DAPEER ROSENBLIT & LITVAK, LLP
William Litvak (CA State Bar No. 90533)
11500 W. Olympic Blvd., Ste. 550
Los Angeles, CA 90064
Tel: (310) 477-5575
Fax: (310) 477-7090
Email: wlitvak@drllaw.com

DAPEER LAW, P.A.
Rachel Dapeer, Esq.*
300 S. Biscayne Blvd., #2704
Miami FL 33131
Tel: (305) 610-5223
Email: rachel@dapeer.com

KOZONIS & KLINGER, LTD.
Gary M. Klinger *
227 W. Monroe St., Ste. 2100
Chicago, IL 60606
Tel: (312) 283-3814
Email: gklinger@kozonislaw.com
**pro hac vice planned*

Counsel For Plaintiff And Proposed Class

IN THE UNITED STATE DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

ALBERT ALMEIDA, MARK MUNOZ, and ANGELO VICTORIANO, *individually and on behalf of all others similarly situated*,

Plaintiffs,

v.

SLICKWRAPS INC., a Wyoming corporation,

Defendant.

Case No.

CLASS ACTION COMPLAINT FOR:
1. NEGLIGENCE
2. INTRUSION INTO PRIVATE AFFAIRS
3. BREACH OF EXPRESS CONTRACT
4. BREACH OF IMPLIED CONTRACT
5. NEGLIGENCE PER SE
6. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code § 17200, et seq.

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

1. Plaintiffs Albert Almeida, Mark Munoz and Angelo Victoriano, individually and on behalf of all others similarly situated, brings this class action lawsuit against Defendant SLICKWRAPS INC. ("SLICKWRAPS" or "Defendant") to obtain legal and equitable relief including damages, restitution and injunctive relief for the Classes, as defined below. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel and the facts that are a matter of public record.

NATURE OF THE ACTION

2. This case does not involve the typical data security incident. Rather, as numerous media sources have reported, SLICKWRAPS was acutely aware that it "had comically bad security, leaving it both wide open to breaches like this and flat-footed when it came to responding to any concerns brought to its attention."[1]

3. SLICKWRAPS makes and sells an assortment of premade and custom cases (known as vinyl skins) for mobile phones, tablets and other electronic devices.

4. SLICKWRAPS boasts that it is the "premier source for quality consumer electronics protection and accessories" and its products have been featured in many of the top online electronics magazines and techno blogs."

5. In addition to traditional brick and mortar retail and e-commerce platforms like www.amazon.com and www.walmart.com, SLICKWRAPS' products are available for purchase on its own website, www.slickwraps.com (the "Site").

[1] *See, e.g., Slickwraps Apologizes to Customers After Comically Bad Data Breach*, The Verge, https://www.theverge.com/2020/2/25/21153434/slickwraps-apologizes-customers-bad-data-breach (last visited March 2, 2020).

6. When accessing the Site, consumers can view SLICKWRAPS' pre-made cases, as well as upload images to the "Customizer," an online portal where they can custom design cases by uploading their own photos.[2]

7. In February 2020, SLICKWRAPS suffered a data breach which resulted in the exposure of the personally identifiable information ("PII") of approximately 858,000 customers, including names, physical addresses, phone numbers purchase histories and unique email addresses (the "Data Breach").

8. To say that SLICKWRAPS "suffered" a data breach is, to put it mildly, being charitable. SLICKWRAPS was well aware that it had lax data security measures and did absolutely nothing to prevent the very kind of cyber security incident that occurred.

9. More accurately, SLICKWRAPS' customers—who had placed their faith and trust in the company believing that it would, at the very least, utilize appropriate and necessary data security measures—suffered a wholly avoidable data breach where their PII was accessed even though SLICKWRAPS was previously informed that such access and potential exfiltration was possible. And, when called out on its woefully lax data security practices, SLICKWRAPS has done nothing but meekly apologize.

10. Specifically, on February 21, 2020, a cybersecurity analyst going by the name Lynx0x00 announced in a blog post that it had accessed the personal information of SLICKWRAPS customers.[3]

[2] *See https://www.slickwraps.com/design* (last accessed March 2, 2020).

[3] The announcement was posted, and later deleted, on the website Medium. An archived copy can be viewed here: https://archive.li/yEIJT (last accessed March 2, 2020).

11. SLICKWRAPS' phone case customization page had a vulnerability that allowed anyone to "upload any file to any location in the highest directory on their server."[4]

12. The vulnerability within the Customizer feature allowed anyone to access SLICKWRAPS' entire network, including the following information:

- 9GB of customer photos uploaded to the case customization tool
- All SLICKWRAPS admin account details, including password hashes
- All current and historical SLICKWRAPS customer billing addresses
- All current and historical SLICKWRAPS customer shipping addresses
- All current and historical SLICKWRAPS customer email addresses
- All current and historical SLICKWRAPS customer phone numbers
- All current and historical SLICKWRAPS customer transaction history and
- The company's content management system.

13. As a result of SLICKWRAPS' "blatant disregard for any semblance of operational security," would-be security thieves could readily access virtually the entire network.

14. Lynx0x00 attempted to alert SLICKWRAPS to the danger its lack of network security posed to the PII of its customers. However, SLICKWRAPS repeatedly and brazenly ignored these warnings, twice blocking Lynx0x00 for reaching out and trying to report the vulnerability.

15. It was not surprising to anyone then that a second hacker accessed the PII of SLICKWRAPS' customers. This unknown second hacker used the accessed email addresses to email 377,428 of those customers notifying them that their PII had been compromised (the "Notification Email").

4 *See id.*

16. The Notification Email, which was sent from hello@slickwraps.com, began in rather jarring fashion by informing recipients that the hacker had some of their personal information including their home address.

17. Some of those recipients (SLICKWRAPS' customers) posted the Notification Email they received to Twitter and tagged SLICKWRAPS:

//

//

//

//

//

//

//

//

//

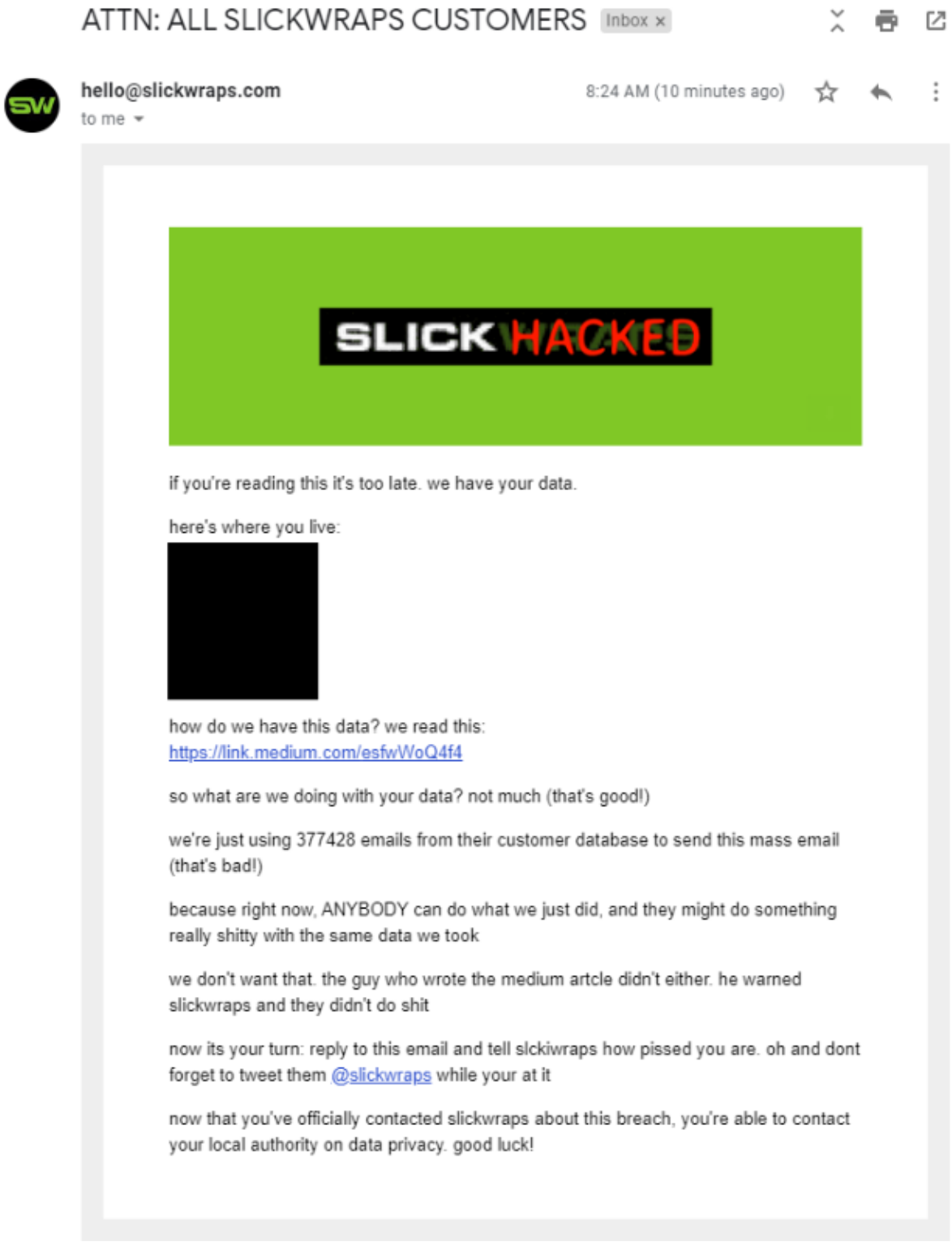
//

//

//

//

//



ATTN: ALL SLICKWRAPS CUSTOMERS Inbox ×

hello@slickwraps.com 8:24 AM (10 minutes ago)

to me

SLICK HACKED

if you're reading this it's too late. we have your data.

here's where you live:

[redacted]

how do we have this data? we read this:
https://link.medium.com/esfwWoQ4f4

so what are we doing with your data? not much (that's good!)

we're just using 377428 emails from their customer database to send this mass email (that's bad!)

because right now, ANYBODY can do what we just did, and they might do something really shitty with the same data we took

we don't want that. the guy who wrote the medium artcle didn't either. he warned slickwraps and they didn't do shit

now its your turn: reply to this email and tell slckiwraps how pissed you are. oh and dont forget to tweet them @slickwraps while your at it

now that you've officially contacted slickwraps about this breach, you're able to contact your local authority on data privacy. good luck!

18. Despite having been alerted to its security vulnerabilities almost a week earlier, SLICKWRAPS did not notify its customers that their PII had been compromised until after the Notification Email was sent on February 21, 2020.

19. Only then did SLICKWRAPS belatedly and meekly apologize by sending an apology email purportedly by the Founder and Chief Executive Officer Jonathan Endicott (the Apology Email").

20. Oddly, the Apology Email, which was sent from the same account as the Notification Email (hello@slickwraps.com) on Friday, February 21, 2020 states that it is reaching out to certain of its customers about a data security incident that occurred in the future:

> We are reaching out to you because we've made a mistake in violation of that trust. ***On February 22nd***, we discovered information in some of our non-production databases was mistakenly made public via an exploit. During this time, the databases were accessed by an unauthorized party.

21. While, SLICKWRAPS' after-the-fact apology states that "[t]here is nothing [it] value[s] higher than trust from [its] users," the truth of the matter is that SLICKWRAPS did not value or prioritize the security of its customer personal information; "[n]ot only did those victims have no idea that their confidential information was up for grabs, but the responsible party seemed to have no interest in being held accountable."[5]

22. In fact, to this day, the SLICKWRAPS' Site, which is accessible to consumers world-wide and within the State of California, does *not* have a privacy policy of any kind. *See* https://www.slickwraps.com/ (last visited March 2, 2020).

5 *I hacked Slickwraps. This is how*., https://archive.is/yEIJT (last visited March 2, 2020).

23. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address SLICKWRAPS' grossly inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party as well as a failure to be truthful and candid regarding precisely what specific types of information were accessed.

24. Plaintiffs assert claims for: (i) negligence, (ii) intrusion into private affairs, (iii) negligence *per se*, (iv) breach of express contract, (v) breach of implied contract, and (vi) deprivation of rights possessed under the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200) and California Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq*.).

25. Plaintiffs seek legal and equitable remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs and injunctive relief including improvements to Defendant's data security systems, future annual audits and adequate credit monitoring services funded by Defendant.

PARTIES

26. Plaintiff Albert Almeida is, and at all times mentioned herein was, an individual citizen of the State of California residing in the City of Vallejo (Solano County).

27. Plaintiff Mark Munoz is, and at all times mentioned herein was, an individual citizen of the State of California residing in Rancho Cucamonga (San Bernardino County

28. Plaintiff Angelo Victoriano is, and at all times mentioned herein was, an individual citizen of the State of California residing in the City of Los Angeles (Los Angeles County).

29. Plaintiffs suffered actual injuries from having their PII compromised and stolen as a result of the Data Breach including, but not limited to: (i) paying monies to SLICKWRAPS for

its goods and services which they would not have had if SLICKWRAPS truthfully and adequately disclosed that it lacked data security practices and capabilities necessary to safeguard consumers' PII from theft; (ii) damages to and diminution in the value of their PII—a form of intangible property that the Plaintiffs entrusted to SLICKWRAPS; (iii) loss of their privacy and (iv) imminent and impending injury arising from the increased risk of fraud and identity theft. As a result of the Data Breach, Plaintiff and the Class Members will continue to be at heightened risk for financial fraud and identity theft, and their attendant damages, for years to come.

30. Defendant SLICKWRAPS INC. is a corporation organized under the laws of Wyoming and headquartered in Kansas at 355 N. Mosley Street, Wichita, Kansas 67202.

31. SLICKWRAPS' registered agent is BD REGISTERED AGENT, INC., 301 Main Street, Suite 600, Wichita, Kansas 67202.

JURISDICTION & VENUE

32. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are at least 857,000 putative class members, many of whom have different citizenship from SLICKWRAPS (including the named Plaintiffs here).

33. This Court has personal jurisdiction over Defendant SLICKWRAPS for at least the following reasons: (i) Defendant regularly does business or solicits business, engages in other persistent courses of conduct and/or derives substantial revenue from products and/or services provided to individuals in this District and in this State (ii) and Defendant has purposefully established substantial, systematic and continuous contacts with this District and expects or should reasonably expect to be hauled into court here. Thus, Defendant SLICKWRAPS has sufficient

minimum contacts with this District, and this Court's exercise of jurisdiction over Defendant will not offend traditional notions of fair play and substantial justice.

34. Through its business operations in this District, SLICKWRAPS intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

35. Venue is proper in this District under 28 U.S.C. § 1391 because Defendant does business in this District and Defendant is subject to personal jurisdiction in this District.

FACTS COMMON TO ALL CLASS MEMBERS

A. *The SLICKWRAPS' Data Breach.*

36. The SLICKWRAPS Data Breach was a direct result of its abject failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect customer PII.

37. The data consisted of a treasure trove of SLICKWRAPS customers' PII including names, addresses, email addresses, telephone numbers, transaction history and passwords.

38. SLICKWRAPS discovered that their consumers PII had been accessed on February 21, 2020.

39. In a post to the website Medium, an online publishing platform, a security researcher, posting under the name Lynx0x00, stated that in "January 2020 he was able to gain full access to the Slickwraps' web site using a path traversal vulnerability in an upload script for case customizations."[6]

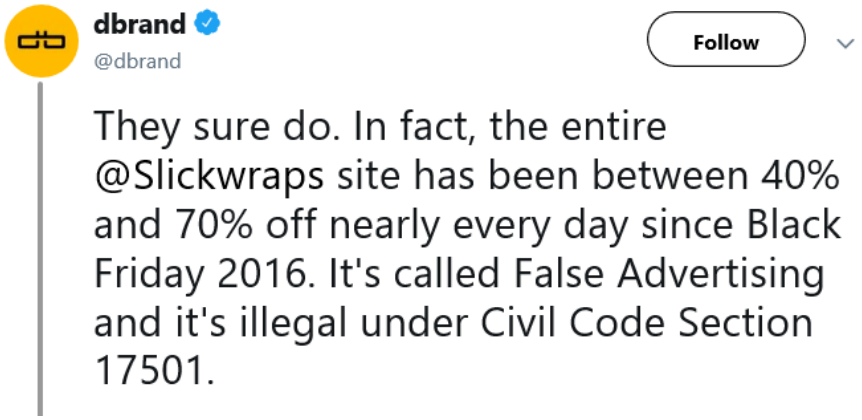
6 *See Slickwraps Data Breach Exposes Financial and Customer Info, February 21, 2020*, available at https://www.bleepingcomputer.com/news/security/slickwraps-data-breach-exposes-financial-and-customer-info/ (last visited March 2, 2020).

40. Lynx0x00 was initially made aware of its security vulnerabilities by accessing publicly-available information on the internet and with this information was able to access the entirety of SLICKWRAPS' network.[7]

41. In order to prevent SLICKWRAPS from denying that its system and customers' PII had been accessed, the post began by revealing that in June of 2019, Slickwraps, "sold precisely 10,744 orders through their eCommerce platform. They collected $199,128.51 USD in revenue. They accepted $1,314.80 USD in refunds. They authorized 560 returns."

42. Lynx0x00 noted that it had this data "because I am a cybersecurity analyst… and SlickWraps has *abysmal cybersecurity*."

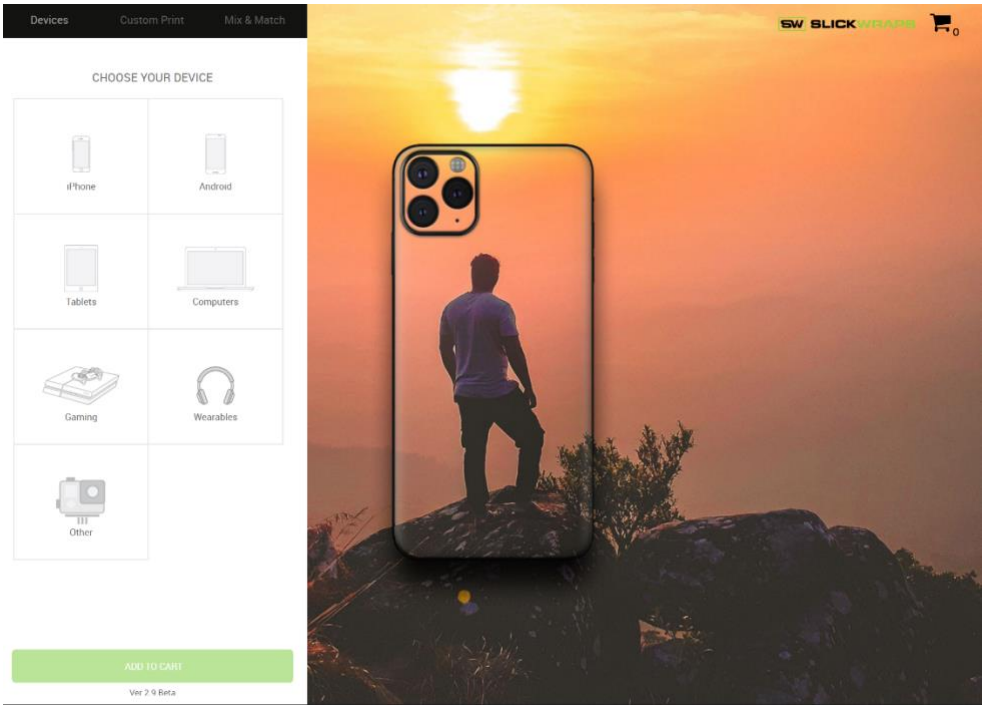
43. The author discovered SLICKWRAPS' security vulnerabilities while it was investigating allegations that SLICKWRAPS engaged in deceptive false advertising of their prices and never-ending sales. Specifically, SLICKWRAPS is alleged to mislead consumers into believing its products are on sale but the discount is taken off of an inflated price.



[7] *See, e.g.*, *I hacked Slickwraps. This is how.*, https://archive.is/yEIJT (last visited March 2, 2020 (detailing Slickwraps' woefully lax data security measures).

44. According to Lynx0x00, when he discovered the "abysmal cybersecurity," SLICKWRAPS was notified "multiple times of their egregious security vulnerabilities which (still) exist on their Magento-based eCommerce platform" and that "Slickwraps simply blocked and ignored [him]."[8]

45. The root of the vulnerabilities stem from SLICKWRAPS' Customizer feature (by which customers could upload photos for custom-made vinyl skins):



46. The Customizer page contained an inexcusable vulnerability in that "anyone with the right toolkit could upload any file to any location in the highest directory on their server (*i.e.* the "web root")."[9]

8 https://archive.li/yEIJT#selection-223.0-275.94. (last visited March 2, 2020).

9 *See Slickwraps Data Breach Exposes Financial and Customer Info*, February 21, 2020, available at https://www.bleepingcomputer.com/news/security/slickwraps-data-breach-exposes-financial-and-customer-info/ (last visited March 2, 2020).

47. The hackers were able to access SLICKWRAPS' *entire 17GB MySQL database*. Or, put another way, using a so-called "remote code execution attack," exfiltrators were able to access a veritable treasure trove of consumer data.[10]

48. Lynx0x00 noted that it had contacted SLICKWRAPS via Twitter, on or about February 15, 2020 and informed SLICKWRAPS of the security vulnerabilities and implored it to report the data security vulnerabilities and breach:

//

//

//

//

//

//

//

//

//

//

//

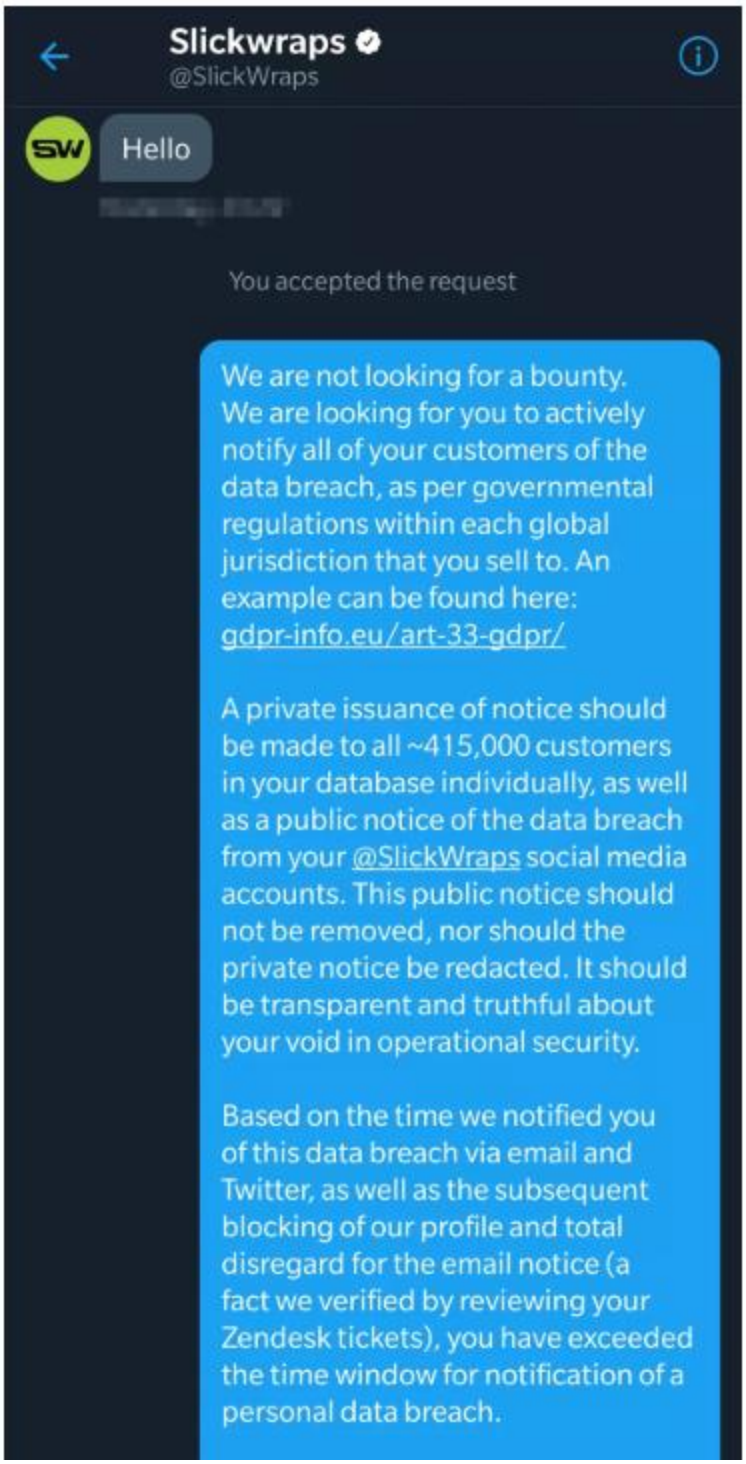
//

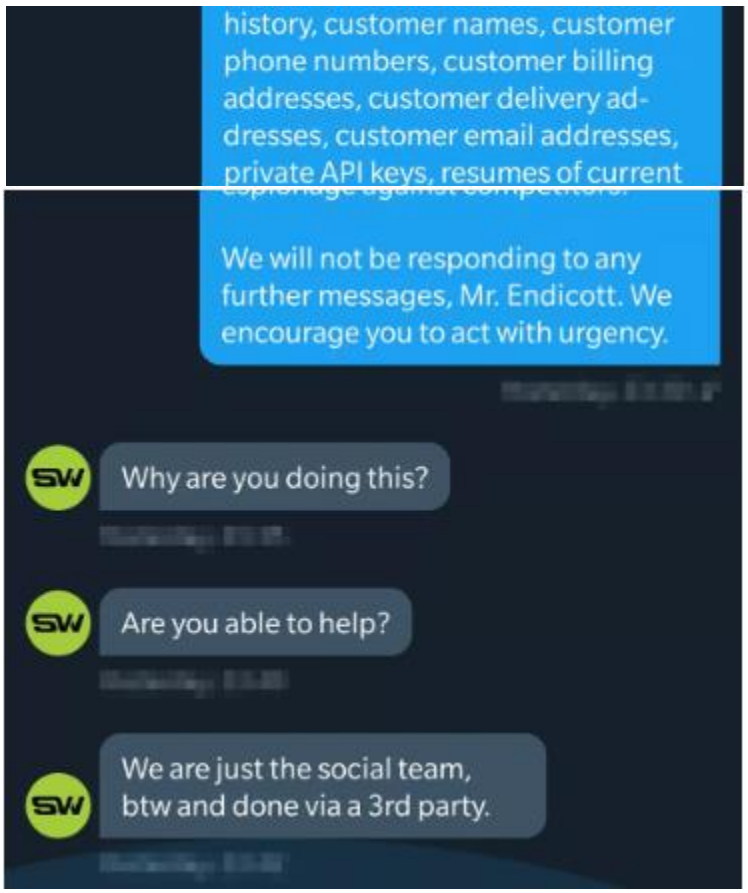
//

//

//

[10] *See id.*


Slickwraps
@SlickWraps
SW
Hello
You accepted the request
We are not looking for a bounty. We are looking for you to actively notify all of your customers of the data breach, as per governmental regulations within each global jurisdiction that you sell to. An example can be found here: gdpr-info.eu/art-33-gdpr/
A private issuance of notice should be made to all ~415,000 customers in your database individually, as well as a public notice of the data breach from your @SlickWraps social media accounts. This public notice should not be removed, nor should the private notice be redacted. It should be transparent and truthful about your void in operational security.
Based on the time we notified you of this data breach via email and Twitter, as well as the subsequent blocking of our profile and total disregard for the email notice (a fact we verified by reviewing your Zendesk tickets), you have exceeded the time window for notification of a personal data breach.



49. In addition to this exchange with SLICKWRAPS, Lynx0x00 also directly emailed SLICKWRAPS' CEO Jonathan Endicott to make sure that he was personally aware of the issues with the company's security vulnerabilities (anticipating the company's retort that its Twitter account was monitored by a third-party).

50. Rather than disclose the breach of its computer network to its customers, Slickwraps merely "blocked" Lynx0x00 on Twitter so that it could no longer send it direct messages.[11]

11 *See Slickwraps Data Breach Exposes Financial and Customer Info*, February 21, 2020, available at https://www.bleepingcomputer.com/news/security/slickwraps-data-breach-exposes-financial-and-customer-info/ (last visited March 2, 2020) (stating that "[t]his one was different in

51. SLICKWRAPS finally come forward—because it had no other choice—only *after* an anonymous hacker gained "complete control of the database" and sent the Notification Email to some of the firm's customers."[12]

52. The Notification Email was sent to 377,428 SLICKWRAPS' consumers. Those consumers' email addresses pulled from the company's records and the email was sent from a corporate email address, hello@slickwraps.com, proving that the hacker had access to virtually all of SLICKWRAPS' system.

//

//

//

//

//

//

//

//

//

//

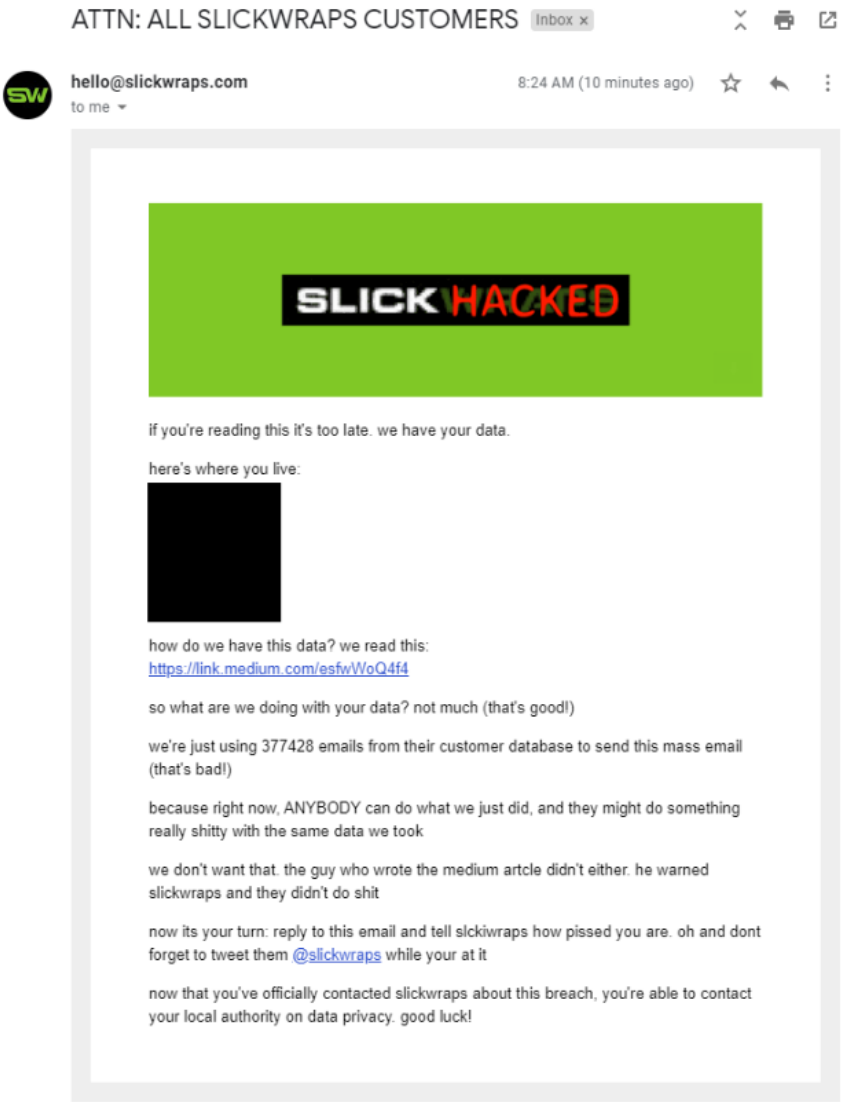
//

//

that sense that they blocked me and did not care about their customers at all. Since this is a major breach, and I exhausted all my other options to contact them, I felt the need to disclose this publicly, in hope that they fix this asap").

12 *See Slickwraps Breach Hits 857,000 Customers*, InfoSecurity Magazine https://www.infosecurity-magazine.com/news/slickwraps-breach-hits-857000/ (last visited March 2, 2020).

53. Some affected users shared the email message on Twitter:



54. According to the breach notification site https://haveibeenpwned.com/, 857,611 unique customer accounts were compromised in the breach.

B. *SLICKWRAPS' "Response."*

55. Despite knowing about the Data Breach for several days, SLICKWRAPS made the conscious and deliberate decision to ***not*** inform the public and only came forward when it feared its inaction would be disclosed to the public.

56. Specifically, Lynx0x00 warned SLICKWRAPS about its security vulnerabilities on or about February 16, 2020. In fact, Lynx0x00 "has stated and showed screenshots of attempts to contact both Endicott via email and Slickwraps on Twitter prior to [that day]."[13]

57. But SLICKWRAPS did not notify its own consumers about the security brief until February 21, 2020 - almost a week later. After the Notification Email went out and customers became aware of the breach, SLICKWRAPS finally commented on the situation.

58. Specifically, on February 21, 2020, SLICKWRAPS' Chief Executive Officer Jonathan Endicott sent an email (from the same hello@slickwraps.com account) informing recipients that the Company had suffered a data security breach and that certain of their information was compromised.

59. Upon information and belief, the Apology Email as well as some video posting on Twitter are the only public statements regarding the Data Breach.

60. Notably, there is absolutely no information on the home page of SLICKWRAPS' website that the Data Breach occurred, where potentially affected persons can go to information or any other information.[14]

61. In sending the Apology Email, SLICKWRAPS misled the public by stating that it had not become aware that their customers' PII had been accessed until that day (in fact, in the original iteration of the Apology Email, Endicott stated that SLICKWRAPS become aware one day in the future, February 22, 2020).

[13] *See Slickwraps Breach Hits 857,000 Customers*, InfoSecurity Magazine https://www.infosecurity-magazine.com/news/slickwraps-breach-hits-857000/ (last visited March 2, 2020).

[14] The Apology Email was posted on SLICKWRAPS' blog, which is accessible here https://www.slickwraps.com/blog/update/.

62. Regrettably, many statements in the Apology Email contained many falsehoods or the following highlighted portions of SLICKWRAPS blogpost are seemingly not accurate or are otherwise misleading:

> Slickwraps Family,
>
> There is nothing we value higher than trust from our users. In fact, our entire business model is dependent on building long-term trust with customers that keep coming back.
>
> We are reaching out to you because we've made a mistake in violation of that trust.
>
> On February 21st, we discovered customer data in some of our non-production databases was mistakenly made public via an exploit. During this time, the databases were accessed by an unauthorized party.
>
> The information did not contain passwords or personal financial data.
>
> The information did contain names, user emails, addresses If you ever checked out as "GUEST" none of your information was compromised.
>
> Upon finding out about the public user data, we took immediate action to secure it by closing any databases in question.
>
> As an additional security measure, we recommend that you reset your Slickwraps account password. Again, no passwords were compromised, but we recommend this as a standard safety measure. Finally, please be watchful for any phishing attempts.
>
> We are deeply sorry for this oversight. We promise to learn from this mistake and will make improvements going forward. This will include enhancing our security processes, improving communication of security guidelines to all Slickwraps employees, and making more of our user-requested security features our top priority in the coming months. We are also partnering with a third-party cybersecurity firm to audit and improve our security protocols.

Timeline of Events

Contacted by an individual claiming to have access to customer data via a Twitter post. These posts were not immediately seen and once seen, contact was made with the individual by our social team.

After receiving said message, contact was made to Troy Hunt @troyhunt on February 20th, 2020, to verify the users' authenticity.

February 20th, 2020 - FBI were notified of the possible threat, and our security team began looking into a potential breach.
February 21st, 2020 - The attacker has emailed customers connected to the breach. Has publicly stated no data was stored and all deleted.

February 21st, 2020 - FBI has opened an investigation with DA approval.

February 21st, 2020 - The exploit was repaired and all data is secured. We are currently working with a 3rd party cybersecurity team for continued analysis.

More details will follow, and we appreciate your patience during this process.
Sincerely,
Jonathan Endicott
CEO @ Slickwraps

63. SLICKWRAPS said customer data in some of the company's non-production databases was "mistakenly made public via an exploit" and that those databases were accessed by an unauthorized party."

64. SLICKWRAPS admitted that the accessed information includes names, emails and addresses.

65. Although Mr. Endicott stated "if you have ever checked out as a guest, none of your personal information was compromised" that contention seems suspect, at best, as several consumers who checked out as guests received the breach email.[15]

66. Internet security specialists recognize that the PII compromised in the Data Breach presents "a treasure trove" of contact details on customers, many of whom will now "face a higher risk of receiving spear-phishing emails, and being SIM swapped."

C. *SLICKWRAPS Acquires, Collects & Stores Plaintiffs' & Class Members' PII.*

67. SLICKWRAPS acquires, collects and stores a massive amount of PII on its customers.

68. By obtaining, collecting, using and deriving a benefit from Plaintiffs' and Class Members' PII, SLICKWRAPS assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

69. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

70. Plaintiffs and the Class Members reasonably and appropriately relied on SLICKWRAPS to keep their PII confidential and securely maintained, to use this information for business purposes only and to make only authorized disclosures of this information.

D. *The Value of Personally Identifiable Information & the Effects of Unauthorized Disclosure.*

71. SLICKWRAPS was well-aware that the PII it collects is highly sensitive, and of significant value to those who would use it for wrongful purposes.

[15] *See* https://latesthackingnews.com/2020/02/25/slickwraps-website-breached-after-disgruntled-researcher-publicly-exposed-findings/. ("I always checked out as a guest, have no account. Still I got TWO emails from the hackers. Your negligence is criminal.").

72. Personally identifiable information is a valuable commodity to identity thieves. As the FTC recognizes, with PII identity thieves can commit an array of crimes including identify theft, medical and financial fraud.[16] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites.

73. The ramifications of SLICKWRAP's failure to keep its customers' PII secure are long lasting and severe. Once PII is stolen, improper and/or fraudulent use of that information and damage to victims may continue for years.

74. At all relevant times, SLICKWRAPS knew or reasonably should have known of the importance of safeguarding PII and of the foreseeable consequences if its data security systems were breached, including, the significant costs that would be imposed on customers as a result.

75. Defendant unequivocally and materially breached obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard the SLICKWRAPS' computer systems and data.

76. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect consumers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions and

[16] Federal Trade Commission, *Warning Signs of Identity Theft,* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited March 2, 2020).

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures.

E. *SLICKWRAPS Fails to Comply with FTC Guidelines.*

77. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[17]

78. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.[18]

79. Those guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities and implement policies to correct any security problems.

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

81. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords

[17] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf. (last visited March 2 , 2020).

[18] https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited March 2 , 2020).

to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network and verify that third-party service providers have implemented reasonable security measures.[19]

82. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

83. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

84. SLICKWRAP's failure to employ reasonable and appropriate measures to protect against unauthorized access to customer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

85. SLICKWRAPS was at all times fully aware of its obligation to protect the PII of customers. SLICKWRAPS was also aware of the significant repercussions that would result from its failure to do so.

F. *SLICKWRAPS Fails to Comply with Industry Standards.*

86. Cyber security firms have promulgated a series of best practices that, a minimum, should be implemented by e-commerce platforms like SLICKWRAPS, including, but not limited to, installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as

[19] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf. (last visited March 2 , 2020).

firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system not to mention training staff regarding these critical points.

G. *Plaintiff & Class Members Suffered Damages.*

87. Defendant SLICKWRAPS maintained its customers' PII in a wantonly reckless manner. In particular, the PII was maintained on Defendant SLICKWRAPS' computer network in a condition extremely vulnerable to cyberattacks.

88. Upon information and belief, the mechanism of the cyberattack and the improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus it was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

89. Defendant disregarded the rights of Plaintiffs and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard customer PII; failing to take standard and reasonably available steps to prevent the Data Breach and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

90. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII that SLICKWRAPS collected and maintained is now in the hands of numerous unknown third-parties, including potentially would-be data thieves.

91. To date, SLICKWRAPS has offered nothing to affected class members other than a belated, half-hearted Apology Email and a similar video posted on Twitter.

92. Victims of data breaches and other unauthorized disclosures commonly face multiple years of potential ongoing identity theft and SLICKWRAPS' response entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII.

93. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate and continuing increased risk of harm from fraud and identity theft.

94. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

95. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud and similar identity theft.

96. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

97. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees and similar costs directly or indirectly related to the Data Breach.

98. Plaintiffs and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in similar cases.

99. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied

by adequate data security but clearly was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant SLICKWRAPS' computer property and Plaintiffs' and Class Members' PII. Thus, Plaintiffs and the Class Members did not get what they paid for.

100. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

101. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

102. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

103. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their PII—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

104. Plaintiffs and the Class Members were also injured in that they were deprived of rights they possess under the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200) and California Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq*.) to keep their PII secure and confidential.

105. What's more, Defendant's delay in identifying and reporting the Data Breach caused additional harm. It is axiomatic that "[t]he quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit

the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[20]

106. Indeed, once a data breach has occurred, "[o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves" (internal citations omitted).[21]

107. The ramifications of SLICKWRAP's failure to keep Customers' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.

108. The PII belonging to Plaintiffs and Class Members is private, sensitive in nature and was left inadequately protected by Defendant who did not obtain Plaintiffs' or Class Members' consent to disclose such PII to any other person as required by applicable law and industry standards.

109. The Data Breach was a direct and proximate result of SLICKWRAP's failure to: (a) properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access,

20 *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent Accordingto New Javelin Strategy & Research Study*, Business Wire, https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million. (last visited March 2, 2020).

21 Consumer Reports, *The Data Breach Next Door Security breaches dont just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too*, January 31, 2019, https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last visited March 2, 2020).

use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

110. Defendant had the resources necessary to prevent the Breach, but neglected to adequately invest in data security measures, despite its obligation to protect customer data.

111. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into their systems and, ultimately, the theft of its customers' PII.

112. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[22]

113. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GOA Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[23]

114. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone

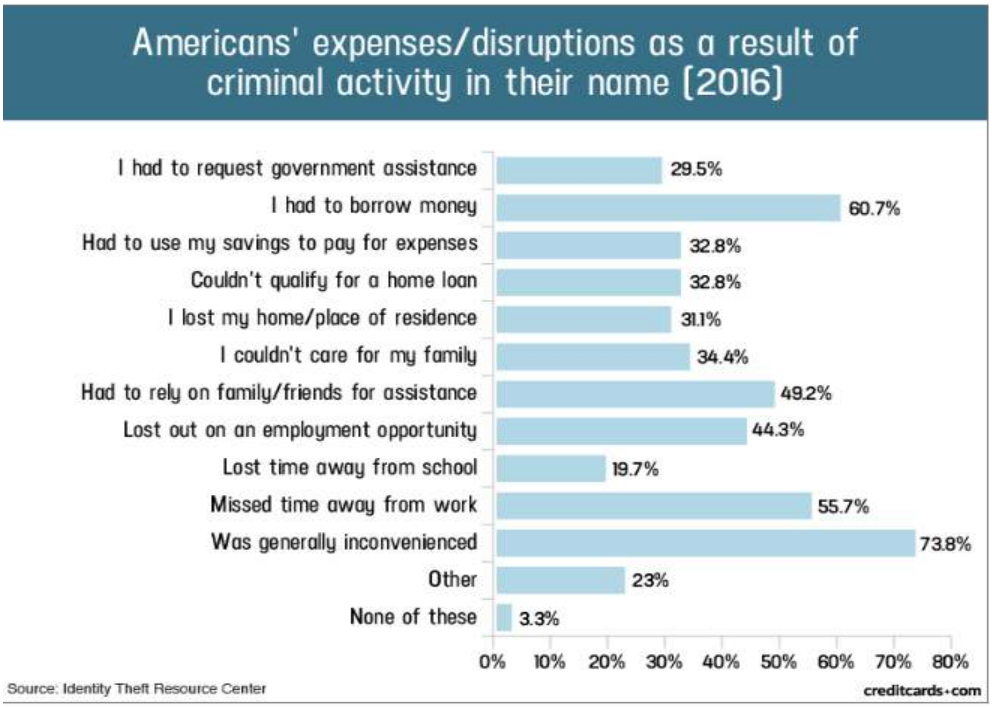
22 U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013 available at https://www.bjs.gov/content/pub/pdf/vit12.pdf

23 *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 (last visited March 2, 2020) ("GAO Report").

steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[24]

115. Identity thieves use stolen personal information numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

116. Identity thieves can also PII to obtain a driver's license or official identification card in the victim's name but with the thief's picture; obtain government benefits or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job



using the victim's PII, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[25]

24 *See* https://www.identitytheft.gov/Steps (last visited March 2, 2020).

25 "*Credit Card and ID Theft Statistics*" by Jason Steele, 10/24/2017, at:

117. PII and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

118. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts for many years to come.

Factual Allegations of Representative Plaintiff Almeida

119. On or about October 28, 2016, Plaintiff Almeida created an account with SLICKWRAPS.com.

120. In order to create his account, Plaintiff Almeida provided to SLICKWRAPS certain of his PII, including his name, address and email address.

121. Plaintiff Almeida created a username and password for his SLICKWRAPS' account, information which was also shared with and stored by SLICKWRAPS.

122. Plaintiff Almeida received an email from SLICKWRAPS on or about October 28, 2016 confirming the creation of his account.

123. On February 21, 2020, Plaintiff Almeida received the Notification Email, an email purporting to be from SLICKWRAPS using the hello@slickwraps.com.

https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited March 2, 2020).

124. The Notification Email informed Plaintiff Almeida that if he was reading the email, it was "too late" because they already "have [his] data." The email then went on to identify to Plaintiff Almeida his home address, information which he had previously provided to SLICKWRAPS during the account formation process.

125. The sender of the Notification Email noted that the reason that they were sending the email was "because right now, ANYBODY can do what we just did, and they might do something really shitty with the same data we took."

126. Plaintiff Almeida also received the Apology Email from SLICKWRAPS.

127. When Plaintiff Almeida's email address is entered into the breach notification site https://haveibeenpwned.com/, it confirms that his email address was compromised during the SLICKWRAPS Data Breach.

Factual Allegations of Representative Plaintiff Munoz

128. On or about July 4, 2016, Plaintiff Munoz created an account with SLICKWRAPS.com.

129. In order to create his account, Plaintiff Munoz provided to SLICKWRAPS certain of his PII, including his name, address and email address.

130. Plaintiff Munoz created a username and password for his SLICKWRAPS' account, information which was also shared with and stored by SLICKWRAPS.

131. On February 21, 2020, Plaintiff Munoz received the Apology Email from SLICKWRAPS.

132. When Plaintiff Munoz's email address is entered into the breach notification site https://haveibeenpwned.com/, it confirms that his email address was compromised during the SLICKWRAPS Data Breach.

Factual Allegations of Representative Plaintiff Victoriano

133. On or about March 27, 2019, Plaintiff Victoriano created an account with SLICKWRAPS.com.

134. In order to create his account, Plaintiff Victoriano shared with SLICKWRAPS certain of his PII, including his name, address and email address.

135. Plaintiff Victoriano created a username and password for his account, which was also shared with SLICKWRAPS.

136. Plaintiff Victoriano received an email from SLICKWRAPS on March 27, 2019 confirming the creation of his account and asking him to change his password.

137. That same day, Plaintiff Victoriano purchased two iPhone cases to be delivered to his home address. A confirmation email was sent to his email address.

138. On July 26, 2019, Plaintiff Victoriano made another purchase with SLICKWRAPS, ordering three iPhone skins to be delivered to his home address. A confirmation email was sent to his email address that same day.

139. On February 21, 2020, Plaintiff Victoriano received the Notification Email, an email purporting to be from SLICKWRAPS using the hello@slickwraps.com.

140. The Notification Email informed Plaintiff Victoriano that if he was reading the email, it was "too late" because they already "have [his] data." The email then went on to identify to Plaintiff Victoriano his home address, information which he had previously provided to SLICKWRAPS during the account formation process.

141. The sender of the Notification Email noted that the reason that they were sending the email was "because right now, ANYBODY can do what we just did, and they might do something really shitty with the same data we took."

142. Plaintiff Victoriano also received the Apology Email from SLICKWRAPS.

143. When Plaintiff Victoriano's email address is entered into the breach notification site https://haveibeenpwned.com/, it confirms that his email address was compromised during the SLICKWRAPS Data Breach.

144. Both Plaintiffs Almeida and Victoriano had their PII compromised and made public as a direct and approximate result of SLICKWRAPS conduct.

CLASS ACTION ALLEGATIONS

145. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated.

146. Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

> **National Class**: All persons whose PII was compromised as a result of the Data Breach announced by SLICKWRAPS on or about February 21, 2020.
>
> **California Subclass:** All persons residing in the State of California whose PII was compromised as a result of the Data Breach announced by SLICKWRAPS on or about February 21, 2020.

147. Excluded from the Classes are Defendant's officers, directors and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Classes are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

148. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

149. The proposed Classes meet the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

150. **Numerosity.** The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of approximately 857,611 customers of Defendant SLICKWRAPS whose data was compromised in the Data Breach.

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

- Whether Defendant unlawfully used, maintained, lost or disclosed Plaintiffs' and Class Members' PII;
- Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- Whether Defendant owed a duty to Class Members to safeguard their PII;
- Whether Defendant breached its duty to Class Members to safeguard their PII;
- Whether computer hackers obtained Class Members' PII in the Data Breach;
- Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

- Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- Whether Defendant's conduct was negligent;
- Whether Defendant's conduct was *per se* negligent;
- Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;
- Whether Defendant violated the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200 *et seq*.);
- Whether Defendant failed to provide notice of the Data Breach in a timely manner and
- Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

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

153. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Classes. Plaintiffs' Counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

154. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

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

156. Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief and corresponding declaratory relief are appropriate on a class-wide basis.

157. 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:

- Whether SLICKWRAPS failed to timely notify the public of the Data Breach;
- Whether SLICKWRAPS owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing and safeguarding their PII;
- Whether SLICKWRAPS' security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

- Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- Whether Defendant failed to take commercially reasonable steps to safeguard customer PII and
- Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

158. Finally, all members of the proposed Classes are readily ascertainable. SLICKWRAPS has access to customer names and addresses affected by the Data Breach. Using this information, Class Members can be identified and ascertained for the purpose of providing notice.

CAUSES OF ACTION

FIRST COUNT

NEGLIGENCE

(On Behalf of Plaintiffs & National Class Members)

159. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

160. Defendant required Plaintiffs and Class Members to submit non-public PII in order to obtain services.

161. Plaintiffs and the Class Members entrusted their PII to SLICKWRAPS with the expectation, belief and understanding that SLICKWRAPS would safeguard their information.

162. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

163. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft.

164. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

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

166. In addition, Cal. Civ. Code §1798.81.5 requires Defendant to take reasonable steps and employ reasonable methods of safeguarding the PII of Class Members who are California residents.

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

168. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII.

169. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

- Failing to adequately monitor the security of their networks and systems;
- Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- Allowing unauthorized access to Class Members' PII;
- Failing to detect in a timely manner that Class Members' PII had been compromised and
- Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

170. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members.

171. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the world today.

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

173. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII and the harm suffered, or risk of imminent harm suffered by Plaintiff and the Class.

174. As a result of Defendant's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to, out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

175. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach

176. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT

INTRUSION INTO PRIVATE AFFAIRS/INVASION OF PRIVACY

(On Behalf of Plaintiffs & National Class Members)

177. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

178. California established the right to privacy in Article I, Section 1 of the California Constitution.

179. The State of California recognizes the tort of Intrusion into Private Affairs, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

180. Other States similarly recognize the tort of intrusion upon seclusion.

181. Plaintiffs and Class Members had a reasonable expectation of privacy in the PII Defendant failed to protect.

182. Defendant's conduct as alleged above intruded upon Plaintiffs' and Class Members' seclusion under common law.

183. By intentionally failing to keep Plaintiffs' and Class Members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs' and Class Members' privacy by:

- Intentionally and substantially intruding into Plaintiffs' and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person and
- Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person and
- Intentionally causing anguish or suffering to Plaintiffs and Class Members.

184. Defendant knew that an ordinary person in Plaintiffs' or a Class Member's position would consider Defendant's intentional actions highly offensive and objectionable.

185. Defendant invaded Plaintiffs and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

186. Defendant intentionally concealed from Plaintiffs and Class Members an incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

187. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendant's conduct, amounting to a substantial and serious invasion of Plaintiffs' and Class Members' protected privacy interests causing anguish and suffering such that an ordinary

person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

188. In failing to protect Plaintiffs' and Class Members' PII, and in intentionally misusing and/or disclosing their PII, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private. Plaintiffs, therefore, seeks an award of damages on behalf of themselves and the Class.

THIRD COUNT

Breach of Implied Contract

(On Behalf of Plaintiffs & National Class Members)

189. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

190. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of their use of Defendant's services.

191. Plaintiff and Class Members paid money to Defendant in exchange for services, along with Defendant's promise to protect their PII from unauthorized disclosure.

192. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses and (f) retain the PII only under conditions that kept such information secure and confidential.

193. When Plaintiffs and Class Members provided their PII to Defendant SLICKWRAPS in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

194. Defendant solicited and invited Class Members to provide their PII as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

195. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

196. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

197. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

198. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

199. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

200. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

201. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

202. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures and (iii) immediately provide adequate credit monitoring to all Class Members.

FOURTH COUNT

Negligence *Per Se*

(On Behalf of Plaintiffs & National Class Members)

203. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

204. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

205. 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 SLICKWRAPS, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

206. SLICKWRAPS violated Section 5 of the FTC Act by failing to use reasonable measures to protect customer PII and not complying with applicable industry standards, as described in detail herein. SLICKWRAPS' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

207. SLICKWRAPS' violation of Section 5 of the FTC Act constitutes negligence *per se* as SLICKWRAPS' violation of the FTC Act establishes the duty and breach elements of negligence.

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

209. The harm that occurred as a result of the Data 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.

210. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendant had a duty to protect the security and confidentiality of Plaintiff's and Class Members' Private Information.

211. Defendant breached its duties to Plaintiff and Class Members under the Gramm-Leach-Bliley Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

212. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

213. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

214. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class

Members to experience the foreseeable harms associated with the exposure of their Private Information.

215. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

FIFTH COUNT

Violation of the California Unfair Competition Law

Cal Bus. & Prof. Code § 17200, *et seq*.

(On Behalf of Plaintiff & California Sub-Class Members)

216. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

217. The California Unfair Competition Law, Cal Bus. & Prof. Code § 17200, *et seq*., prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

218. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

219. In the course of conducting its business, Defendant committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' PII, and violating the statutory and common law alleged herein in the process, including, *inter alia*, the California CRA, the California CCPA, the Federal Trade Commission

Act, and the Gramm- Leach-Bliley Act. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

220. Defendant also violated the UCL by failing to timely notify Plaintiffs and Class Members regarding the unauthorized release and disclosure of their PII. If Plaintiffs and Class Members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII and identities.

221. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends public policy, and is immoral, unethical, oppressive, and unscrupulous. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

222. The UCL also prohibits any "fraudulent" business act or practice, above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

223. By the acts and conduct alleged herein, Defendant committed fraudulent acts and practices by:

- failure to maintain adequate computer systems and data security practices to safeguard PII;

- failure to maintain a privacy policy and inform consumers what Defendant does with their PII;
- failure to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft;
- continued gathering and storage of PII, and other personal information after Defendant knew or should have known of the security vulnerabilities of its computer systems that were exploited in the Data Breach;
- making and using false promises, set out in the SLICKWRAPS Privacy Policies, about the privacy and security of PII and the Private Information of Plaintiffs and Class Members, and;
- continued gathering and storage of PII and other personal information after Defendant knew or should have known of the Data Breach and before Defendant allegedly remediated the data security incident.

224. Defendant's business practices, as alleged herein, constitute fraudulent conduct because they were likely to deceive, and did deceive, Plaintiff and Class Members into purchasing Defendant's services when those services were misrepresented and otherwise did not perform as advertised as to the confidentiality, safety, and security of PII.

225. The foregoing fraudulent acts and practices are deceptive and misleading in a material way because they fundamentally misrepresent the character of the services provided, specifically as to the safety and security of PII and other personal and private information, to induce consumers to purchase the same.

226. Defendant's unconscionable commercial practices, false promises, misrepresentations, and omissions set forth in this Complaint are material in that they relate to

matters which reasonable consumers, including Plaintiffs and Members of the Class, would attach importance to in making their purchasing decisions or conducting themselves regarding the purchase of services from Defendant.

227. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the UCL, Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which she is entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of her PII, (iv) deprivation of the value of their PII, for which there is a well-established national and international market, and/or (v) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

228. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves, Class Members, and the general public, also seek restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Cal. Bus. & Prof. Code § 17203.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and the class the seek to represent, pray for judgment as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiffs and their counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e. Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded and

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

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: March 13, 2020 Respectfully submitted,

By: */s/ William Litvak*

William Litvak (SBN 90533)
DAPEER ROSENBLIT LITVAK, LLP
wlitvak@drllaw.com
11500 W. Olympic Blvd. Ste. 550.
Los Angeles, California 90064

Rachel Dapeer, Esq.*
DAPEER LAW, P.A.
rachel@dapeer.com
300 S Biscayne Blvd, #2704, Miami, FL 33131

Gary M. Klinger*
KOZONIS & KLINGER, LTD
gklinger@kozonislaw.com
227 W. Monroe Street, Suite 2100, Chicago, IL 60630

*Attorneys for Plaintiffs - *pro hac vice to be filed*