

1 Cristina Perez Hesano (#027023)
2 *cperez@perezlawgroup.com*
3 **PEREZ LAW GROUP, PLLC**
4 7508 N. 59th Avenue
5 Glendale, AZ 85301
6 Telephone: 602.730.7100
7 Fax: 623.235.6173

8 John J. Nelson, *Pro Hac Vice Application Forthcoming*
9 **MILBERG COLEMAN BRYSON**
10 **PHILLIPS GROSSMAN, PLLC**
11 280 S. Beverly Drive
12 Beverly Hills, CA 90212
13 Telephone: (858) 209-6941
14 Email: jnelson@milberg.com

15 *Attorneys for Plaintiff and*
16 *The Proposed Class*

17 **IN THE UNITED STATES DISTRICT COURT**
18 **FOR THE DISTRICT OF ARIZONA**

19 Barbara Squier, on behalf of herself and all
20 others similarly situated,

21 Plaintiff,

22 v.

23 On Q Financial, LLC,

24 Defendant.

25 Case No.

26 **CLASS ACTION**

27 **DEMAND FOR A JURY TRIAL**

28 Plaintiff Barbara Squier ("Plaintiff") brings this Class Action Complaint ("Complaint")
29 against On Q Financial, LLC ("Q Financial" or "Defendant") as an individual and on behalf of
30



1 all others similarly situated, and alleges, upon personal knowledge as to her own actions and
2 her counsels' investigation, and upon information and belief as to all other matters, as follows:

3 **SUMMARY OF ACTION**

4 1. Plaintiff brings this class action against Defendant for its failure to properly
5 secure and safeguard sensitive information of its customers.
6

7 2. Defendant is an Arizona-based mortgage company.

8 3. Plaintiff's and Class Members' sensitive personal information—which they
9 entrusted to Defendant on the mutual understanding that Defendant would protect it against
10 disclosure—was targeted, compromised and unlawfully accessed due to the Data Breach.
11

12 4. Q Financial collected and maintained certain personally identifiable information
13 and protected health information of Plaintiff and the putative Class Members (defined below),
14 who are (or were) customers at Defendant.
15

16 5. The PII compromised in the Data Breach included Plaintiff's and Class Members'
17 full names and Social Security numbers (“personally identifiable information” or “PII”).
18

19 6. The PII compromised in the Data Breach was exfiltrated by cyber-criminals and
20 remains in the hands of those cyber-criminals who target PII for its value to identity thieves.
21

22 7. As a result of the Data Breach, Plaintiff and approximately 211,000 Class
23 Members,¹ suffered concrete injuries in fact including, but not limited to: (i) invasion of
24 privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity
25 costs associated with attempting to mitigate the actual consequences of the Data Breach; (v)
26

27 ¹ <https://apps.web.maine.gov/online/aeviewer/ME/40/bfabbd9-6593-4e0f-a9b5-bf21a94b2329.shtml>



1 lost opportunity costs associated with attempting to mitigate the actual consequences of the
2 Data Breach; (vi) actual misuse of the compromised data consisting of an increase in spam
3 calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the
4 continued and certainly increased risk to their PII, which: (a) remains unencrypted and available
5 for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's
6 possession and is subject to further unauthorized disclosures so long as Defendant fails to
7 undertake appropriate and adequate measures to protect the PII.

8
9 8. The Data Breach was a direct result of Defendant's failure to implement adequate
10 and reasonable cyber-security procedures and protocols necessary to protect consumers' PII
11 from a foreseeable and preventable cyber-attack.

12
13 9. Moreover, upon information and belief, Defendant was targeted for a cyber-
14 attack due to its status as a mortgage company that collects and maintains highly confidential
15 and valuable PII on its systems.

16
17 10. Defendant maintained, used, and shared the PII in a reckless manner. In
18 particular, the PII was used and transmitted by Defendant in a condition vulnerable to
19 cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for
20 improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and
21 thus, Defendant was on notice that failing to take steps necessary to secure the PII from those
22 risks left that property in a dangerous condition.

23
24 11. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*,
25 intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable
26 measures to ensure its data systems were protected against unauthorized intrusions; failing to
27

1 take standard and reasonably available steps to prevent the Data Breach; and failing to provide
2 Plaintiff and Class Members prompt and accurate notice of the Data Breach.

3 12. Plaintiff's and Class Members' identities are now at risk because of Defendant's
4 negligent conduct because the PII that Defendant collected and maintained has been accessed
5 and acquired by data thieves.
6

7 13. Armed with the PII accessed in the Data Breach, data thieves have already
8 engaged in identity theft and fraud and can in the future commit a variety of crimes including,
9 *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class
10 Members' names, using Class Members' information to obtain government benefits, filing
11 fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class
12 Members' names but with another person's photograph, and giving false information to police
13 during an arrest.
14

15 14. As a result of the Data Breach, Plaintiff and Class Members have been exposed
16 to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must
17 now and in the future closely monitor their financial accounts to guard against identity theft.
18

19 15. Plaintiff and Class Members may also incur out of pocket costs, *e.g.*, for
20 purchasing credit monitoring services, credit freezes, credit reports, or other protective
21 measures to deter and detect identity theft.
22

23 16. Plaintiff brings this class action lawsuit on behalf all those similarly situated to
24 address Defendant's inadequate safeguarding of Class Members' PII that it collected and
25 maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class
26 Members that their information had been subject to the unauthorized access by an unknown
27



1 third party and precisely what specific type of information was accessed.

2 17. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of
3 herself and all similarly situated individuals whose PII was accessed during the Data Breach.

4 18. Plaintiff and Class Members have a continuing interest in ensuring that their
5 information is and remains safe, and they should be entitled to injunctive and other equitable
6 relief.
7

8 JURISDICTION AND VENUE

9 19. This Court has subject matter jurisdiction over this action under 28 U.S.C. §
10 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or
11 value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the
12 proposed class, and at least one member of the class, including Plaintiff, is a citizen of a state
13 different from Defendant.
14

15 20. This Court has personal jurisdiction over Defendant because its principal place
16 of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred
17 in and emanated from this District.
18

19 21. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place
20 of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred
21 in and emanated from this District.
22

23 PARTIES

24 22. Plaintiff Barbara Squier is a resident and citizen of Apopka, Florida.

25 23. Defendant On Q Financial, LLC is a limited liability organized under the state
26 laws of Arizona with its principal place of business located in Scottsdale, Arizona.
27

FACTUAL ALLEGATIONS

Defendant's Business

24. Defendant is an Arizona-based mortgage company.

25. Class Members are current and former customers of Defendant or individuals for whom Defendant provided mortgage or lending services.

26. In the course of their relationship, customers, including Class Members, directly or indirectly provided Defendant with at least the following: names, Social Security numbers, and other sensitive information.

27. Upon information and belief, in the course of collecting PII from customers, including Plaintiff, Defendant promised to provide confidentiality and adequate security for the data it collected from customers through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

28. Indeed, Defendant provides on its website that:

We have implemented measures designed to secure your personal information from accidental loss and from unauthorized access, use, alteration, and disclosure. All information you provide to us is stored using commercially reasonable security measures. Any payment transactions will be encrypted using commercially reasonable means.²

29. Plaintiff and Class Members relied on these promises and on this sophisticated business entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Consumers, in general, demand security to safeguard their PII, especially when

² <https://onqfinancial.com/privacy-policies/>



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

1 their Social Security numbers and other sensitive PII is involved.

2 ***The Data Breach***

3 30. On or about March 29, 2024, Defendant began sending Plaintiff and other Data
4 Breach victims a Notice of Data Security Incident letter (the "Notice Letter"), informing them
5 that:
6

7 **What Happened?** On February 20, 2024, On Q Financial received a notification
8 from ConnectWise, a software and IT management provider, regarding a
9 vulnerability involving its product, ScreenConnect, which is a software program On
10 Q Financial used for remote access to computers in our network. In response to the
11 notification received from ConnectWise, we immediately patched and upgraded the
12 application and began an investigation. The investigation revealed some suspicious
13 activity through the Screen Connect application. On Q Financial engaged a
14 computer forensics investigation firm to conduct an independent investigation into
15 what happened and determine whether personal information may have been
16 accessed or acquired without authorization. Our investigation confirmed that the
17 ConnectWise vulnerability has been successfully patched and the On Q Financial
18 computer network is secure. However, on March 14, 2023, the investigation
19 determined that the ConnectWise vulnerability permitted an unknown individual to
20 gain access to our computer network and the personal information of some of our
21 clients was exfiltrated from our network. Please note that at this time we are not
22 aware of any evidence that any of our clients' personal information has been
23 misused, and out of an abundance of caution, we are notifying all of our clients
24 whose personal information has potentially been impacted.

19 **What Information was Involved?** The information that may have been affected in
20 connection with this incident includes your name and Social Security number.³

21 31. Omitted from the Notice Letter were the date(s) of the Data Breach, the identity
22 of the cybercriminals who perpetrated this Data Breach the details of the root cause of the Data
23 Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a
24

25
26 ³ The "Notice Letter". A sample copy is available at
27 [https://apps.web.maine.gov/online/aeviewer/ME/40/bfabbd9-6593-4e0f-a9b5-
bf21a94b2329.shtml](https://apps.web.maine.gov/online/aeviewer/ME/40/bfabbd9-6593-4e0f-a9b5-bf21a94b2329.shtml)

1 breach does not occur again. To date, these omitted details have not been explained or clarified
2 to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains
3 protected.

4 32. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with
5 any degree of specificity, Plaintiff and Class Members of the Data Breach’s critical facts.
6 Without these details, Plaintiff’s and Class Members’ ability to mitigate the harms resulting
7 from the Data Breach is severely diminished.
8

9 33. Despite Defendant’s intentional opacity about the root cause of this incident,
10 several facts may be gleaned from the Notice Letter, including: a) that this Data Breach was the
11 work of cybercriminals; b) that the cybercriminals first infiltrated Defendant’s networks and
12 systems, and downloaded data from the networks and systems (aka exfiltrated data, or in
13 layperson’s terms “stole” data; and c) that once inside Defendant’s networks and systems, the
14 cybercriminals targeted information including Plaintiff’s and Class Members’ Social Security
15 numbers for download and theft.
16

17 34. Companies only send notice letters because data breach notification laws require
18 them to do so. And such letters are only sent to those persons who Defendant itself has has a
19 reasonable belief that such personal information was accessed or acquired by an unauthorized
20 individual or entity. By sending a notice of data breach letter to Plaintiff and Class Members,
21 Defendant admits that it has a “reasonable belief that Plaintiff’s and Class Members’ names
22 and Social Security numbers were accessed or acquired by an “unknown actor” – aka
23 cybercriminals.
24
25

26 35. Moreover, in its Notice Letter, Defendant failed to specify whether it undertook
27

1 any efforts to contact the approximate 211,000 Class Members whose data was accessed and
2 acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of
3 their data or whether Defendant was interested in hearing about misuse of their data or set up a
4 mechanism for Class Members to report misuse of their data.

5
6 36. Defendant had obligations created by the FTC Act, GLBA, contract, common
7 law, and industry standards to keep Plaintiff's and Class Members' PII confidential and to
8 protect it from unauthorized access and disclosure.

9
10 37. Defendant did not use reasonable security procedures and practices appropriate
11 to the nature of the sensitive information they were maintaining for Plaintiff and Class
12 Members, causing the exposure of PII, such as encrypting the information or deleting it when
13 it is no longer needed.

14
15 38. The attacker accessed and acquired files Defendant shared with a third party
16 containing unencrypted PII of Plaintiff and Class Members. Plaintiff's and Class Members' PII
17 was accessed and stolen in the Data Breach.

18
19 39. Plaintiff further believes that her PII and that of Class Members was subsequently
20 sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals
21 that commit cyber-attacks of this type.

22 ***Data Breaches Are Preventable***

23
24 40. Defendant did not use reasonable security procedures and practices appropriate
25 to the nature of the sensitive information they were maintaining for Plaintiff and Class
26 Members, causing the exposure of PII, such as encrypting the information or deleting it when
27 it is no longer needed.

1 41. Defendant could have prevented this Data Breach by, among other things,
2 properly encrypting or otherwise protecting their equipment and computer files containing PII.

3 42. As explained by the Federal Bureau of Investigation, “[p]revention is the most
4 effective defense against ransomware and it is critical to take precautions for protection.”⁴
5

6 43. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could
7 and should have implemented, as recommended by the United States Government, the
8 following measures:

- 9 • Implement an awareness and training program. Because end users are targets,
10 employees and individuals should be aware of the threat of ransomware and how it
11 is delivered.
- 12 • Enable strong spam filters to prevent phishing emails from reaching the end users
13 and authenticate inbound email using technologies like Sender Policy Framework
14 (SPF), Domain Message Authentication Reporting and Conformance (DMARC),
15 and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- 16 • Scan all incoming and outgoing emails to detect threats and filter executable files
17 from reaching end users.
- 18 • Configure firewalls to block access to known malicious IP addresses.
- 19 • Patch operating systems, software, and firmware on devices. Consider using a
20 centralized patch management system.
- 21 • Set anti-virus and anti-malware programs to conduct regular scans automatically.
- 22 • Manage the use of privileged accounts based on the principle of least privilege: no
23 users should be assigned administrative access unless absolutely needed; and those
24 with a need for administrator accounts should only use them when necessary.
- 25 • Configure access controls—including file, directory, and network share
26 permissions—with least privilege in mind. If a user only needs to read specific files,
27 the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office
Viewer software to open Microsoft Office files transmitted via email instead of full
office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs

⁴ How to Protect Your Networks from RANSOMWARE, at 3, *available at*:
<https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>



1 from executing from common ransomware locations, such as temporary folders
2 supporting popular Internet browsers or compression/decompression programs,
3 including the AppData/LocalAppData folder.

- 4 • Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- 5 • Use application whitelisting, which only allows systems to execute programs known
6 and permitted by security policy.
- 7 • Execute operating system environments or specific programs in a virtualized
8 environment.
- 9 • Categorize data based on organizational value and implement physical and logical
10 separation of networks and data for different organizational units.⁵

11 44. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and
12 should have implemented, as recommended by the Microsoft Threat Protection Intelligence
13 Team, the following measures:

14 **Secure internet-facing assets**

- 15 - Apply latest security updates
- 16 - Use threat and vulnerability management
- 17 - Perform regular audit; remove privileged credentials;

18 **Thoroughly investigate and remediate alerts**

- 19 - Prioritize and treat commodity malware infections as potential
20 full compromise;

21 **Include IT Pros in security discussions**

- 22 - Ensure collaboration among [security operations], [security
23 admins], and [information technology] admins to configure
24 servers and other endpoints securely;

25 **Build credential hygiene**

- 26 - Use [multifactor authentication] or [network level authentication]
27 and use strong, randomized, just-in-time local admin passwords;

⁵ *Id.* at 3-4.

1 **Apply principle of least-privilege**

- 2 -Monitor for adversarial activities
3 -Hunt for brute force attempts
4 -Monitor for cleanup of Event Logs
5 -Analyze logon events;

6 **Harden infrastructure**

- 7 -Use Windows Defender Firewall
8 -Enable tamper protection
9 -Enable cloud-delivered protection
10 - Turn on attack surface reduction rules and [Antimalware Scan
11 Interface] for Office [Visual Basic for Applications].⁶

12 45. Given that Defendant was storing the PII of its current and former customers,
13 Defendant could and should have implemented all of the above measures to prevent and detect
14 cyberattacks.

15 46. The occurrence of the Data Breach indicates that Defendant failed to adequately
16 implement one or more of the above measures to prevent cyberattacks, resulting in the Data
17 Breach and data thieves acquiring and accessing the PII of more than two hundred thousand
18 individuals, including that of Plaintiff and Class Members.

19 ***Defendant Acquires, Collects, And Stores Its Customers' PII***

20 47. Defendant acquires, collects, and stores a massive amount of PII on its current
21 and former customers.

22 48. As a condition of obtaining mortgage products and/or services at Defendant,
23 Defendant requires that customers and other personnel entrust it with highly sensitive personal
24

25 _____
26 ⁶ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*:
27 <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>



1 information.

2 49. By obtaining, collecting, and using Plaintiff's and Class Members' PII, Defendant
3 assumed legal and equitable duties and knew or should have known that it was responsible for
4 protecting Plaintiff's and Class Members' PII from disclosure.

5
6 50. Plaintiff and the Class Members have taken reasonable steps to maintain the
7 confidentiality of their PII and would not have entrusted it to Defendant absent a promise to
8 safeguard that information.

9
10 51. Upon information and belief, in the course of collecting PII from customers,
11 including Plaintiff, Defendant promised to provide confidentiality and adequate security for
12 their data through its applicable privacy policy and through other disclosures in compliance
13 with statutory privacy requirements.

14 52. Indeed, Defendant provides on its website that:

15
16 We have implemented measures designed to secure your personal information from
17 accidental loss and from unauthorized access, use, alteration, and disclosure. All
18 information you provide to us is stored using commercially reasonable security
19 measures. Any payment transactions will be encrypted using commercially reasonable
20 means.⁷

21 53. Plaintiff and the Class Members relied on Defendant to keep their PII confidential
22 and securely maintained, to use this information for business purposes only, and to make only
23 authorized disclosures of this information.

24 ***Defendant Knew, Or Should Have Known, Of The Risk Because Mortgage
25 Companies In Possession Of PII Are Particularly Susceptible To Cyber Attacks***

26
27 ⁷ <https://onqfinancial.com/privacy-policies/>

1 54. Defendant’s data security obligations were particularly important given the
2 substantial increase in cyber-attacks and/or data breaches targeting mortgage companies that
3 collect and store PII, like Defendant, preceding the date of the breach.

4 55. Data breaches, including those perpetrated against mortgage companies that store
5 PII in their systems, have become widespread.
6

7 56. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced
8 data breaches, resulting in 66,658,764 individuals’ personal information being compromised.⁸
9

10 57. In light of recent high profile data breaches at other industry leading companies,
11 including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20
12 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023),
13 NCB Management Services, Inc. (1 million records, February 2023), Defendant knew or should
14 have known that the PII that it collected and maintained would be targeted by cybercriminals.
15

16 58. Indeed, cyber-attacks, such as the one experienced by Defendant, have become
17 so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have
18 issued a warning to potential targets so they are aware of, and prepared for, a potential attack.
19 As one report explained, smaller entities that store PII are “attractive to ransomware
20 criminals...because they often have lesser IT defenses and a high incentive to regain access to
21 their data quickly.”⁹
22

23
24 _____
25 ⁸ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>

26 ⁹ https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection
27

1 59. Additionally, as companies become more dependent on computer systems to run
2 their business,¹⁰ e.g., working remotely as a result of the Covid-19 pandemic, and the Internet
3 of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the
4 need for adequate administrative, physical, and technical safeguards.¹¹

5
6 60. Defendant knew and understood unprotected or exposed PII in the custody of
7 insurance companies, like Defendant, is valuable and highly sought after by nefarious third
8 parties seeking to illegally monetize that PII through unauthorized access.

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

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

19
20 63. The injuries to Plaintiff and Class Members were directly and proximately caused
21 by Defendant’s failure to implement or maintain adequate data security measures for the PII of
22 Plaintiff and Class Members.

23
24 64. The ramifications of Defendant’s failure to keep secure the PII of Plaintiff and

25 _____
26 ¹⁰<https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

27 ¹¹ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

1 Class Members are long lasting and severe. Once PII is stolen—particularly Social Security
2 numbers and —fraudulent use of that information and damage to victims may continue for
3 years.

4 65. In the Notice Letter, Defendant makes an offer of 12 months of identity
5 monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as
6 it fails to provide for the fact victims of data breaches and other unauthorized disclosures
7 commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to
8 provide sufficient compensation for the unauthorized release and disclosure of Plaintiff’s and
9 Class Members’ PII.
10

11 66. Defendant's offer of credit and identity monitoring establishes that Plaintiff’s and
12 Class Members’ sensitive PII was in fact affected, accessed, compromised, and exfiltrated from
13 Defendant's computer systems.
14

15 67. As a mortgage company in custody of the PII of its customers, Defendant knew,
16 or should have known, the importance of safeguarding PII entrusted to it by Plaintiff and Class
17 Members, and of the foreseeable consequences if its data security systems were breached. This
18 includes the significant costs imposed on Plaintiff and Class Members as a result of a breach.
19 Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.
20

21 ***Value Of Personally Identifying Information***

22 68. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud
23 committed or attempted using the identifying information of another person without
24
25
26
27

P
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 authority.”¹² The FTC describes “identifying information” as “any name or number that may
 2 be used, alone or in conjunction with any other information, to identify a specific person,”
 3 including, among other things, “[n]ame, Social Security number, date of birth, official State or
 4 government issued driver’s license or identification number, alien registration number,
 5 government passport number, employer or taxpayer identification number.”¹³
 6

7 69. The PII of individuals remains of high value to criminals, as evidenced by the
 8 prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen
 9 identity credentials.¹⁴
 10

11 70. For example, PII can be sold at a price ranging from \$40 to \$200.¹⁵ Criminals can
 12 also purchase access to entire company data breaches from \$900 to \$4,500.¹⁶
 13

14 71. Moreover, Social Security numbers are among the worst kind of PII to have stolen
 15 because they may be put to a variety of fraudulent uses and are difficult for an individual to
 16 change.
 17

18 72. According to the Social Security Administration, each time an individual’s Social
 19 Security number is compromised, “the potential for a thief to illegitimately gain access to bank
 20 accounts, credit cards, driving records, tax and employment histories and other private
 21

22 ¹² 17 C.F.R. § 248.201 (2013).

23 ¹³ *Id.*

24 ¹⁴ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

25 ¹⁵ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

26 ¹⁶ *In the Dark*, VPNOverview, 2019, available at:
 27 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>

1 information increases.”¹⁷ Moreover, “[b]ecause many organizations still use SSNs as the
2 primary identifier, exposure to identity theft and fraud remains.”¹⁸

3 73. The Social Security Administration stresses that the loss of an individual’s Social
4 Security number, as experienced by Plaintiff and some Class Members, can lead to identity
5 theft and extensive financial fraud:
6

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

15 74. In fact, “[a] stolen Social Security number is one of the leading causes of identity
16 theft and can threaten your financial health.”²⁰ “Someone who has your SSN can use it to
17 impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds,
18 get medical treatment, and steal your government benefits.”²¹

19 75. What’s more, it is no easy task to change or cancel a stolen Social Security
20 number. An individual cannot obtain a new Social Security number without significant
21

22 ¹⁷ See
23 <https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.>

24 ¹⁸ *Id.*

25 ¹⁹ Social Security Administration, *Identity Theft and Your Social Security Number*, available
26 at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>

27 ²⁰ See <https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/>

²¹ See <https://www.investopedia.com/terms/s/ssn.asp>

1 paperwork and evidence of actual misuse. In other words, preventive action to defend against
 2 the possibility of misuse of a Social Security number is not permitted; an individual must show
 3 evidence of actual, ongoing fraud activity to obtain a new number.

4 76. Even then, a new Social Security number may not be effective. According to Julie
 5 Ferguson of the Identity Theft Resource Center, “[t]he credit bureaus and banks are able to link
 6 the new number very quickly to the old number, so all of that old bad information is quickly
 7 inherited into the new Social Security number.”²²

8 77. For these reasons, some courts have referred to Social Security numbers as the
 9 “gold standard” for identity theft. *Portier v. NEO Tech. Sols.*, No. 3:17-CV-30111, 2019 WL
 10 7946103, at *12 (D. Mass. Dec. 31, 2019) (“Because Social Security numbers are the gold
 11 standard for identity theft, their theft is significant Access to Social Security numbers
 12 causes long-lasting jeopardy because the Social Security Administration does not normally
 13 replace Social Security numbers.”), report and recommendation adopted, No. 3:17-CV-30111,
 14 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc.*, 2021 WL
 15 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiffs’ Social
 16 Security numbers are: arguably “the most dangerous type of personal information in the hands
 17 of identity thieves” because it is immutable and can be used to “impersonat[e] [the victim] to
 18 get medical services, government benefits, ... tax refunds, [and] employment.” . . . Unlike a
 19 credit card number, which can be changed to eliminate the risk of harm following a data breach,
 20
 21
 22
 23
 24

25 _____
 26 ²² Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR
 27 (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>

1 “[a] social security number derives its value in that it is immutable,” and when it is stolen it can
2 “forever be wielded to identify [the victim] and target her in fraudulent schemes and identity
3 theft attacks.”)

4 78. Similarly, the California state government warns consumers that: “[o]riginally,
5 your Social Security number (SSN) was a way for the government to track your earnings and
6 pay you retirement benefits. But over the years, it has become much more than that. It is the
7 key to a lot of your personal information. With your name and SSN, an identity thief could open
8 new credit and bank accounts, rent an apartment, or even get a job.”²³

9
10
11 79. Based on the foregoing, the information compromised in the Data Breach is
12 significantly more valuable than the loss of, for example, credit card information in a retailer
13 data breach because, there, victims can cancel or close credit and debit card accounts. The
14 information compromised in this Data Breach is impossible to “close” and difficult, if not
15 impossible, to change—Social Security numbers and names.

16
17 80. This data demands a much higher price on the black market. Martin Walter, senior
18 director at cybersecurity firm RedSeal, explained, “Compared to credit card information,
19 personally identifiable information and Social Security numbers are worth more than 10x on
20 the black market.”²⁴

21
22 81. Among other forms of fraud, identity thieves may obtain driver’s licenses,
23

24
25 ²³ See <https://oag.ca.gov/idtheft/facts/your-ssn>

26 ²⁴ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*
27 *Numbers*, IT World, (Feb. 6, 2015), available at:
<https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

1 government benefits, medical services, and housing or even give false information to police.

2 82. The fraudulent activity resulting from the Data Breach may not come to light for
3 years. There may be a time lag between when harm occurs versus when it is discovered, and
4 also between when PII is stolen and when it is used. According to the U.S. Government
5 Accountability Office (“GAO”), which conducted a study regarding data breaches:
6

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

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

16 ***Defendant Fails To Comply With FTC Guidelines***

17 84. The Federal Trade Commission (“FTC”) has promulgated numerous guides for
18 businesses which highlight the importance of implementing reasonable data security practices.
19 According to the FTC, the need for data security should be factored into all business decision-
20 making.
21

22 85. In 2016, the FTC updated its publication, Protecting Personal Information: A
23 Guide for Business, which established cyber-security guidelines for businesses. These
24 guidelines note that businesses should protect the personal consumer information that they
25

26 _____
27 ²⁵ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:
<https://www.gao.gov/assets/gao-07-737.pdf>

1 keep; properly dispose of personal information that is no longer needed; encrypt information
2 stored on computer networks; understand their network’s vulnerabilities; and implement
3 policies to correct any security problems.²⁶

4 86. The guidelines also recommend that businesses use an intrusion detection system
5 to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating
6 someone is attempting to hack the system; watch for large amounts of data being transmitted
7 from the system; and have a response plan ready in the event of a breach.²⁷

8 87. The FTC further recommends that companies not maintain PII longer than is
9 needed for authorization of a transaction; limit access to sensitive data; require complex
10 passwords to be used on networks; use industry-tested methods for security; monitor for
11 suspicious activity on the network; and verify that third-party service providers have
12 implemented reasonable security measures.

13 88. The FTC has brought enforcement actions against businesses for failing to
14 adequately and reasonably protect consumer data, treating the failure to employ reasonable and
15 appropriate measures to protect against unauthorized access to confidential consumer data as
16 an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act
17 (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures
18 businesses must take to meet their data security obligations.

19 89. These FTC enforcement actions include actions against mortgage companies, like
20
21
22

23
24
25 ²⁶ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).
26 Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

27 ²⁷ *Id.*

1 Defendant.

2 90. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or
3 affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or
4 practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII.
5 The FTC publications and orders described above also form part of the basis of Defendant's
6 duty in this regard.
7

8 91. Defendant failed to properly implement basic data security practices.

9 92. Defendant's failure to employ reasonable and appropriate measures to protect
10 against unauthorized access to the PII of its customers or to comply with applicable industry
11 standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C.
12 § 45.
13

14 93. Upon information and belief, Q Financial was at all times fully aware of its
15 obligation to protect the PII of its customers, Q Financial was also aware of the significant
16 repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was
17 particularly unreasonable given the nature and amount of PII it obtained and stored and the
18 foreseeable consequences of the immense damages that would result to Plaintiff and the Class.
19

20
21 ***Defendant Failed to Comply with the Gramm-Leach-Bliley Act***

22 94. Defendant is a financial institution, as that term is defined by Section 509(3)(A)
23 of the Gramm-Leach-Bliley Act (“GLBA”), 15 U.S.C. § 6809(3)(A), and thus is subject to the
24 GLBA.
25

26 95. The GLBA defines a financial institution as “any institution the business of which
27 is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding



1 Company Act of 1956].” 15 U.S.C. § 6809(3)(A).

2 96. Defendant collects nonpublic personal information, as defined by 15 U.S.C. §
3 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the
4 relevant time period Defendant was subject to the requirements of the GLBA, 15 U.S.C. §§
5 6801.1, *et seq.*, and is subject to numerous rules and regulations promulgated on the GLBA
6 statutes.
7

8 97. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part
9 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became
10 responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the
11 implementing regulations in an interim final rule that established the Privacy of Consumer
12 Financial Information, Regulation P, 12 C.F.R. § 1016 (“Regulation P”), with the final version
13 becoming effective on October 28, 2014.
14

15 98. Accordingly, Defendant’s conduct is governed by the Privacy Rule prior to
16 December 30, 2011, and by Regulation P after that date.
17

18 99. Both the Privacy Rule and Regulation P require financial institutions to provide
19 customers with an initial and annual privacy notice. These privacy notices must be “clear and
20 conspicuous.” 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. “Clear and
21 conspicuous means that a notice is reasonably understandable and designed to call attention to
22 the nature and significance of the information in the notice.” 16 C.F.R. § 313.3(b)(1); 12 C.F.R.
23 § 1016.3(b)(1). These privacy notices must “accurately reflect[] [the financial institution’s]
24 privacy policies and practices.” 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5.
25 They must include specified elements, including the categories of nonpublic personal
26
27



1 information the financial institution collects and discloses, the categories of third parties to
2 whom the financial institution discloses the information, and the financial institution's security
3 and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. §
4 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can
5 reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As
6 alleged herein, Defendant violated the Privacy Rule and Regulation P.
7

8 100. Upon information and belief, Defendant failed to provide annual privacy notices
9 to customers after the customer relationship ended, despite retaining these customers' PII and
10 storing that PII on Defendant's network systems.
11

12 101. Defendant failed to adequately inform their customers that they were storing
13 and/or sharing, or would store and/or share, the customers' PII on an insecure platform,
14 accessible to unauthorized parties from the internet, and would do so after the customer
15 relationship ended.
16

17 102. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C.
18 § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of
19 customer information by developing a comprehensive written information security program
20 that contains reasonable administrative, technical, and physical safeguards, including: (1)
21 designating one or more employees to coordinate the information security program; (2)
22 identifying reasonably foreseeable internal and external risks to the security, confidentiality,
23 and integrity of customer information, and assessing the sufficiency of any safeguards in place
24 to control those risks; (3) designing and implementing information safeguards to control the
25 risks identified through risk assessment, and regularly testing or otherwise monitoring the
26
27



1 effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service
2 providers and requiring them by contract to protect the security and confidentiality of customer
3 information; and (5) evaluating and adjusting the information security program in light of the
4 results of testing and monitoring, changes to the business operation, and other relevant
5 circumstances. 16 C.F.R. §§ 314.3 and 314.4.
6

7 103. As alleged herein, Defendant violated the Safeguard Rule.

8 104. Defendant failed to assess reasonably foreseeable risks to the security,
9 confidentiality, and integrity of customer information and failed to monitor the systems of its
10 IT partners or verify the integrity of those systems.
11

12 105. Defendant violated the GLBA and its own policies and procedures by sharing the
13 PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff
14 and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such
15 disclosure.
16

17 ***Defendant Fails To Comply With Industry Standards***

18 106. As noted above, experts studying cyber security routinely identify mortgage
19 companies in possession of PII as being particularly vulnerable to cyberattacks because of the
20 value of the PII which they collect and maintain.
21

22 107. Several best practices have been identified that, at a minimum, should be
23 implemented by mortgage companies in possession of PII, like Defendant, including but not
24 limited to: educating all employees; strong passwords; multi-layer security, including firewalls,
25 anti-virus, and anti-malware software; encryption, making data unreadable without a key;
26 multi-factor authentication; backup data and limiting which employees can access sensitive
27

1 data. Q Financial failed to follow these industry best practices, including a failure to implement
2 multi-factor authentication.

3 108. Other best cybersecurity practices that are standard for mortgage companies
4 include installing appropriate malware detection software; monitoring and limiting the network
5 ports; protecting web browsers and email management systems; setting up network systems
6 such as firewalls, switches and routers; monitoring and protection of physical security systems;
7 protection against any possible communication system; training staff regarding critical points.
8 Q Financial failed to follow these cybersecurity best practices, including failure to train staff.
9

10 109. Defendant failed to meet the minimum standards of any of the following
11 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation
12 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,
13 PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center
14 for Internet Security's Critical Security Controls (CIS CSC), which are all established standards
15 for Internet Security's Critical Security Controls (CIS CSC), which are all established standards
16 in reasonable cybersecurity readiness.
17

18 110. These foregoing frameworks are existing and applicable industry standards for
19 mortgage companies, and upon information and belief, Defendant failed to comply with at least
20 one—or all—of these accepted standards, thereby opening the door to the threat actor and
21 causing the Data Breach.
22

23 *Common Injuries & Damages*

24 111. As a result of Defendant's ineffective and inadequate data security practices, the
25 Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals,
26 the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent,
27

1 and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i)
2 invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and
3 opportunity costs associated with attempting to mitigate the actual consequences of the Data
4 Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting
5 to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal
6 damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains
7 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains
8 backed up in Defendant's possession and is subject to further unauthorized disclosures so long
9 as Defendant fails to undertake appropriate and adequate measures to protect the PII.
10
11

12 ***Data Breaches Increase Victims' Risk Of Identity Theft***

13 112. The unencrypted PII of Class Members will end up for sale on the dark web as
14 that is the *modus operandi* of hackers.
15

16 113. Unencrypted PII may also fall into the hands of companies that will use the
17 detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Simply
18 put, unauthorized individuals can easily access the PII of Plaintiff and Class Members.
19

20 114. The link between a data breach and the risk of identity theft is simple and well
21 established. Criminals acquire and steal PII to monetize the information. Criminals monetize
22 the data by selling the stolen information on the black market to other criminals who then utilize
23 the information to commit a variety of identity theft related crimes discussed below.
24

25 115. Plaintiff's and Class Members' PII is of great value to hackers and cyber
26 criminals, and the data stolen in the Data Breach has been used and will continue to be used in
27 a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off



PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 their misfortune.

2 116. Due to the risk of one’s Social Security number being exposed, state legislatures
3 have passed laws in recognition of the risk: “[t]he social security number can be used as a tool
4 to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and
5 familial information, the release of which could cause great financial or personal harm to an
6 individual. While the social security number was intended to be used solely for the
7 administration of the federal Social Security System, over time this unique numeric identifier
8 has been used extensively for identity verification purposes[.]”²⁸

9
10
11 117. Moreover, “SSNs have been central to the American identity infrastructure for
12 years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked
13 into their identification process for years. In fact, SSNs have been the gold standard for
14 identifying and verifying the credit history of prospective customers.”²⁹

15
16 118. “Despite the risk of fraud associated with the theft of Social Security numbers,
17 just five of the nation’s largest 25 banks have stopped using the numbers to verify a customer’s
18 identity after the initial account setup[.]”³⁰ Accordingly, since Social Security numbers are
19 frequently used to verify an individual’s identity after logging onto an account or attempting a
20 transaction, “[h]aving access to your Social Security number may be enough to help a thief steal
21
22
23

24 _____
25 ²⁸ See N.C. Gen. Stat. § 132-1.10(1).

26 ²⁹ See <https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers>

27 ³⁰ See <https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/>

1 money from your bank account”³¹

2 119. One such example of criminals piecing together bits and pieces of compromised
3 PII for profit is the development of “Fullz” packages.³²

4 120. With “Fullz” packages, cyber-criminals can cross-reference two sources of PII to
5 marry unregulated data available elsewhere to criminally stolen data with an astonishingly
6 complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

7 121. The development of “Fullz” packages means here that the stolen PII from the
8 Data Breach can easily be used to link and identify it to Plaintiff’s and Class Members’ phone
9 numbers, email addresses, and other unregulated sources and identifiers. In other words, even
10 if certain information such as emails, phone numbers, or credit card numbers may not be
11 included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a
12 Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as
13
14
15
16

17 ³¹ See <https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>

18 ³² “Fullz” is fraudster speak for data that includes the information of the victim, including, but
19 not limited to, the name, address, credit card information, social security number, date of birth,
20 and more. As a rule of thumb, the more information you have on a victim, the more money that
21 can be made off of those credentials. Fullz are usually pricier than standard credit card
22 credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed
23 out (turning credentials into money) in various ways, including performing bank transactions
24 over the phone with the required authentication details in-hand. Even “dead Fullz,” which are
25 Fullz credentials associated with credit cards that are no longer valid, can still be used for
26 numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim,
27 or opening a “mule account” (an account that will accept a fraudulent money transfer from a
compromised account) without the victim’s knowledge. See, e.g., Brian Krebs, *Medical
Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security
(Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/)

1 illegal and scam telemarketers) over and over.

2 122. The existence and prevalence of “Fullz” packages means that the PII stolen from
3 the data breach can easily be linked to the unregulated data (like insurance information) of
4 Plaintiff and the other Class Members.

5 123. Thus, even if certain information (such as insurance information) was not stolen
6 in the data breach, criminals can still easily create a comprehensive “Fullz” package.
7

8 124. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to
9 crooked operators and other criminals (like illegal and scam telemarketers).
10

11 ***Loss Of Time To Mitigate Risk Of Identity Theft & Fraud***

12 125. As a result of the recognized risk of identity theft, when a Data Breach occurs,
13 and an individual is notified by a company that their PII was compromised, as in this Data
14 Breach, the reasonable person is expected to take steps and spend time to address the dangerous
15 situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of
16 identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports
17 could expose the individual to greater financial harm – yet, the resource and asset of time has
18 been lost.
19

20 126. Thus, due to the actual and imminent risk of identity theft, Defendant, in its
21 Notice Letter instructs Plaintiff and Class Members to take the following measures to protect
22 themselves: “remain vigilant by reviewing your account statements and credit reports
23 closely.”³³
24

25
26 _____
27 ³³ Notice Letter.

1 127. In addition, Defendant’s Notice letter includes a full two pages devoted to “Steps
2 You Can Take To Protect Your Information” that recommend Plaintiff and Class Members to
3 partake in activities such as obtaining their credit reports, placing fraud alerts and security
4 freezes on their accounts, and contacting government agencies.³⁴
5

6 128. Defendant’s extensive suggestion of steps that Plaintiff and Class Members must
7 take in order to protect themselves from identity theft and/or fraud demonstrates the significant
8 time that Plaintiffs and Class Members must undertake in response to the Data Breach.
9 Plaintiff’s and Class Members’ time is highly valuable and irreplaceable, and accordingly,
10 Plaintiff and Class Members suffered actual injury and damages in the form of lost time that
11 they spent on mitigation activities in response to the Data Breach and at the direction of
12 Defendant’s Notice Letter.
13

14 129. Plaintiff and Class Members have spent, and will spend additional time in the
15 future, on a variety of prudent actions, such as researching and verifying the legitimacy of the
16 Data Breach and monitoring their financial accounts for any indication of fraudulent activity,
17 which may take years to detect. Accordingly, the Data Breach has caused Plaintiff and Class
18 Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent
19 on mitigation activities.
20
21

22 130. Plaintiff’s mitigation efforts are consistent with the U.S. Government
23 Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”)
24 in which it noted that victims of identity theft will face “substantial costs and time to repair the
25

26
27 ³⁴ *Id.*

1 damage to their good name and credit record.”³⁵

2 131. Plaintiff’s mitigation efforts are also consistent with the steps that FTC
3 recommends that data breach victims take several steps to protect their personal and financial
4 information after a data breach, including: contacting one of the credit bureaus to place a fraud
5 alert (consider an extended fraud alert that lasts for seven years if someone steals their identity),
6 reviewing their credit reports, contacting companies to remove fraudulent charges from their
7 accounts, placing a credit freeze on their credit, and correcting their credit reports.³⁶

8 132. And for those Class Members who experience actual identity theft and fraud, the
9 United States Government Accountability Office released a report in 2007 regarding data
10 breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial
11 costs and time to repair the damage to their good name and credit record.”^[4]

12
13
14 ***Diminution of Value of PII***

15 133. PII is a valuable property right.³⁷ The value is axiomatic, considering the value of
16 Big Data in corporate America and the consequences of cyber thefts include heavy prison
17 sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has
18 considerable market value.

19 134. Sensitive PII can sell for as much as \$363 per record according to the Infosec
20
21
22

23
24 ³⁵ See United States Government Accountability Office, GAO-07-737, Personal Information:
25 Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However,
26 the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

27 ³⁶ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

³⁷ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”).

1 Institute.³⁸

2 135. An active and robust legitimate marketplace for PII also exists. In 2019, the data
3 brokering industry was worth roughly \$200 billion.³⁹

4 136. In fact, the data marketplace is so sophisticated that consumers can actually sell
5 their non-public information directly to a data broker who in turn aggregates the information
6 and provides it to marketers or app developers.^{40,41}

7 137. Consumers who agree to provide their web browsing history to the Nielsen
8 Corporation can receive up to \$50.00 a year.⁴²

9 138. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an
10 inherent market value in both legitimate and dark markets, has been damaged and diminished
11 by its compromise and unauthorized release. However, this transfer of value occurred without
12 any consideration paid to Plaintiff or Class Members for their property, resulting in an economic
13 loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby
14 causing additional loss of value.

15 139. At all relevant times, Q Financial knew, or reasonably should have known, of the
16
17

18
19
20
21 ³⁸ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally
22 Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech.
23 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is
24 rapidly reaching a level comparable to the value of traditional financial assets.") (citations
25 omitted).

26 ³⁹ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015),
27 <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

⁴⁰ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

⁴¹ <https://datacoup.com/>

⁴² <https://digi.me/what-is-digime/>

1 importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable
2 consequences that would occur if Defendant's data security system was breached, including,
3 specifically, the significant costs that would be imposed on Plaintiff and Class Members as a
4 result of a breach.

5
6 140. The fraudulent activity resulting from the Data Breach may not come to light for
7 years.

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

11
12 142. Q Financial was, or should have been, fully aware of the unique type and the
13 significant volume of data on Defendant's network, amounting to more than two hundred
14 thousand individuals' detailed personal information and, thus, the significant number of
15 individuals who would be harmed by the exposure of the unencrypted data.

16
17 143. The injuries to Plaintiff and Class Members were directly and proximately caused
18 by Defendant's failure to implement or maintain adequate data security measures for the PII of
19 Plaintiff and Class Members.

20
21 ***Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary***

22 144. Given the type of targeted attack in this case, sophisticated criminal activity, and
23 the type of PII involved, there is a strong probability that entire batches of stolen information
24 have been placed, or will be placed, on the black market/dark web for sale and purchase by
25 criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in
26 the victims' names to make purchases or to launder money; file false tax returns; take out loans
27

1 or lines of credit; or file false unemployment claims.

2 145. Such fraud may go undetected until debt collection calls commence months, or
3 even years, later. An individual may not know that his or her PII was used to file for
4 unemployment benefits until law enforcement notifies the individual's employer of the
5 suspected fraud. Fraudulent tax returns are typically discovered only when an individual's
6 authentic tax return is rejected.

7
8 146. Consequently, Plaintiff and Class Members are at an increased risk of fraud and
9 identity theft for many years into the future.

10
11 147. The retail cost of credit monitoring and identity theft monitoring can cost around
12 \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class
13 Members from the risk of identity theft that arose from Defendant's Data Breach.

14 ***Plaintiff Barbara Squier's Experience***

15
16 148. Plaintiff Barbara Squier was not familiar with Defendant prior to receiving the
17 Notice Letter in the mail, but upon information and belief, Defendant obtained her PII in the
18 course of its regular business operations.

19 149. Upon information and belief, at the time of the Data Breach, Defendant
20 maintained Plaintiff's PII in its system.

21
22 150. Plaintiff Squier is very careful about sharing her sensitive PII. Plaintiff stores any
23 documents containing her PII in a safe and secure location. She has never knowingly
24 transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff
25 would not have entrusted her PII to Defendant had she known of Defendant's lax data security
26 policies.
27



1 151. Plaintiff Barbara Squier received the Notice Letter, by U.S. mail, directly from
2 Defendant, dated March 29 2024. According to the Notice Letter, Plaintiff’s PII was improperly
3 accessed and obtained by unauthorized third parties, including her name and Social Security
4 number.

5
6 152. As a result of the Data Breach, and at the direction of Defendant’s Notice Letter,
7 which instructs Plaintiff to “remain vigilant by reviewing your account statements and credit
8 reports closely[,]”⁴³ Plaintiff made reasonable efforts to mitigate the impact of the Data Breach,
9 including researching and verifying the legitimacy of the Data Breach and monitoring her
10 financial accounts for any indication of fraudulent activity, which may take years to detect.
11 Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff
12 otherwise would have spent on other activities, including but not limited to work and/or
13 recreation. This time has been lost forever and cannot be recaptured.

14
15
16 153. Plaintiff suffered actual injury from having her PII compromised as a result of the
17 Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost
18 or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to
19 mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with
20 attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii)
21 nominal damages; and (viii) the continued and certainly increased risk to her PII, which: (a)
22 remains unencrypted and available for unauthorized third parties to access and abuse; and (b)
23 remains backed up in Defendant’s possession and is subject to further unauthorized disclosures
24
25

26 _____
27 ⁴³ Notice Letter.

1 so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

2 154. Plaintiff additionally suffered actual injury in the form of experiencing an
3 increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by
4 the Data Breach. This misuse of her PII was caused, upon information and belief, by the fact
5 that cybercriminals are able to easily use the information compromised in the Data Breach to
6 find more information about an individual, such as their phone number or email address, from
7 publicly available sources, including websites that aggregate and associate personal
8 information with the owner of such information.
9

10 155. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has
11 been compounded by the fact that Defendant has still not fully informed her of key details about
12 the Data Breach's occurrence.
13

14 156. As a result of the Data Breach, Plaintiff anticipates spending considerable time
15 and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.
16

17 157. As a result of the Data Breach, Plaintiff is at a present risk and will continue to
18 be at increased risk of identity theft and fraud for years to come.
19

20 158. Plaintiff Barbara Squier has a continuing interest in ensuring that her PII, which,
21 upon information and belief, remains backed up in Defendant's possession, is protected and
22 safeguarded from future breaches.
23

24 CLASS ALLEGATIONS

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

1 160. The Class that Plaintiff seeks to represent is defined as follows:

2 **Nationwide Class**

3 All individuals residing in the United States whose PII was accessed and/or
4 acquired by an unauthorized party as a result of the data breach reported by
5 Defendant in March 2024 (the “Class”).

6 161. Excluded from the Class are the following individuals and/or entities: Defendant
7 and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which
8 Defendant have a controlling interest; all individuals who make a timely election to be excluded
9 from this proceeding using the correct protocol for opting out; and all judges assigned to hear
10 any aspect of this litigation, as well as their immediate family members.

11 162. Plaintiff reserves the right to amend the definitions of the Class or add a Class or
12 Subclass if further information and discovery indicate that the definitions of the Class should
13 be narrowed, expanded, or otherwise modified.

14 163. Numerosity: The members of the Class are so numerous that joinder of all
15 members is impracticable, if not completely impossible. According to the breach report
16 submitted to the Office of the Maine Attorney General, at least 211,000 Class Members were
17 impacted in the Data Breach.⁴⁴ The Class is apparently identifiable within Defendant's records,
18 and Defendant has already identified these individuals (as evidenced by sending them breach
19 notification letters).

20 164. Common questions of law and fact exist as to all members of the Class and
21 predominate over any questions affecting solely individual members of the Class. Among the
22
23
24
25

26 ⁴⁴ See [https://apps.web.maine.gov/online/aeviewer/ME/40/bfabbd9-6593-4e0f-a9b5-
27 bf21a94b2329.shtml](https://apps.web.maine.gov/online/aeviewer/ME/40/bfabbd9-6593-4e0f-a9b5-bf21a94b2329.shtml)

1 questions of law and fact common to the Class that predominate over questions which may
2 affect individual Class members, including the following:

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



PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress
2 the imminent and currently ongoing harm faced as a result of the Data Breach.

3 165. Typicality: Plaintiff's claims are typical of those of the other members of
4 the Class because Plaintiff, like every other Class Member, was exposed to virtually
5 identical conduct and now suffers from the same violations of the law as each other
6 member of the Class.

7
8 166. Policies Generally Applicable to the Class: This class action is also appropriate
9 for certification because Defendant acted or refused to act on grounds generally applicable to
10 the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible
11 standards of conduct toward the Class Members and making final injunctive relief appropriate
12 with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect
13 Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's
14 conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

15
16
17 167. Adequacy: Plaintiff will fairly and adequately represent and protect the interests
18 of the Class Members in that she has no disabling conflicts of interest that would be antagonistic
19 to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to
20 the Class Members and the infringement of the rights and the damages she has suffered are
21 typical of other Class Members. Plaintiff has retained counsel experienced in complex class
22 action and data breach litigation, and Plaintiff intend to prosecute this action vigorously.

23
24 168. Superiority and Manageability: The class litigation is an appropriate method for
25 fair and efficient adjudication of the claims involved. Class action treatment is superior to all
26 other available methods for the fair and efficient adjudication of the controversy alleged herein;
27

1 it will permit a large number of Class Members to prosecute their common claims in a single
2 forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort,
3 and expense that hundreds of individual actions would require. Class action treatment will
4 permit the adjudication of relatively modest claims by certain Class Members, who could not
5 individually afford to litigate a complex claim against large corporations, like Defendant.
6 Further, even for those Class Members who could afford to litigate such a claim, it would still
7 be economically impractical and impose a burden on the courts.
8

9
10 169. The nature of this action and the nature of laws available to Plaintiff and Class
11 Members make the use of the class action device a particularly efficient and appropriate
12 procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because
13 Defendant would necessarily gain an unconscionable advantage since they would be able to
14 exploit and overwhelm the limited resources of each individual Class Member with superior
15 financial and legal resources; the costs of individual suits could unreasonably consume the
16 amounts that would be recovered; proof of a common course of conduct to which Plaintiff was
17 exposed is representative of that experienced by the Class and will establish the right of each
18 Class Member to recover on the cause of action alleged; and individual actions would create a
19 risk of inconsistent results and would be unnecessary and duplicative of this litigation.
20
21

22 170. The litigation of the claims brought herein is manageable. Defendant's uniform
23 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class
24 Members demonstrates that there would be no significant manageability problems with
25 prosecuting this lawsuit as a class action.
26

27 171. Adequate notice can be given to Class Members directly using information

1 maintained in Defendant's records.

2 172. Unless a Class-wide injunction is issued, Defendant may continue in its failure to
3 properly secure the PII of Class Members, Defendant may continue to refuse to provide proper
4 notification to Class Members regarding the Data Breach, and Defendant may continue to act
5 unlawfully as set forth in this Complaint.
6

7 173. Further, Defendant has acted on grounds that apply generally to the Class as a
8 whole, so that class certification, injunctive relief, and corresponding declaratory relief are
9 appropriate on a class- wide basis.
10

11 174. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification
12 because such claims present only particular, common issues, the resolution of which would
13 advance the disposition of this matter and the parties' interests therein. Such particular issues
14 include, but are not limited to:
15

- 16 a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data
17 Breach;
- 18 b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due
19 care in collecting, storing, and safeguarding their PII;
- 20 c. Whether Defendant's security measures to protect their data systems were
21 reasonable in light of best practices recommended by data security experts;
- 22 d. Whether Defendant's failure to institute adequate protective security measures
23 amounted to negligence;
- 24 e. Whether Defendant failed to take commercially reasonable steps to safeguard
25 consumer PII; and Whether adherence to FTC data security recommendations,
26
27

1 and measures recommended by data security experts would have reasonably
2 prevented the Data Breach.

3 **CAUSES OF ACTION**

4 **COUNT I**

5 **Negligence**

6 **(On Behalf of Plaintiff and the Class)**

7 175. Plaintiff re-alleges and incorporates by reference all of the allegations contained
8 in paragraphs 1 through 174, as if fully set forth herein.

9 176. Defendant required Plaintiff and Class Members, to submit non-public PII in the
10 ordinary course of providing its mortgage products and/or services.

11 177. Defendant gathered and stored the PII of Plaintiff and Class Members as part of
12 its business of soliciting its services, which solicitations and services affect commerce.

13 178. Plaintiff and Class Members entrusted Defendant with their PII with the
14 understanding that Defendant would safeguard their information.

15 179. Defendant had full knowledge of the sensitivity of the PII and the types of harm
16 that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

17 180. By voluntarily undertaking and assuming the responsibility to collect and store
18 this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had
19 a duty of care to use reasonable means to secure and safeguard their computer property—and
20 Class Members' PII held within it—to prevent disclosure of the information, and to safeguard
21 the information from theft. Defendant's duty included a responsibility to implement processes
22 by which they could detect a breach of its security systems in a reasonably expeditious period
23 of time and to give prompt notice to those affected in the case of a data breach.
24
25
26
27

P

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 181. Defendant had a duty to employ reasonable security measures under Section 5 of
2 the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or
3 affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of
4 failing to use reasonable measures to protect confidential data.

5
6 182. Defendant's duty to use reasonable security measures also arose under the GLBA,
7 under which they were required to protect the security, confidentiality, and integrity of customer
8 information by developing a comprehensive written information security program that contains
9 reasonable administrative, technical, and physical safeguards.

10
11 183. Defendant owed a duty of care to Plaintiff and Class Members to provide data
12 security consistent with industry standards and other requirements discussed herein, and to
13 ensure that its systems and networks adequately protected the PII.

14
15 184. Defendant's duty of care to use reasonable security measures arose as a result of
16 the special relationship that existed between Q Financial and Plaintiff and Class Members. That
17 special relationship arose because Plaintiff and the Class entrusted Q Financial with their
18 confidential PII, a necessary part of being customers of Defendant.

19
20 185. Defendant's duty to use reasonable care in protecting confidential data arose not
21 only as a result of the statutes and regulations described above, but also because Defendant is
22 bound by industry standards to protect confidential PII.

23
24 186. Defendant was subject to an “independent duty,” untethered to any contract
25 between Defendant and Plaintiff or the Class.

26
27 187. Defendant also had a duty to exercise appropriate clearinghouse practices to
remove former customers' PII it was no longer required to retain pursuant to regulations.

P

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 188. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and
2 the Class of the Data Breach.

3 189. Defendant had and continues to have a duty to adequately disclose that the PII of
4 Plaintiff and the Class within Defendant's possession might have been compromised, how it
5 was compromised, and precisely the types of data that were compromised and when. Such
6 notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and
7 repair any identity theft and the fraudulent use of their PII by third parties.
8

9 190. Defendant breached its duties, pursuant to the FTC Act, GLBA, and other
10 applicable standards, and thus was negligent, by failing to use reasonable measures to protect
11 Class Members' PII. The specific negligent acts and omissions committed by Defendant
12 include, but are not limited to, the following:
13

- 14 a. Failing to adopt, implement, and maintain adequate security measures to
15 safeguard Class Members' PII;
- 16 b. Failing to adequately monitor the security of their networks and systems;
- 17 c. Allowing unauthorized access to Class Members' PII;
- 18 d. Failing to detect in a timely manner that Class Members' PII had been
19 compromised;
- 20 e. Failing to remove former customers' PII it was no longer required to retain
21 pursuant to regulations, and
- 22 f. Failing to timely and adequately notify Class Members about the Data Breach's
23 occurrence and scope, so that they could take appropriate steps to mitigate the
24 potential for identity theft and other damages.
25
26
27

P

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 191. Defendant violated Section 5 of the FTC Act and GLBA by failing to use
2 reasonable measures to protect PII and not complying with applicable industry standards, as
3 described in detail herein. Defendant's conduct was particularly unreasonable given the nature
4 and amount of PII it obtained and stored and the foreseeable consequences of the immense
5 damages that would result to Plaintiff and the Class.
6

7 192. Plaintiff and Class Members were within the class of persons the Federal Trade
8 Commission Act and GLBA were intended to protect and the type of harm that resulted from
9 the Data Breach was the type of harm that the statutes were intended to guard against.
10

11 193. Defendant's violation of Section 5 of the FTC Act and GLBA constitutes
12 negligence.

13 194. The FTC has pursued enforcement actions against businesses, which, as a result
14 of their failure to employ reasonable data security measures and avoid unfair and deceptive
15 practices, caused the same harm as that suffered by Plaintiff and the Class.
16

17 195. A breach of security, unauthorized access, and resulting injury to Plaintiff and the
18 Class was reasonably foreseeable, particularly in light of Defendant's inadequate security
19 practices.
20

21 196. It was foreseeable that Defendant's failure to use reasonable measures to protect
22 Class Members' PII would result in injury to Class Members. Further, the breach of security
23 was reasonably foreseeable given the known high frequency of cyberattacks and data breaches
24 in the mortgage industry.
25

26 197. Defendant has full knowledge of the sensitivity of the PII and the types of harm
27 that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

1 198. Plaintiff and the Class were the foreseeable and probable victims of any
2 inadequate security practices and procedures. Defendant knew or should have known of the
3 inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance
4 of providing adequate security of that PII, and the necessity for encrypting PII stored on
5 Defendant's systems or transmitted through third party systems.
6

7 199. It was therefore foreseeable that the failure to adequately safeguard Class
8 Members' PII would result in one or more types of injuries to Class Members.
9

10 200. Plaintiff and the Class had no ability to protect their PII that was in, and possibly
11 remains in, Defendant's possession.

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

14 202. Defendant's duty extended to protecting Plaintiff and the Class from the risk of
15 foreseeable criminal conduct of third parties, which has been recognized in situations where the
16 actor's own conduct or misconduct exposes another to the risk or defeats protections put in
17 place to guard against the risk, or where the parties are in a special relationship. *See* Restatement
18 (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence
19 of a specific duty to reasonably safeguard personal information.
20

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

24 204. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff
25 and the Class, the PII of Plaintiff and the Class would not have been compromised.
26

27 205. There is a close causal connection between Defendant's failure to implement

1 security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent
2 harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and
3 accessed as the proximate result of Defendant's failure to exercise reasonable care in
4 safeguarding such PII by adopting, implementing, and maintaining appropriate security
5 measures.

6
7 206. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class
8 have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii)
9 theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs
10 associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost
11 opportunity costs associated with attempting to mitigate the actual consequences of the Data
12 Breach; (vi) actual misuse of the compromised data consisting of an increase in spam calls,
13 texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued
14 and certainly increased risk to their PII, which: (a) remains unencrypted and available for
15 unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's
16 possession and is subject to further unauthorized disclosures so long as Defendant fails to
17 undertake appropriate and adequate measures to protect the PII.

18
19
20
21 207. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff
22 and the Class have suffered and will suffer the continued risks of exposure of their PII, which
23 remain in Defendant's possession and is subject to further unauthorized disclosures so long as
24 Defendant fails to undertake appropriate and adequate measures to protect the PII in its
25 continued possession.

26
27 208. Plaintiff and Class Members are entitled to compensatory and consequential

1 damages suffered as a result of the Data Breach.

2 209. Plaintiff and Class Members are also entitled to injunctive relief requiring
3 Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to
4 future annual audits of those systems and monitoring procedures; and (iii) continue to provide
5 adequate credit monitoring to all Class Members.
6

7 **COUNT II**
8 **Negligence *Per Se***
9 **(On Behalf of Plaintiff and the Class)**

10 210. Plaintiff re-alleges and incorporates by reference all of the allegations
11 contained in paragraphs 1 through 174, as if fully set forth herein.

12 211. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a
13 duty to provide fair and adequate computer systems and data security practices to safeguard
14 Plaintiff's and Class Members' PII.

15
16 212. Defendant's duty to use reasonable security measures also arose under the GLBA,
17 under which they were required to protect the security, confidentiality, and integrity of customer
18 information by developing a comprehensive written information security program that contains
19 reasonable administrative, technical, and physical safeguards.
20

21 213. Defendant breached its duties to Plaintiff and Class Members under the FTCA
22 and GLBA by failing to provide fair, reasonable, or adequate computer systems and data
23 security practices to safeguard Plaintiff's and Class Members' PII.

24 214. Defendants' failure to comply with applicable laws and regulations constitutes
25 negligence *per se*.
26

27 215. Plaintiff and Class Members are within the class of persons the statutes were

1 intended to protect and the harm to Plaintiff and Class Members resulting from the Data Breach
2 was the type of harm against which the statutes were intended to prevent.

3 216. But for Defendants' wrongful and negligent breach of their duties owed to
4 Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

5 217. The injury and harm suffered by Plaintiff and Class Members was the reasonably
6 foreseeable result of Defendants' breach of their duties. Defendant knew or should have known
7 that by failing to meet its duties, Defendants' breach would cause Plaintiff and Class Members
8 to experience the foreseeable harms associated with the exposure of their PII.
9

10 218. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and
11 Class Members have suffered injury and are entitled to compensatory, consequential, and
12 punitive damages in an amount to be proven at trial.
13

14 **COUNT III**
15 **Unjust Enrichment**
16 **(On Behalf of Plaintiff and the Class)**

17 219. Plaintiff re-alleges and incorporates by reference all of the allegations contained
18 in paragraphs 1 through 174, as if fully set forth herein.

19 220. Plaintiff and Class Members conferred a monetary benefit on Defendant.
20 Specifically, they paid Defendant and/or its agents for products and/or services and in so doing
21 also provided Defendant with their PII. In exchange, Plaintiff and Class Members should have
22 received from Defendant the products and/or services that were the subject of the transaction
23 and should have had their PII protected with adequate data security.
24

25 221. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and
26 has accepted and retained that benefit by accepting and retaining the PII entrusted to it.
27

1 Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII
2 for business purposes.

3 222. Defendant diverted funds intended to pay for data security to its own profit and
4 failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate
5 Plaintiff or Class Members for the value that their PII provided.
6

7 223. Defendant acquired the PII through inequitable record retention as it failed to
8 investigate and/or disclose the inadequate data security practices previously alleged.
9

10 224. If Plaintiff and Class Members had known that Defendant would not use adequate
11 data security practices, procedures, and protocols to adequately monitor, supervise, and secure
12 their PII, they would have entrusted their PII at Defendant or obtained products and/or services
13 at Defendant.

14 225. Plaintiff and Class Members have no adequate remedy at law.

15 226. Under the circumstances, it would be unjust for Defendant to be permitted to
16 retain any of the benefits that Plaintiff and Class Members conferred upon it.
17

18 227. As a direct and proximate result of Defendant's conduct, Plaintiff and Class
19 Members have suffered and will suffer injury, including but not limited to: (i) invasion of
20 privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity
21 costs associated with attempting to mitigate the actual consequences of the Data Breach; (v)
22 loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate
23 the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts,
24 and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and
25 certainly increased risk to their PII, which: (a) remains unencrypted and available for
26
27

P

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1 unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's
2 possession and is subject to further unauthorized disclosures so long as Defendant fails to
3 undertake appropriate and adequate measures to protect the PII.

4 228. Plaintiff and Class Members are entitled to full refunds, restitution, and/or
5 damages from Defendant and/or an order proportionally disgorging all profits, benefits, and
6 other compensation obtained by Defendant from its wrongful conduct. This can be
7 accomplished by establishing a constructive trust from which the Plaintiff and Class Members
8 may seek restitution or compensation.
9

10 229. Plaintiff and Class Members may not have an adequate remedy at law against
11 Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the
12 alternative to, other claims pleaded herein.
13

14 **PRAYER FOR RELIEF**

15 **WHEREFORE**, Plaintiff, on behalf of herself and Class Members, requests judgment
16 against Defendant and that the Court grants the following:
17

- 18 A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to
19 represent the Class;
20
21 B. For equitable relief enjoining Defendant from engaging in the wrongful conduct
22 complained of herein pertaining to the misuse and/or disclosure of the PII of
23 Plaintiff and Class Members;
24
25 C. For injunctive relief requested by Plaintiff, including but not limited to,
26 injunctive and other equitable relief as is necessary to protect the interests of
27 Plaintiff and Class Members, including but not limited to an order:

- i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
- ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
- iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;
- v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
- vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
- vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on



PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27



PEREZ LAW GROUP, PLLC
7508 North 69th Avenue
Glendale, Arizona 85301

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

1 response to a breach;

2 xiv. requiring Defendant to implement a system of tests to assess its respective
3 employees' knowledge of the education programs discussed in the preceding
4 subparagraphs, as well as randomly and periodically testing employees'
5 compliance with Defendant's policies, programs, and systems for protecting
6 personal identifying information;

7
8 xv. requiring Defendant to implement, maintain, regularly review, and revise as
9 necessary a threat management program designed to appropriately monitor
10 Defendant's information networks for threats, both internal and external, and
11 assess whether monitoring tools are appropriately configured, tested, and
12 updated;

13
14 xvi. requiring Defendant to meaningfully educate all Class Members about the
15 threats that they face as a result of the loss of their confidential personal
16 identifying information to third parties, as well as the steps affected
17 individuals must take to protect herself;

18
19 xvii. requiring Defendant to implement logging and monitoring programs
20 sufficient to track traffic to and from Defendant's servers; and

21
22 xviii. for a period of 10 years, appointing a qualified and independent third party
23 assessor to conduct a SOC 2 Type 2 attestation on an annual basis to
24 evaluate Defendant's compliance with the terms of the Court's final
25 judgment, to provide such report to the Court and to counsel for the class,
26 and to report any deficiencies with compliance of the Court's final
27



PEREZ LAW GROUP, PLLC
7508 North 89th Avenue
Glendale, Arizona 85301

1 judgment;

2 D. For an award of damages, including actual, nominal, statutory, consequential,
3 and punitive damages, as allowed by law in an amount to be determined;

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

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

7 G. Such other and further relief as this Court may deem just and proper.
8

9 **JURY TRIAL DEMANDED**

10 Plaintiff hereby demands a trial by jury on all claims so triable.
11

12
13 Dated: April 10, 2024.

Respectfully Submitted,

14 */s/ Cristina Perez Hesano*

15 Cristina Perez Hesano (#027023)

16 *cperez@perezlawgroup.com*

17 **PEREZ LAW GROUP, PLLC**

18 7508 N. 59th Avenue

19 Glendale, AZ 85301

20 Telephone: 602.730.7100

21 Fax: 623.235.6173

22 John J. Nelson*

23 **MILBERG COLEMAN BRYSON**

24 **PHILLIPS GROSSMAN, PLLC**

25 280 S. Beverly Drive

26 Beverly Hills, CA 90212

27 Telephone: (858) 209-6941

Email: *jnelson@milberg.com*

Attorney for Plaintiff and

The Proposed Class

**Pro Hac Vice application forthcoming*

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Mortgage Company On Q Financial Facing Class Action Over Cyberattack Affecting 211K People](#)
