UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

EMMANUEL LLAMAS, an individual and California resident, on behalf of himself and all others similarly situated, Plaintiff, vs. TRUEFIRE, LLC, and TRUEFIRE, INC. Defendants.	Case No.: _____ **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff, Emmanuel Llamas ("Plaintiff"), brings this Class Action Complaint against TrueFire, LLC and TrueFire, Inc. (collectively, "TrueFire" or "Defendants"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. TrueFire specializes in selling online guitar lessons on TrueFire's mobile apps and popular websites, including www.truefire.com, www.truefirestudios.com, and www.jamplay.com. The company claims to have "a worldwide community of over three million music students." For online sales, TrueFire uses an ecommerce platform to take customers' personal and payment information.

2. On or about March 9, 2020, TrueFire began notifying customers and various state Attorneys General about a widespread data breach that occurred from August 3, 2019 to January 14, 2020. Hackers not only "scraped" many of TrueFire's customers' names from the website by infecting it with malware, they also stole customers' addresses, payment card numbers, CVV security codes, and credit card expiration dates ("PII") (the "Breach"). The criminals obtained

everything they needed to illegally use TrueFire's customers' credit cards to make fraudulent purchases, and to steal the customers' identities.

3. Not only did hackers skim TrueFire's customers' PII, on information and belief the stolen names and card information are now for sale on the dark web. That means the Breach worked. Hackers accessed and then offered for sale the unencrypted, unredacted stolen PII to criminals. Because of Defendants' Breach, customers' PII is still available on the dark web for criminals to access and abuse. TrueFire's customers face a lifetime risk of identity theft.

4. This PII was compromised due to TrueFire's negligent and/or careless acts and omissions and the failure to protect customers' data. In addition to TrueFire's failure to prevent the Breach, Defendants failed to detect the Breach for over five months, and when they did discover the Breach on January 10, 2020, it took them almost two more months to report the Breach to the affected customers on or about March 9, 2020.

5. The stolen PII has great value to hackers: It is likely that hundreds of thousands of music students—residents of most states—were affected by the Breach. For example, TrueFire filed data breach notices in California, Indiana, Illinois, Massachusetts and Montana, among others.

6. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect their users' PII; (ii) warn users of their inadequate information security practices; and (iii) effectively monitor TrueFire's websites, apps, and ecommerce platforms for security vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates several California and Florida statutes.

7. Plaintiff and similarly situated TrueFire customers ("Class Members") have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery

from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Breach, including but not limited to lost time, (iv) deprivation of rights they possess under Florida's Deceptive and Unfair Trade Practices Act (Florida Statute § 501.203, *et seq*.); (v) deprivation of rights they possess under the California Unfair Competition Law, (Cal. Business & Professions Code § 17200, *et seq*.); (vi) deprivation of rights they possess under the California Consumer Privacy Act, (Cal. Civ. Code § 1798.100, *et seq*. (§ 1798.150(a)); and (vii) the continued and certainly an increased risk to their PII, which: (a) remains available on the dark web for individuals to access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

II. PARTIES

8. Plaintiff Emmanuel Llamas is a citizen of California residing in San Diego County, California. Mr. Llamas purchased TrueFire classes in 2019 using his debit card, including on or about October 11, 2019. He received TrueFire's *Notice of Data Breach*, dated March 10, 2020, on or about that date.

9. Defendant TrueFire, Inc (aka TrueFire.com, Inc.) was incorporated in Florida with its principle place of business located at 2500 Emerson Avenue South, St. Petersburg, Florida, from approximately February 26, 1999, until approximately November 22, 2019, when it was converted to a limited liability company. During the relevant period and prior to that conversion, TrueFire operated across the United States through TrueFire's apps and websites.

10. Defendant TrueFire, LLC, is a Florida Limited Liability Company with its principal place of business located at 2500 Emerson Avenue South, St. Petersburg, Florida. Upon information and belief, the members of TrueFire, LLC, are: Ren F. Wright, Jr., a Florida resident; and Ignite Legacy Holdings, LLC, whose sole member is Brad Wendkos, a Florida Resident.

During the relevant period, TrueFire operated across the United States through TrueFire's apps and websites.

III. JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants. Plaintiff is a citizen of California and therefore diverse from TrueFire, LLC, which is headquartered in Florida.

12. This Court has personal jurisdiction over Defendants because TrueFire is headquartered in St. Petersburg, Florida and conducts business in the state. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District.

IV. FACTUAL ALLEGATIONS

Background

13. TrueFire was founded in 1991 and boasts that it has over 600 "top educators" and what *Guitar Player Magazine* calls "the planet's largest and most comprehensive selection of online guitar lessons."[1] In late 2019, TrueFire, Inc. merged with a competing online guitar lesson website, JamPlay.com, to form TrueFire, LLC, also referred to as TrueFire Studios. The "alliance" of these companies, according to TrueFire, increased TrueFire's worldwide customer base to over 3 million.[2]

[1] www.truefire.com/about (last accessed on Apr. 6, 2020).
[2] https://newyork.citybizlist.com/article/604008/truefire-studios-appoints-owen-grover-ceo (last accessed on Apr. 6, 2020).

14. Customers demand security to safeguard their PII. TrueFire touts the secure nature of TrueFire's website in the Privacy Policy: "we strive to protect your personal data."[3] TrueFire claims that it would be an "unlikely event" that TrueFire's customers' "personal data in our control" would be "compromised." TrueFire also states: "we may process your personal data to: Protect you, us or others from threats (such as security threats or fraud)," and:

> TrueFire . . . is committed to respecting the privacy rights of its customers, visitors, and other users of the Company Websites . . . and Mobile Applications[.] We created this Privacy Policy to give you confidence as you visit and use our Services and to demonstrate our commitment to fair information practices and to the protection of privacy. This Privacy Policy is only applicable to the Services, and not to any other websites that you may be able to access from the Services, each of which may have data collection, storage, and use practices and policies that differ materially from this Privacy Policy.

15. The PCI DSS (Payment Card Industry Data Security Standard) compliance is a requirement for businesses that store, process, or transmit payment card data. The PCI DSS defines measures for ensuring data protection and consistent security processes and procedures around online financial transactions.

16. As formulated by the PCI Security Standards Council, the mandates of PCI DSS compliance include, in part: Developing and maintaining a security policy that covers all aspects of the business, installing firewalls to protect data, and encrypting cardholder data that is transmitted over public networks using anti-virus software and updating it regularly.[4]

17. TrueFire offers free memberships, options to purchase individual educational products and services, and options to purchase subscriptions to certain educational products and services. Customers can purchase a monthly or annual subscription for a product or service; monthly fees are $29; annual fees range from $149 to $249 per year. A lifetime membership is

[3] TrueFire Privacy Policy, Effective Date: May 28, 2018; *available at*: www.truefire.com/privacy-policy (last accessed on Apr. 6, 2020).
[4] PCI Security Standards Council, *available at*: https://www.pcisecuritystandards.org/ (last accessed Jan. 30, 2020).

$1,499.[5]

18. To purchase products, services or subscriptions on TrueFire's websites, customers must create an account. To complete a purchase, at a minimum, the customer must enter the following PII:

- Name;
- billing address;
- email address;
- name on the credit card;
- type of credit card;
- full credit card number;
- credit card expiration date; and
- security code, or CVV code (card verification number).

19. At no time during the final checkout process does TrueFire require customers to expressly agree to TrueFire's "Terms of Use" or "Terms & Conditions."

The Data Breach

20. Beginning on or about March 9, 2020, TrueFire LLC sent customers a *Notice of Data Breach*.[6] TrueFire's Chief Customer Officer, Ren Wright, informed the recipients of the notice that:

> **What happened?** On January 10, 2020, TrueFire discovered that an unauthorized person gained access to our computer system and, more specifically, to information that consumers had entered through the Website. While we do not store credit card information on our website, it appears that the unauthorized person gained access to the Website and could have accessed the data of consumers who made payment card purchases, while that data was being entered, between August 3, 2019 and January 14, 2020.
>
> **What Information Was Involved?** We cannot state with certainty that your data was specifically accessed, however you should know that the information that was potentially subject to unauthorized access includes your: name, address, payment card account number, card expiration data and security code.[7]

[5] https://truefire.com/all-access/upgrade/ (last accessed Apr. 6, 2020).
[6] TrueFire LLC's *Notification of Data Breach*, March 9, 2020, archived by the California Attorney General, *available at*: https://oag.ca.gov/system/files/TrueFire%20-%20Notice%20of%20Data%20Event%20-%20CA.pdf (last accessed Apr. 6, 2020).
[7] *Id.*

> **What are we doing?** We take the privacy and protection of personal information very seriously. As soon as we discovered the incident, we immediately took steps to address it, including working with computer forensic specialists to determine the full nature and scope of the intrusion and reporting the incident to law enforcement. We are continuing to monitor all activity on the Website to ensure the intrusion remains contained, and are working with an outside computer forensic team to monitor, remediate and identify any issues.

21. TrueFire's customers' information is likely for sale on the dark web and, on information and belief, is still for sale to criminals. This means that the breach was successful; unauthorized individuals accessed TrueFire's customers' unencrypted, unredacted information, including "name, address, payment card account number, card expiration date and security code," and possibly more, without alerting Defendants, then offered the "scraped" information for sale online. There is no indication that Defendants' customers' PII was removed from the dark web where it likely remains.

22. During the time TrueFire admits hackers were "scraping" TrueFire's customers' PII, the FBI issued yet another warning to companies about this exact type of fraud. In the FBI's *Oregon FBI Tech Tuesday: Building a Digital Defense Against E-Skimming*, dated October 22, 2019, the agency stated:

> This warning is specifically targeted to . . . businesses . . . that take credit card payments online. E-skimming occurs when cyber criminals inject malicious code onto a website. The bad actor may have gained access via a phishing attack targeting your employees—or through a vulnerable third-party vendor attached to your company's server.

23. The FBI gave some stern advice to companies like TrueFire:

> Here's what businesses and agencies can do to protect themselves:
> - Update and patch all systems with the latest security software.
> - Anti-virus and anti-malware need to be up-to-date and firewalls strong.
> - Change default login credentials on all systems.
> - Educate employees about safe cyber practices. Most importantly, do not click on links or unexpected attachments in messages.

- Segregate and segment network systems to limit how easily cyber criminals can move from one to another.

24. But Defendants apparently did not take this advice: hackers were actively scraping customers' PII off their website—and continued until at least January 14, 2020.

25. Web scraping or skimming data breaches are commonly made possible through a vulnerability in a website or its backend content management system. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were collecting, causing customers' PII to be exposed and sold on the dark web.

Scraping and E-Skimming Breaches

26. *Magecart* is a loose affiliation of hacker groups responsible for skimming payment card attacks on various high-profile companies, including British Airways and Ticketmaster.[8] Typically, these hackers insert virtual credit card skimmers or scrapers (also known as *formjacking*) into a web application (usually the shopping cart), and proceed to scrape credit card information to sell on the dark web.[9]

27. The hackers target what they refer to as the *fullz*; a term used by criminals to refer to stealing the full primary account number, card holder contact information, credit card number, CVV security code and expiration date. The *fullz* is exactly what TrueFire admits the malware infecting TrueFire's platform scraped.

28. These cyber-attacks exploit weaknesses in the code of the ecommerce platform, without necessarily comprising the victim websites' networks or servers.[10] These attacks have targeted payment processors, but the attack on British Airways in 2018 was far more tailored to

[8] *Magecart Hits 80 Major eCommerce Sites in Card-Skimming Bonanza*, Threatpost, Aug. 28, 2019, *available at*: https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/ (last accessed Jan. 30, 2020).
[9] *Id*.
[10] *What is Magecart and was it behind the Ticketmaster and BA hacks?*, Computerworld, Sep. 18, 2018, *available at*: https://www.computerworld.com/article/3427858/what-is-magecart-and-was-it-behind-the-ticketmaster-and-ba-hacks-.html (last accessed Jan. 30, 2020).

the company's particular infrastructure, as may be the case here.[11]

29. Magecart and these scraping breaches are not new: RiskIQ's earliest Magecart observation occurred on August 8th, 2010.[12] Since it's been going on for almost a decade, and with the well-publicized and widespread attacks on British Airways and Ticketmaster, among many others in and since 2018, Defendants should have known the imminent danger facing Defendants' millions of customers.

30. Unfortunately, despite all of the publicly available information of the continued compromises of PII in this manner, including the FBI's current warnings, Defendants' approach to maintaining the privacy and security of Plaintiff's and Class Members' PII was negligent, or at the very least, Defendants did not maintain reasonable security procedures and practices appropriate to the nature of the information to protect their customers' valuable PII.[13]

Value of Personally Identifiable Information

31. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14] Experian reports that a stolen credit or debit

---

[11] *Id*.

[12] *Magecart: New Research Shows the State of a Growing Threat*, RiskIQ, Oct. 4, 2019, *available at*: https://www.riskiq.com/blog/external-threat-management/magecart-growing-threat/ (last accessed Jan. 30, 2020).

[13] While skimming attacks have become more popular, the practice of hackers using legitimate online services to host their infrastructure has expanded. Researchers at Malwarebytes recently discovered a rash of skimmers on the Heroku engagement platform, which is a PaaS run by Salesforce. This platform offers a free starter service for legitimate app developers to deploy, manage and scale their apps without needing to maintain their own infrastructure. Hackers are registering free accounts on Heroku to host their skimming schemes. Malwarebytes reported its findings to the Salesforce Abuse Operations team in late 2019. *There's an app for that: web skimmers found on PaaS Heroku*, Malwarebytes Labs, Dec. 4, 2019, available at: https://blog.malwarebytes.com/web-threats/2019/12/theres-an-app-for-that-web-skimmers-found-on-paas-heroku/ (last accessed Jan. 31, 2020).

[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 30, 2020).

card number can sell for $5 to $110 on the dark web; the *fullz* sold for $30 in 2017.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16]

32. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Defendants' customers as a result of a breach.

33. Defendants were, or should have been, fully aware of the significant volume of daily credit and debit card transactions on Defendants' website—the malware infected Defendants' platform during the lead up to Christmas 2019—amounting to thousands of payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of Defendants' systems.

Plaintiff Llamas' Experience

34. Plaintiff Emmanuel Llamas first became a member of TrueFire through www.truefire.com from his home in San Diego County, California, in or about June 2019. On or about July 4, 2019, he began purchasing online guitar lessons. He made numerous purchases using his bank debit card, including a purchase on or about October 11, 2019, during the period TrueFire admits to being breached.

35. Mr. Llamas made these and other purchases through his TrueFire account. On the payment platform, Mr. Llamas entered his PII: name, billing address, payment card type and full number, CVV security code, debit card expiration date, and email address. During these transactions, Mr. Llamas was not asked to "agree" to any "Terms of Use" or "Terms &

[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 30, 2020).
[16] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Jan. 30, 2020).

Conditions."

36. In late October 2019, Mr. Llamas noticed that the debit card he used on TrueFire earlier that same month was used multiple times by unknown third-parties in another state. He immediately contacted his bank by secure messaging and by telephone. The bank confirmed that his card had been used by unauthorized third-parties.

37. The bank changed Mr. Llamas' account number in response to the illegal charges and mailed him a new debit card. While waiting for the new account number, Mr. Llamas had no choice but to personally go to his bank to withdraw funds to continue to make essential purchases. This required Mr. Llamas to take time out of his day to drive to the bank, withdraw the funds, and drive back to return to his daily activities, time he otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

38. On or about March 10, 2020, TrueFire notified Mr. Llamas by U.S. mail of the Breach in the *Notice of Data Breach*. He did not receive notice by email.

39. In response to the *Notice of Data Breach*, Mr. Llamas again had to spend time dealing with the consequences of the Breach, which includes time reviewing the account compromised by the breach, contacting his bank, exploring credit monitoring options, and self-monitoring his accounts. This is time Mr. Llamas otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

40. Knowing that the hacker stole his PII, and that his PII may be available for sale on the dark web, has caused Mr. Llamas great anxiety. He is now very concerned about credit card theft and identity theft in general. This breach has given Mr. Llamas hesitation about using TrueFire's services, and reservations about shopping on other online websites.

41. Now, due to Defendants' misconduct and the resulting Breach, hackers obtained his PII at no compensation to Mr. Llamas whatsoever. That is money lost for him, and money

gained for the hackers, who could sell his PII on the dark web.

Plaintiff Llamas' Efforts to Secure PII

42. Defendants' Breach caused Mr. Llamas harm.

43. Prior to the activity described above during the period in which the Breach occurred, the debit card Plaintiff used on Defendants' website had never been stolen or compromised. Mr. Llamas reviewed his credit monitoring service, credit report, and other financial statements routinely and this card had not been compromised in any manner.

44. Additionally, Mr. Llamas never transmitted unencrypted PII over the internet or any other unsecured source.

45. Mr. Llamas stores any and all documents containing his PII in a safe and secure physical location, and destroys any documents he receives in the mail that contain any of his PII, or that may contain any information that could otherwise be used to compromise his debit card.

TrueFire's Offer of No Credit Monitoring is Inadequate

46. At present, TrueFire, unlike most companies that commit data breaches, has not offered TrueFire's affected customers free enrollment in a credit monitoring service. Although TrueFire admits that Mr. Llamas' and other Class Members' unencrypted credit card numbers, CVV codes and expiration dates, among other things, have been accessed by unauthorized third-parties through their websites, TrueFire is not willing to even attempt to protect their customers with basic credit monitoring.[17]

47. Consumers' PII may exist on the dark web for months, or even years, before it is used by criminals. With monitoring, and no form of insurance or other protection, Plaintiff and

[17] In the recent Equifax data breach, for example, Equifax agreed to free monitoring of victims' credit reports at all three major credit bureaus for four years, plus $1 million of identity theft insurance. For an additional six years, victims can opt for free monitoring, but it only monitors victims' credit reports at one credit bureau, Equifax. In addition, if a victim's child was a minor in May 2017, he or she is eligible for a total of 18 years of free credit monitoring under the same terms as for adults.

Class Members remain unprotected from the real and long-term threats against their PII; PII that TrueFire admits was scraped from TrueFire's apps and websites.

48. Therefore, the "monitoring" services are inadequate, and Plaintiff and Class Members have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

49. TrueFire's response to the Breach, and the services it offered to consumers to address the breach, are insufficient, resulting in consumers spending a significant amount of time taking measures to protect themselves. Thus, TrueFire cannot be heard to complain about customers taking TrueFire's advice and suggestions for how to respond in the face of this latest data breach.

V. CLASS ALLEGATIONS

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

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

> All individuals whose PII was compromised in the data breach first announced by TrueFire LLC on March 9, 2020 (the "Nationwide Class").

52. The California Subclass is initially defined as follows:

> All persons residing in California whose PII was compromised in the data breach first announced by TrueFire LLC on March 9, 2020 (the "California Subclass").

53. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting

out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

54. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

55. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class and California Subclass (the "Classes") are so numerous that joinder of all members is impracticable. Defendants have identified thousands of customers whose PII may have been improperly accessed in the Breach, and the Classes are apparently identifiable within Defendants' records.

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

a. Whether and when Defendants actually learned of the Breach and whether their response was adequate;

b. Whether Defendants owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class Members' PII;

e. Whether Defendants acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class Members' PII;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiff's and Class Members' PII secure and prevent loss or misuse of that PII;

g. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Breach to occur;

h. Whether Defendants caused Plaintiff and Class Members damages;

i. Whether Defendants violated the law by failing to promptly notify Class Members that their PII had been compromised;

j. Whether Plaintiff and the other Class Members are entitled to credit monitoring and other monetary relief;

k. Whether Defendants violated Florida's Deceptive and Unfair Trade Practices Act (Florida Statute § 501.203, *et seq.*);

l. Whether Defendants violated the California Unfair Competition Law (Business & Professions Code § 17200, *et seq.*)

m. Whether Defendants violated the California Consumer Privacy Act (Cal. Civ. Code § 1798.100, et seq. (§ 1798.150(a)).

57. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Breach, due to Defendants' misfeasance.

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

59. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent

and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

60. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

61. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action

alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

62. TrueFire is based in Florida, and on information and belief, all managerial decisions emanate from Florida, and therefore application of Florida law to the Nationwide Class is appropriate.

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

64. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

65. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

66. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

67. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and the Class Members to

exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiff and the Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

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

e. Whether Class Members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

68. Plaintiff re-allege and incorporates by reference herein all of the allegations contained in paragraphs 1 through 67.

69. As a condition of their utilizing the services of Defendants, Plaintiff and Class Members were obligated to provide Defendants with the PII.

70. Plaintiff and the Class Members entrusted their PII to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

71. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

72. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their customers' PII involved an unreasonable risk of

harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

73. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that Plaintiff and Class Members' information in Defendants' possession was adequately secured and protected.

74. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

75. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of Defendants' inadequate information security practices.

76. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew of should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendants' systems.

77. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII.

78. Plaintiff and the Class Members had no ability to protect their PII that was in Defendants' possession.

79. Defendants were in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Breach.

80. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiff and Class Members within Defendants' possession might have been compromised, how it was compromised, and precisely the types of information that were compromised and when. Such notice was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

81. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

82. Defendants have admitted that the PII of Plaintiff and Class Members was wrongfully disclosed to unauthorized third persons as a result of the Breach.

83. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within Defendants' possession or control.

84. Defendants improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Breach.

85. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect customers' PII in the face of increased risk of theft.

86. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of their customers/patients' PII.

87. Defendants, through their actions and/or omissions, unlawfully breached their duty

to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Breach.

88. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

89. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' PII was stolen and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

90. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of customers in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Defendants' goods and services they received.

91. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II
Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)

92. Plaintiff restate and reallege paragraphs 1 through 67 above as if fully set forth herein.

93. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

94. Defendants owed a duty to their customers, including Plaintiff and Class Members, to keep their PII contained as a part thereof, confidential.

95. Defendants failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and Class Members.

96. Defendants allowed unauthorized and unknown third parties unfettered access to and examination of the PII of Plaintiff and Class Members, by way of Defendants' failure to protect the PII.

97. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and Class Members is highly offensive to a reasonable person.

98. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendants as part of their use of Defendants' services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their

authorization.

99. The Breach at the hands of Defendants constitutes an intentional interference with Plaintiff and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

100. Defendants acted with a knowing state of mind when they permitted the Breach to occur because they were with actual knowledge that their information security practices were inadequate and insufficient.

101. Because Defendants acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

102. As a proximate result of the above acts and omissions of Defendants, the PII of Plaintiff and Class Members was disclosed to and used by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

103. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendants can be viewed, distributed, and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

COUNT III
Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class)

104. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 67.

105. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce,"

including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

106. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Breach for companies of Defendants' magnitude, including, specifically, the immense damages that would result to Plaintiff and Class Members.

107. Defendants' violations of Section 5 of the FTC Act constitute negligence *per se*.

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

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

110. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain

in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Defendants' goods and services they received.

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

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

112. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 67.

113. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Defendants and provided Defendants with their PII. In exchange, Plaintiff and Class Members should have received from Defendants the goods and services that were the subject of the transaction and should have been entitled to have Defendants protect their PII with adequate data security.

114. Defendants knew that Plaintiff and Class Members conferred a benefit on Defendants and accepted and have accepted or retained that benefit. Defendants profited from the purchases and used the PII of Plaintiff and Class Members for business purposes.

115. The amounts Plaintiff and Class Members paid for Defendants' goods and services should have been used, in part, to pay for the administrative costs of data management and security.

116. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement the data management and security measures that are mandated by industry standards.

117. Defendants failed to secure the PII of Plaintiff and Class Members and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

118. Defendants acquired the PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

119. If Plaintiff and Class Members knew that Defendants would not secure their PII using adequate security, they would not have made purchases with Defendants.

120. Plaintiff and Class Members have no adequate remedy at law.

121. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII

compromised as a result of the Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Defendants' goods and services they received.

122. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

123. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants goods and services.

COUNT V
Declaratory Judgment
(On Behalf of Plaintiff and the Nationwide Class)

124. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 67.

125. Defendants owe duties of care to Plaintiff and Class Members which would require it to adequately secure PII.

126. Defendants still possess PII regarding Plaintiff and Class Members.

127. Plaintiff and Class Members' PII is still for sale on the dark web.

128. Although Defendants claim they "are working with an outside computer forensic team to monitor, remediate and identify any issues," there is no detail on what, if any, fixes have really occurred.

129. Plaintiff and Class Members are at risk of harm due to the exposure of their PII and Defendants' failure to address the security failings that lead to such exposure.

130. There is no reason to believe that Defendants' security measures are any more adequate than they were before the breach to meet Defendants' contractual obligations and legal duties, and there is no reason to think Defendants have no other security vulnerabilities that have not yet been knowingly exploited.

131. Plaintiff, therefore, seek a declaration that: (1) each Defendants' existing security measures do not comply with Defendants' explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information; and (2) to comply with Defendants' explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train Defendants' security personnel regarding any new or modified procedures;

d. Ordering that Defendants user applications be segmented by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants conduct regular database scanning and securing checks;

f. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Ordering Defendants to purchase credit monitoring services for Plaintiff and Class Members for a period of ten years; and

h. Ordering Defendants to meaningfully educate Defendants' users about the threats they face as a result of the loss of their PII to third-parties, as well as the steps Defendants customers must take to protect themselves.

COUNT VI
Violation of Florida's Deceptive and Unfair Trade Practices Act,
Florida Statute § 501.203, *et seq*.
(On Behalf of Plaintiff and the Nationwide Class)

132. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 67.

133. Plaintiff and the Class Members are "consumers." Fla. Stat. § 501.203(7).

134. Plaintiff and Class Members purchased "things of value" insofar as products and services from Defendants. These purchases were made primarily for personal, family, or household purposes. Fla. Stat. § 501.203(9).

135. Defendants engaged in the conduct alleged in this Complaint by advertising and entering into transactions intended to result, and which did result, in the sale, rental of goods, services, and/or property to consumers, including Plaintiff and the Class Members. Fla. Stat. § 501.203(8).

136. Defendants engaged in, and their acts and omissions affected trade and commerce. Defendants' acts, practices, and omissions were done in the course of Defendants' business of

advertising, marketing, offering to sell, and selling and/or renting goods and services throughout Florida and the United States. Fla. Stat. § 501.203(8).

137. Defendants, headquartered and operating in Florida, engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. charging a premium for the goods and services, implicitly representing that the premium would be used to protect Plaintiff's and Class Members' protected health information and other PII;

b. failure to timely and accurately disclose the Breach to Plaintiff and the Class Members;

c. continued acceptance of credit and debit card payments and storage of other PII after Defendants knew or should have known of the Breach and before they allegedly remediated the Breach.

138. This conduct is considered unfair methods of competition, and constitutes unfair and unconscionable acts and practices. Fla. Stat. § 501.204(1).

139. As a direct and proximate result of Defendants' violation of Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA"), Plaintiff and the Class Members suffered actual damages by paying a premium for Defendants' goods and services with the understanding that at least part of the premium would be applied toward sufficient and adequate information security practices that comply with industry standards, when in fact no portion of that premium was applied toward sufficient and adequate information security practices. Fla. Stat. § 501.211(2).

140. Moreover, as a direct result of Defendants' knowing violation of FDUTPA, Plaintiff and Class Members are not only entitled to actual damages, but also declaratory judgment

that Defendants' actions and practices alleged herein violate FDUTPA, and injunctive relief, including, but not limited to:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendants segment PII by, among other things, creating firewalls and access controls so that if one area of Defendants is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants purge, delete, and destroy in a reasonable secure manner PII not necessary for their provisions of services;

f. Ordering that Defendants conduct regular database scanning and securing checks;

g. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendants to meaningfully educate their customers about the threats they face as a result of the loss of their financial and personal information to third-parties, as well as the steps Defendants' customers must take to protect themselves.

Fla. Stat. § 501.211(1).

141. Plaintiff bring this action on behalf of themselves and the Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and the Class Members and the public from Defendants' unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful practices. Defendants' wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

142. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and the Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

143. Defendants knew or should have known that the lack of encryption on their computer systems and data security practices were inadequate to safeguard the Class Members' PII and that the risk of a data disclosure or theft was high.

144. Defendants' actions and inactions in engaging in the unfair practices and deceptive acts described herein were negligent, knowing and willful, and/or wanton and reckless.

Plaintiff and the Class Members seek relief under Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq*., including, but not limited to, damages, injunctive relief, and attorneys' fees and costs, and any other just and proper relief.

COUNT VII
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful Business Practices
(On Behalf of the California Subclass)

145. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 67.

146. Defendants have violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the California Class.

147. Defendants engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and California Subclass members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and California Subclass members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendants to take reasonable methods of safeguarding the PII of Plaintiff and the California Subclass members.

148. In addition, Defendants engaged in unlawful acts and practices by failing to disclose the Breach to California Subclass members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

149. As a direct and proximate result of Defendants' unlawful practices and acts, Plaintiff and the California Subclass members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of California Subclass members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

150. Defendants knew or should have known that Defendants' computer systems and data security practices were inadequate to safeguard California Subclass members' PII and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Subclass.

151. California Subclass members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and California Subclass members of money or property that Defendants may have acquired by means of Defendants'

unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of Defendants' unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT VIII
Violation of California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq.* – Unfair Business Practices
(On Behalf of the California Subclass)

152. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 67.

153. Defendants engaged in unfair acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and California Subclass members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and California Subclass members' PII in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and California Subclass members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiff and the California Subclass members outweighed their utility, if any.

154. Defendants engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the Breach to enact adequate privacy and security measures and protect California Subclass members' PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and California Subclass members. They were likely to deceive the public into believing their PII was

securely stored, when it was not. The harm these practices caused to Plaintiff and the California Subclass members outweighed their utility, if any.

155. As a direct and proximate result of Defendants' acts of unfair practices, Plaintiff and the California Subclass members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of California Subclass members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

156. Defendants knew or should have known that Defendants' computer systems and data security practices were inadequate to safeguard California Subclass members' PII and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Subclass.

157. California Subclass members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff and California Subclass members of money or property that the Defendants may have acquired by means of Defendants' unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of Defendants' unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT IX
Violation of the California Consumer Privacy Act,
Cal. Civ. Code § 1798.100, *et seq*. (§ 1798.150(a)
(On Behalf of Plaintiff Llamas and the California Subclass)

158. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 67.

159. Defendants violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff's and California Subclass members' nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and California Class members.

160. As a direct and proximate result of Defendants' acts, Plaintiff's and the California Subclass members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violation of the duty: through TrueFire's website, the ecommerce platform, and/or from the dark web, where hackers further disclosed ("as a result of [Defendants'] violation of the duty") TrueFire's customers' PII from at least August 3, 2019 to January 14, 2020.

161. As a direct and proximate result of Defendants' acts, Plaintiff and the California Subclass members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of California Class members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

162. Defendants knew or should have known that Defendants' computer systems and data security practices were inadequate to safeguard California Subclass members' PII and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and the California Class members.

163. TrueFire is a limited liability company that is organized or operated for the profit or financial benefit of TrueFire's owners, with annual gross revenues over $25 million. TrueFire collects consumers' PII as defined in Cal. Civ. Code § 1798.140.

164. Plaintiff and California Subclass members seek relief under § 1798.150(a), including, but not limited to, recovery of actual damages; injunctive or declaratory relief; any other relief the court deems proper; and attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5).

165. Plaintiff and the California Subclass members reserve the right to amend this Complaint as of right to seek statutory damages and relief under Cal. Civ. Code § 1798.100, *et seq*.

PRAYER FOR RELIEF

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

A. An order certifying the Nationwide Class and California Subclass as defined herein, and appointing Plaintiff and his Counsel to represent the Class;

B. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiff's and Class Members' PII;

C. An order instructing Defendants to purchase or provide funds for credit monitoring services for Plaintiff and all Class Members;

D. An award of compensatory, statutory, and punitive damages, in an amount to be determined;

E. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

F. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

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

DEMAND FOR JURY TRIAL

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

Date: April 14, 2020 Respectfully Submitted,

/s/ *John A. Yanchunis*

John A. Yanchunis *jyanchunis@ForThePeople.com* Ryan J. McGee *rmcgee@ForThePeople.com* **MORGAN & MORGAN COMPLEX LITIGATION GROUP** 201 N. Franklin Street, 7th Floor Tampa, Florida 33602 T: (813) 223-5505 F: (813) 223-5402	M. Anderson Berry (*Pro Hac Vice* Forthcoming) *aberry@justice4you.com* Leslie Guillon (*Pro Hac Vice* Forthcoming) *lguillon@justice4you.com* **CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORPORATION** 865 Howe Avenue Sacramento, CA 95825 T: (916) 777-7777 F: (916) 924-1829

JS 44 (Rev. 09/19)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

EMMANUEL LLAMAS, an individual and California resident, on behalf of himself and all others similarly situated,

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
John A. Yanchunis, Morgan & Morgan Complex Litigation Group
201 N. Franklin St., 7th Floor, Tampa, FL 33602, (813) 223-5505

DEFENDANTS

TRUEFIRE, LLC, and TRUEFIRE, INC.

County of Residence of First Listed Defendant Pinellas
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ❒ 1 U.S. Government Plaintiff
- ❒ 3 Federal Question *(U.S. Government Not a Party)*
- ❒ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	❒ 1	❒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	☒ 4
Citizen of Another State	☒ 2	❒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	❒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ❒ 110 Insurance
- ❒ 120 Marine
- ❒ 130 Miller Act
- ❒ 140 Negotiable Instrument
- ❒ 150 Recovery of Overpayment & Enforcement of Judgment
- ❒ 151 Medicare Act
- ❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ❒ 153 Recovery of Overpayment of Veteran's Benefits
- ❒ 160 Stockholders' Suits
- ❒ 190 Other Contract
- ❒ 195 Contract Product Liability
- ❒ 196 Franchise

REAL PROPERTY
- ❒ 210 Land Condemnation
- ❒ 220 Foreclosure
- ❒ 230 Rent Lease & Ejectment
- ❒ 240 Torts to Land
- ❒ 245 Tort Product Liability
- ❒ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ❒ 310 Airplane
- ❒ 315 Airplane Product Liability
- ❒ 320 Assault, Libel & Slander
- ❒ 330 Federal Employers' Liability
- ❒ 340 Marine
- ❒ 345 Marine Product Liability
- ❒ 350 Motor Vehicle
- ❒ 355 Motor Vehicle Product Liability
- ❒ 360 Other Personal Injury
- ❒ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ❒ 365 Personal Injury - Product Liability
- ❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ❒ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ❒ 370 Other Fraud
- ❒ 371 Truth in Lending
- ❒ 380 Other Personal Property Damage
- ❒ 385 Property Damage Product Liability

CIVIL RIGHTS
- ❒ 440 Other Civil Rights
- ❒ 441 Voting
- ❒ 442 Employment
- ❒ 443 Housing/ Accommodations
- ❒ 445 Amer. w/Disabilities - Employment
- ❒ 446 Amer. w/Disabilities - Other
- ❒ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ❒ 463 Alien Detainee
- ❒ 510 Motions to Vacate Sentence
- ❒ 530 General
- ❒ 535 Death Penalty

Other:
- ❒ 540 Mandamus & Other
- ❒ 550 Civil Rights
- ❒ 555 Prison Condition
- ❒ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ❒ 625 Drug Related Seizure of Property 21 USC 881
- ❒ 690 Other

LABOR
- ❒ 710 Fair Labor Standards Act
- ❒ 720 Labor/Management Relations
- ❒ 740 Railway Labor Act
- ❒ 751 Family and Medical Leave Act
- ❒ 790 Other Labor Litigation
- ❒ 791 Employee Retirement Income Security Act

IMMIGRATION
- ❒ 462 Naturalization Application
- ❒ 465 Other Immigration Actions

BANKRUPTCY
- ❒ 422 Appeal 28 USC 158
- ❒ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ❒ 820 Copyrights
- ❒ 830 Patent
- ❒ 835 Patent - Abbreviated New Drug Application
- ❒ 840 Trademark

SOCIAL SECURITY
- ❒ 861 HIA (1395ff)
- ❒ 862 Black Lung (923)
- ❒ 863 DIWC/DIWW (405(g))
- ❒ 864 SSID Title XVI
- ❒ 865 RSI (405(g))

FEDERAL TAX SUITS
- ❒ 870 Taxes (U.S. Plaintiff or Defendant)
- ❒ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ❒ 375 False Claims Act
- ❒ 376 Qui Tam (31 USC 3729(a))
- ❒ 400 State Reapportionment
- ❒ 410 Antitrust
- ❒ 430 Banks and Banking
- ❒ 450 Commerce
- ❒ 460 Deportation
- ❒ 470 Racketeer Influenced and Corrupt Organizations
- ❒ 480 Consumer Credit (15 USC 1681 or 1692)
- ❒ 485 Telephone Consumer Protection Act
- ❒ 490 Cable/Sat TV
- ❒ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ❒ 891 Agricultural Acts
- ❒ 893 Environmental Matters
- ❒ 895 Freedom of Information Act
- ❒ 896 Arbitration
- ❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ❒ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding | ❒ 2 Removed from State Court | ❒ 3 Remanded from Appellate Court | ❒ 4 Reinstated or Reopened | ❒ 5 Transferred from Another District *(specify)* | ❒ 6 Multidistrict Litigation - Transfer | ❒ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 USC 1332(d)

Brief description of cause:
Tort and consumer protection act claims for loss of confidential information

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 04/13/2020

SIGNATURE OF ATTORNEY OF RECORD /s/John A. Yanchunis

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

Reset

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

EMMANUEL LLAMAS, an individual and California resident, on behalf of himself and all others similarly situated,

Plaintiff(s)

v.

TRUEFIRE, LLC, and TRUEFIRE, INC.

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* TRUEFIRE, INC
c/o Chestnut Business Services, LLC - Registered Agent
911 Chestnut St.
Clearwater, FL 33756

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: John A. Yanchunis
Morgan & Morgan Complex Litigation Group
201 N. Franklin St., 7th Floor
Tampa, FL 33602

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Reset

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

EMMANUEL LLAMAS, an individual and California resident, on behalf of himself and all others similarly situated,

Plaintiff(s)

v.

TRUEFIRE, LLC, and TRUEFIRE, INC.

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* TRUEFIRE, INC
c/o Chestnut Business Services, LLC - Registered Agent
911 Chestnut St.
Clearwater, FL 33756

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: John A. Yanchunis
Morgan & Morgan Complex Litigation Group
201 N. Franklin St., 7th Floor
Tampa, FL 33602

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Reset