintiff and Class Members’ PII was taken
5 and is in the hands of those who will use it for their own advantage, or is being sold for value,
6 making it clear that the hacked information is of tangible value. Plaintiff and Class Members have
7 also suffered consequential out of pocket losses for procuring credit freeze or protection services,
8 identity theft monitoring, and other expenses relating to identity theft losses or protective
9 measures.

10 151. As a result of Defendant’s unlawful and unfair business practices in violation of the
11 UCL, Plaintiff and Class Members are entitled to damages, injunctive relief, and reasonable
12 attorneys’ fees and costs.

13 **COUNT IV**
14 **Violation of California’s Consumer Privacy Act**
15 **(Cal. Civ. Code § 1798.150)**
16 **(On behalf of Plaintiff and the California Class)**

17 152. Plaintiff and California Class members re-allege and incorporate by reference
18 herein all of the allegations contained in paragraphs 1 through 90.

19 153. Defendant violated section 1798.150(a) of the California Consumer Privacy Act
20 (“CCPA”) by failing to prevent Plaintiff’s and California Class members’ PII from unauthorized
21 access and exfiltration, theft, or disclosure as a result of Defendant’s violations of its duty to
22 implement and maintain reasonable security procedures and practices appropriate to the nature of
23 the information to protect the PII of Plaintiff and California Class members and failure to ensure
24 its affiliates with which it directly or indirectly shared the PII did the same.

25 154. As a direct and proximate result of Defendant’s acts, Plaintiff’s and California Class
26 members’ PII was subjected to unauthorized access and exfiltration, theft, or disclosure as a result
27 of Defendant’s violation of the duty.

1 the Court deems proper; and attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

2 **PRAYER FOR RELIEF**

3 **WHEREFORE**, Plaintiff, on behalf of himself and all Class Members, requests judgment
4 against Defendant and that the Court grant the following:

- 5 A. For an Order certifying the Nationwide Class and the California Class as defined
6 herein, and appointing Plaintiff and their Counsel to represent the Class;
- 7 B. For equitable relief enjoining Defendant from engaging in the wrongful conduct
8 complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and
9 Class Members' PII, and from refusing to issue prompt, complete, any accurate
10 disclosures to Plaintiff and the Class Members;
- 11 C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive
12 and other equitable relief as is necessary to protect the interests of Plaintiff and
13 Class Members, including but not limited to an order:
- 14 i. prohibiting Defendant from engaging in the wrongful and unlawful acts
15 described herein;
 - 16 ii. requiring Defendant to protect, including through encryption, all data collected
17 through the course of its business in accordance with all applicable regulations,
18 industry standards, and federal, state or local laws;
 - 19 iii. requiring Defendant to delete, destroy, and purge the personal identifying
20 information of Plaintiff and Class Members unless Defendant can provide to
21 the Court reasonable justification for the retention and use of such information
22 when weighed against the privacy interests of Plaintiff and Class Members;
 - 23 iv. requiring Defendant to implement and maintain a comprehensive Information
24 Security Program designed to protect the confidentiality and integrity of the
25 personal identifying information of Plaintiff's and Class Members' personal
26 identifying information;
 - 27 v. prohibiting Defendant from maintaining Plaintiff's and Class Members'

- 1 personal identifying information on a cloud-based database;
- 2 vi. requiring Defendant to engage independent third-party security
- 3 auditors/penetration testers as well as internal security personnel to conduct
- 4 testing, including simulated attacks, penetration tests, and audits on
- 5 Defendant's systems on a periodic basis, and ordering Defendant to promptly
- 6 correct any problems or issues detected by such third-party security auditors;
- 7 vii. requiring Defendant to engage independent third-party security auditors and
- 8 internal personnel to run automated security monitoring;
- 9 viii. requiring Defendant to audit, test, and train its security personnel regarding any
- 10 new or modified procedures;
- 11 ix. requiring Defendant to segment data by, among other things, creating firewalls
- 12 and access controls so that if one area of Defendant's network is compromised,
- 13 hackers cannot gain access to other portions of Defendant's systems;
- 14 x. requiring Defendant to conduct regular database scanning and securing checks;
- 15 xi. requiring Defendant to establish an information security training program that
- 16 includes at least annual information security training for all employees, with
- 17 additional training to be provided as appropriate based upon the employees'
- 18 respective responsibilities with handling personal identifying information, as
- 19 well as protecting the personal identifying information of Plaintiff and Class
- 20 Members;
- 21 xii. requiring Defendant to routinely and continually conduct internal training and
- 22 education, and on an annual basis to inform internal security personnel how to
- 23 identify and contain a breach when it occurs and what to do in response to a
- 24 breach;
- 25 xiii. requiring Defendant to implement a system of tests to assess its respective
- 26 employees' knowledge of the education programs discussed in the preceding
- 27 subparagraphs, as well as randomly and periodically testing employees'
- 28

1 compliance with Defendant's policies, programs, and systems for protecting
2 personal identifying information;

3 xiv. requiring Defendant to implement, maintain, regularly review, and revise as
4 necessary a threat management program designed to appropriately monitor
5 Defendant's information networks for threats, both internal and external, and
6 assess whether monitoring tools are appropriately configured, tested, and
7 updated;

8 xv. requiring Defendant to meaningfully educate all Class Members about the
9 threats that they face as a result of the loss of their confidential personal
10 identifying information to third parties, as well as the steps affected individuals
11 must take to protect themselves;

12 xvi. requiring Defendant to implement logging and monitoring programs sufficient
13 to track traffic to and from Defendant's servers; and for a period of 10 years,
14 appointing a qualified and independent third party assessor to conduct a SOC 2
15 Type 2 attestation on an annual basis to evaluate Defendant's compliance with
16 the terms of the Court's final judgment, to provide such report to the Court and
17 to counsel for the class, and to report any deficiencies with compliance of the
18 Court's final judgment; For an award of damages, including actual, nominal,
19 and consequential damages, as allowed by law in an amount to be determined;

20 D. For an award of damages, including actual, nominal, and consequential damages,
21 as allowed by law in an amount to be determined;

22 E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

23 F. For prejudgment interest on all amounts awarded; and

24 G. Such other and further relief as this Court may deem just and proper.

25
26 **DEMAND FOR JURY TRIAL**

27 Plaintiff hereby demands that this matter be tried before a jury.

1 Date: March 30, 2022

Respectfully Submitted,

2 By: /s/ M. Anderson Berry
3 M. Anderson Berry (SBN 262879)
4 Gregory Haroutunian (SBN 300263)
5 **CLAYEO C. ARNOLD,**
6 **A PROFESSIONAL LAW CORP.**
7 865 Howe Avenue
8 Sacramento, CA 95825
9 Telephone: (916) 239-4778
10 Facsimile: (916) 924-1829
11 aberry@justice4you.com
12 gharoutunian@justice4you.com

13 JOHN A. YANCHUNIS
14 (*Pro Hac Vice*)
15 RYAN D. MAXEY
16 (*Pro Hac Vice*)
17 **MORGAN & MORGAN**
18 201 N. Franklin Street, 7th Floor
19 Tampa, Florida 33602
20 (813) 223-5505
21 jyanchunis@ForThePeople.com
22 rmaxey@ForThePeople.com

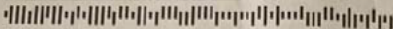
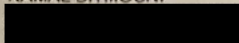
23 *Attorneys for Plaintiff*

Exhibit 1



17 1 6353 *****MIXED AADC 300
KAMAL BITMOUNI

December 16, 2020



NOTICE OF DATA BREACH

Dear Kamal Bitmouni,

We are writing to inform you of a cybersecurity incident that may have affected personal information related to you. You provided the information to Merchant Services* in the course of enrolling for a merchant account.

WHAT HAPPENED

On November 6, 2020, through Merchant Services* internal cybersecurity program, we discovered a potential compromise of a website used by part of our U.S. business. We promptly initiated an investigation to determine the nature and potential impact of the vulnerability. In the course of doing so, we identified suspicious activity indicating that an unauthorized actor submitted automated queries to the website. We created a secure environment to test the queries, using available logs and other information to assess potential impact. By November 19, 2020, we determined that a subset of the queries identified might have involved data held on the website. We analyzed logs and other information available to assess whether those queries could have returned information to unauthorized actors, and we engaged external forensics experts to assist. By December 3, 2020, we determined that some queries may have compromised certain information held on the website, although the evidence is not conclusive. At this time, we have identified evidence of suspicious activity on the website between May 13, 2018, and November 24, 2020. We have notified law enforcement. Although we are not aware of any evidence confirming that the activity resulted in unauthorized actors acquiring or misusing your personal information, we are providing this notice out of an abundance of caution so that you can take steps to protect yourself.

WHAT INFORMATION WAS INVOLVED

The information about you that may have been accessed includes your name, contact details, Social Security number, and bank account information. The website did not hold customer transaction data, consumer data, or payment card information. The website impacted is separate from Merchant Services* core processing and operating systems. The website was part of a legacy system used internally and by a small group of former Chi Payment agents, a group acquired in an acquisition of iPayment in 2018, and contains certain data of a limited subset of merchants and agents.

WHAT WE ARE DOING

We take the privacy and security of your personal information seriously. After discovering the incident, we took steps to prevent further unauthorized access and have closed the website. We continue to invest in cybersecurity, including enhancing our website scanning practices and vulnerability detection program. Additionally, we have arranged for you to obtain credit monitoring and identity monitoring services at no cost to you for two years through Kroll, a leading provider of credit monitoring and identity monitoring services. Information regarding the package of services is included in Attachment 2 to this letter.

WHAT YOU CAN DO

We are not aware of any evidence indicating that your personal information has been misused or sold. Out of an abundance of caution, we recommend that you remain vigilant and review your financial records and statements for signs of suspicious activity. Please find additional information in Attachment 1 to this letter. As noted above, you can activate, at no cost to you, in the Kroll credit monitoring and identity monitoring services. Information about activation is contained in Attachment 2 to this letter.

FOR MORE INFORMATION

If you have any questions or need additional information, please call 1-833-971-3287, Monday through Friday from 8:00 am to 5:30 pm Central Time, excluding major U.S. holidays. Be prepared to provide your membership number:



We apologize for any inconvenience this may cause.

Sincerely,

Merchant Services

Enclosures * Merchant Services includes, for purposes of this notification, CHI Payments, iPayment, and Paysafe.

PO Box 8339, The Woodlands, TX 77387-8339

ELN-6007-1220-6353

Attachment 1: Additional Information

You should be cautious about using email to provide sensitive personal information, whether sending it yourself or in response to email requests. You should also be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software on your devices or to trick you into sharing valuable personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at <https://www.consumer.ftc.gov/articles/0003-phishing>.

You should review your financial statements and accounts for signs of suspicious transactions and activities. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to local law enforcement, your State's Attorney General's office, or the FTC. If you are a resident of Rhode Island, you have the right to obtain a police report. You will find contact information for some of those entities below. If you discover unauthorized charges, promptly inform the relevant payment card companies and financial institutions.

Fraud Alert Information

Whether or not you enroll in the credit monitoring product offered, we recommend that you consider placing a free "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Fraud alerts last one year. Identity theft victims can get an extended fraud alert for seven years.

Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. You may also contact any of the consumer reporting agencies or the FTC for more information regarding fraud alerts. The contact information for the three nationwide credit reporting companies is:

Equifax
PO Box 740256
Atlanta, GA 30374
www.alerts.equifax.com
1-800-525-6285

TransUnion
PO Box 2000
Chester, PA 19016
www.transunion.com/fraud
1-800-680-7289

Experian
PO Box 9554
Allen, TX 75013
www.experian.com/fraud
1-888-397-3742

Free Credit Report Information

You have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score. Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud and identity theft. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency or state attorney general and file a police report. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also should file a complaint with the FTC using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcement for their investigations.

You may also contact the FTC at the contact information below to learn more about identity theft and the steps you can take to protect yourself. If you are a resident of the District of Columbia, Maryland, North Carolina, Iowa, Oregon, or Rhode Island, you can also reach out to your respective state's Attorney General's office at the contact information below. All other residents can find information on how to contact your state attorney general at www.naag.org/naag/attorneys-general/whos-my-ag.php.

Attachment 2: Credit Monitoring and Identity Theft Services Enrollment Information

Kroll | A Division of
DUFF & PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.
You have until **March 18, 2021** to activate your identity monitoring services.

Membership Number: [REDACTED]

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

* Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-FTC.HELP (382.4357) / www.ftc.gov/idtheft

North Carolina Attorney General's Office
90001 Mail Service Center
Raleigh, NC 27699
1-919-716-6400 / <https://ncdoj.gov/>

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
1-877-877-9392 / <https://justice.oregon.gov>

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
1-202-727-3400 / oag.dc.gov

Maryland Attorney General's Office
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023 / www.marylandattorneygeneral.gov

Rhode Island Attorney General's Office
150 South Main Street
Providence, Rhode Island 02903
1-401-274-4400 / <http://www.riag.ri.gov/>

Consumer Protection Division
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319
1-515-281-5926 / www.iowaattorneygeneral.gov

Security Freeze Information

You have the right to request a free Security Freeze (aka "Credit Freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a Credit Freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A Credit Freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. You may also contact any of the consumer reporting agencies or the FTC for more information regarding security freezes.

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
1-800-349-9960

TransUnion Security Freeze
PO Box 2000
Chester, PA 19016
www.transunion.com/freeze
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742

To request a Credit Freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

Exhibit 2

Office of the Maine Attorney General

[Home](#) > [Consumer Information](#) > [Privacy, Identity Theft and Data Security Breaches](#) > [Data Breach Notifications](#)

Data Breach Notifications

Entity Information

- Type of Organization: **Financial Services**
- Entity Name: **Paysafe Group Holdings Limited**
- Street Address: **2600 Michelson Drive, 1600**
- City: **Irvine**
- State, or Country if outside the US: **CALIFORNIA**
- Zip Code: **92612**

Submitted By

- Name: **W. James Denvil**
- Title: **Counsel**
- Firm name (if different than entity): **Hogan Lovells US LLP**
- Telephone Number: **2026375521**
- Email Address: **w.james.denvil@hoganlovells.com**
- Relationship to entity whose information was compromised: **Legal Counsel**

Breach Information

- Total number of persons affected (including residents): **91706**
- Total number of Maine residents affected: **485**
- If the number of Maine residents exceeds 1,000, have the consumer reporting agencies been notified:
- Date(s) Breach Occured: **5/13/2018 to 11/24/2020**
- Date Breach Discovered: **12/3/2020**
- Description of the Breach:
 - **External system breach (hacking)**
- Information Acquired - Name or other personal identifier in combination with: **Social Security Number**

Notification and Protection Services

- Type of Notification: **Written**
- Date(s) of consumer notification: **12/18/2020**
- Copy of notice to affected Maine residents: **[Template Individual Notification.pdf](#)[Maine Incident Report.pdf](#)**
- Date of any previous (within 12 months) breach notifications:
- Were identity theft protection services offered: **Yes**

- If yes, please provide the duration, the provider of the service and a brief description of the service: **Paysafe Group Holding Limited is offering credit monitoring and identity protection services for 2 years through Kroll to affected individuals, at no cost to them.**

Credits

Copyright © 2014
All rights reserved.

Exhibit 3



Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

December 16, 2020

By Certified Mail

Office of the Maine Attorney General
109 Sewall St
Augusta, ME 04330

Re: Security Incident Notification

To Whom It May Concern:

I am writing on behalf of Paysafe Group Holdings Limited (“Company” or “Paysafe”) to inform you of an incident that may have impacted personal information of 485 Maine residents who established merchant accounts with the Company. Paysafe is an online payments company headquartered at 25 Canada Square, 27th Floor, London, United Kingdom E14 5LQ. The Company offers or has offered services branded as CHI Payments, iPayment, and Paysafe.

On November 6, 2020, the Company discovered a potential compromise of a website used by part of its U.S. business. The Company promptly initiated an investigation to determine the nature and potential impact of the vulnerability. In the course of doing so, the Company identified suspicious activity indicating that an unauthorized actor submitted automated queries to the website. The Company created a secure environment to test the queries, using available logs and other information to assess potential impact. On November 19, 2020, the Company determined that a subset of the queries identified might have involved data held on the website. The Company analyzed logs and other information available to assess whether those queries could have returned information to unauthorized actors, and engaged external forensics experts to assist. By December 3, 2020, the Company determined that some queries may have compromised certain information held on the website, although the evidence is not conclusive. At this time, the Company has identified evidence of suspicious activity on the website between May 13, 2018, and November 24, 2020. The Company has notified law enforcement.

The information that may have been accessed includes names, contact details, Social Security numbers, and bank account information. The website did not hold customer transaction data, consumer data, or payment card information. The website impacted is separate from Paysafe’s core processing and operating systems. After discovering the incident, the Company took steps to prevent further unauthorized access and has closed the website. Although the Company is not aware of any evidence confirming that the activity resulted in unauthorized actors acquiring or misusing personal information, the Company is notifying affected individuals out of an abundance of caution so that they can take steps to protect themselves. The Company continues to invest in cybersecurity and is enhancing its website scanning practices and vulnerability detection program.

On December 18, 2020, the Company will send notice by postal mail to the potentially impacted Maine residents. We enclose a sample notice in this notification. In addition to providing information regarding credit reporting agencies, security freezes, fraud alerts, and other identity theft prevention tools, the Company is offering credit monitoring and

Office of the Attorney General

- 2 -

December 16, 2020

identity protection services for 2 years through Kroll to affected individuals, at no cost to them. The field for the phone number in the sample notice will be populated with the call center number: (833) 971-3287.

Please feel free to contact me if you have any questions or require additional information.

Sincerely,

A handwritten signature in black ink, appearing to read "W. Denvil", written over a light gray rectangular background.

James Denvil

Senior Associate
w.james.denvil@hoganlovells.com
D 1 202-637-5521

Enclosure

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a cybersecurity incident that may have affected personal information related to you. You provided the information to Merchant Services* in the course of enrolling for a merchant account.

WHAT HAPPENED

On November 6, 2020, through Merchant Services'* internal cybersecurity program, we discovered a potential compromise of a website used by part of our U.S. business. We promptly initiated an investigation to determine the nature and potential impact of the vulnerability. In the course of doing so, we identified suspicious activity indicating that an unauthorized actor submitted automated queries to the website. We created a secure environment to test the queries, using available logs and other information to assess potential impact. By November 19, 2020, we determined that a subset of the queries identified might have involved data held on the website. We analyzed logs and other information available to assess whether those queries could have returned information to unauthorized actors, and we engaged external forensics experts to assist. By December 3, 2020, we determined that some queries may have compromised certain information held on the website, although the evidence is not conclusive. At this time, we have identified evidence of suspicious activity on the website between May 13, 2018, and November 24, 2020. We have notified law enforcement. Although we are not aware of any evidence confirming that the activity resulted in unauthorized actors acquiring or misusing your personal information, we are providing this notice out of an abundance of caution so that you can take steps to protect yourself.

WHAT INFORMATION WAS INVOLVED

The information about you that may have been accessed includes your name, contact details, Social Security number, and bank account information. The website did not hold customer transaction data, consumer data, or payment card information. The website impacted is separate from Merchant Services'* core processing and operating systems. The website was part of a legacy system used internally and by a small group of former Chi Payment agents, a group acquired in an acquisition of iPayment in 2018, and contains certain data of a limited subset of merchants and agents.

WHAT WE ARE DOING

We take the privacy and security of your personal information seriously. After discovering the incident, we took steps to prevent further unauthorized access and have closed the website. We continue to invest in cybersecurity, including enhancing our website scanning practices and vulnerability detection program. Additionally, we have arranged for you to obtain credit monitoring and identity monitoring services at no cost to you for two years through Kroll, a leading provider of credit monitoring and identity monitoring services. Information regarding the package of services is included in Attachment 2 to this letter.

WHAT YOU CAN DO

We are not aware of any evidence indicating that your personal information has been misused or sold. Out of an abundance of caution, we recommend that you remain vigilant and review your financial records and statements for signs of suspicious activity. Please find additional information in Attachment 1 to this letter. As noted above, you can activate, at no cost to you, in the Kroll credit monitoring and identity monitoring services. Information about activation is contained in Attachment 2 to this letter.

* Merchant Services includes, for purposes of this notification, CHI Payments, iPayment, and Paysafe.

FOR MORE INFORMATION

If you have any questions or need additional information, please call [1-800-828-8282](tel:1-800-828-8282), Monday through Friday from 8:00 am to 5:30 pm Central Time, excluding major U.S. holidays. Be prepared to provide your membership number: <<Member ID>>.

We apologize for any inconvenience this may cause.

Sincerely,

Merchant Services

Enclosures

Attachment 1: Additional Information

You should be cautious about using email to provide sensitive personal information, whether sending it yourself or in response to email requests. You should also be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software on your devices or to trick you into sharing valuable personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at <https://www.consumer.ftc.gov/articles/0003-phishing>.

You should review your financial statements and accounts for signs of suspicious transactions and activities. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to local law enforcement, your State's Attorney General's office, or the FTC. If you are a resident of Rhode Island, you have the right to obtain a police report. You will find contact information for some of those entities below. If you discover unauthorized charges, promptly inform the relevant payment card companies and financial institutions.

Fraud Alert Information

Whether or not you enroll in the credit monitoring product offered, we recommend that you consider placing a free "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Fraud alerts last one year. Identity theft victims can get an extended fraud alert for seven years.

Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. You may also contact any of the consumer reporting agencies or the FTC for more information regarding fraud alerts. The contact information for the three nationwide credit reporting companies is:

Equifax	TransUnion	Experian
PO Box 740256	PO Box 2000	PO Box 9554
Atlanta, GA 30374	Chester, PA 19016	Allen, TX 75013
www.alerts.equifax.com	www.transunion.com/fraud	www.experian.com/fraud
1-800-525-6285	1-800-680-7289	1-888-397-3742

Free Credit Report Information

You have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score. Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud and identity theft. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency or state attorney general and file a police report. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also should file a complaint with the FTC using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcement for their investigations.

You may also contact the FTC at the contact information below to learn more about identity theft and the steps you can take to protect yourself. If you are a resident of the District of Columbia, Maryland, North Carolina, Iowa, Oregon, or Rhode Island, you can also reach out to your respective state's Attorney General's office at the contact information below. All other residents can find information on how to contact your state attorney general at www.naag.org/naag/attorneys-general/whos-my-ag.php.

Federal Trade Commission

Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.FTC.HELP (382.4357) / www.ftc.gov/idtheft

North Carolina Attorney General's Office

90001 Mail Service Center
Raleigh, NC 27699
1-919-716-6400 / <https://ncdoj.gov/>

Oregon Department of Justice

1162 Court Street NE
Salem, OR 97301
1-877-877-9392 / <https://justice.oregon.gov>

Office of the Attorney General for the District of Columbia

400 6th Street NW
Washington, D.C. 20001
1-202-727-3400 / oag.dc.gov

Maryland Attorney General's Office

200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023 / www.marylandattorneygeneral.gov

Rhode Island Attorney General's Office

150 South Main Street
Providence, Rhode Island 02903
1-401-274-4400 / <http://www.riag.ri.gov>

Consumer Protection Division

Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319
1-515-281-5926 / www.iowaattorneygeneral.gov

Security Freeze Information

You have the right to request a free Security Freeze (aka "Credit Freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a Credit Freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A Credit Freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. You may also contact any of the consumer reporting agencies or the FTC for more information regarding security freezes.

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
1-800-349-9960

TransUnion Security Freeze
PO Box 2000
Chester, PA 19016
www.transunion.com/freeze
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742

To request a Credit Freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

Attachment 2: Credit Monitoring and Identity Theft Services Enrollment Information



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

Visit <https://enroll.idheadquarters.com>* to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

* Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.