Joshua B. Swigart, SBN 225557
josh@swigartlawgroup.com
Jayson B. Swigart, SBN 338498
jayson@swigartlawgroup.com
SWIGART LAW GROUP, APC
2221 Camino Del Rio S., Suite 308
San Diego, CA 92108
Tel: (866) 219-3343; Fax: (866) 219-8344

Counsel for Plaintiff Foster, and the Putative Class

SUPERIOR COURT OF THE STATE OF CALIFORIA
COUNTY OF SAN DIEGO

ROBIN FOSTER, individually and on behalf of all others similarly situated,

Plaintiff,

v.

LEO HAMEL FINE JEWELERS, INC.,

Defendant.

Case No. 37-2023-00019871-CU-MC-CTL

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

COMPLEX

Plaintiff ROBIN HAMEL ("Plaintiff") bring this Class Action Complaint against LEO HAMEL FINE JEWELERS, INC. ("Defendant") in their individual capacities and on behalf of all others similarly situated (the "Class," defined below), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Defendant Leo Hamel Fine Jewelers, Inc. is a retailer with multiple locations of fine jewelry, including rings earrings, bracelets, necklaces and watches.

2. A part of Defendant's business involves collecting and storing confidential employee information.

3. Under California law, including California common law, the California Unfair Competition Law, ("UCL"), Plaintiff and all other persons similarly situated had a right to keep their Personal Identifying Information ("PII") provided to Defendant confidential (PII collectively "Sensitive Information"). Plaintiff and other members of the Class relied on Defendant to keep their sensitive PII confidential as required by the applicable laws.

4. Defendant violated this right. It failed to implement or follow reasonable data security procedures as required by law and failed to protect Plaintiff and the proposed Class Employees' Sensitive Information from unauthorized access.

5. As a result of Defendant's inadequate data security and inadequate or negligent training of its employees, on or around November 10, 2022, Defendant was alerted to suspicious activity on Defendant's computer network which took place on November 6, 2022. Plaintiff and Class Employees' Sensitive Information was accessed and viewed by unauthorized and unknown persons through Defendant's employee email accounts. On or about Marsh 24, 2023, Defendant confirmed which individuals sensitive information was within the impacted files.

6. On information and belief, on or around August 28, 2023, Defendant provided notice of a security breach involving the unauthorized access to Defendant's

network. The attacker viewed and removed data stored in Defendant's system which contained sensitive and confidential Sensitive Information. The notice stated that the information included employees name, and Social Security number were compromised in the Data Breach.

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect its employees' Sensitive Information.

8. Defendant disregarded the rights of Plaintiff and Class members by, among other things, 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 reasonable or adequately robust computer systems and security practices to safeguard its employees' Sensitive Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

9. As a result of Defendant's failure to implement and follow reasonable security procedures, Class employees' Sensitive Information is now in the hands of thieves. Plaintiff and Class members have spent, and will continue to spend, significant amounts of time and money trying to protect themselves from the adverse ramifications of the Data Breach and dealing with actual fraud and will forever be at a heightened risk of identity theft and fraud.

10. Plaintiff, on behalf of all others similarly situated, allege claims for (1) negligence; (2) invasion of privacy; (3) breach of implied contract; (4) unjust enrichment; (5) breach of fiduciary duty; (6) breach of confidence; (7) violation of the California Unfair Competition Law (Cal. Business & Professions Code § 17200, *et seq.*); (8) violation of the California Information Practices Act of 1977 (Cal. Civ. Code § 1798, *et seq.*); (9) violation of the California Consumer Records Act ("CCRA") (Cal. Civ. Code § 1798.80, *et seq.*), and violations of the California Consumer Privacy Act ("CCPA")

(Cal. Civ. Code § 1798.150, *et seq.*). Plaintiff and the Class members seek damages, including but not limited to nominal damages from Defendant, and to compel Defendant to adopt reasonably sufficient security practices to safeguard its Employees' Sensitive Information that remains in Defendant's custody to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

11. Plaintiff Robin Foster is a resident of the State of California and was an employee of Defendant. On or about June 8, 2023, Plaintiff Foster received notice from Defendant that his Sensitive Information had been improperly exposed to unauthorized third parties.

12. The notices received by Plaintiff are substantially similar to the exemplar Notice of Data Breach letter submitted to the State of California. On information and belief, Defendant has not posted a notice of the Data Breach on Defendant's website.

13. Defendant conducts business in the state of California. Defendant's headquarters are located at 1851 San Diego Avenue, San Diego, CA 92110.

JURISDICTION AND VENUE

14. This Court has jurisdiction over this action because Defendant is a citizen of California and conducts business in California.

15. Venue in this Court is proper pursuant to California Code of Civil Procedure § 395, *et seq.*, because—on information and belief—the acts complained of herein took place within the county of San Diego, California; and Defendant conducts business is in San Diego County, California.

FACTUAL ALLEGATIONS

A. <u>Background.</u>

16. Defendant buys and sells fine jewelry through retail stores throughout San Diego County, and conducts business online throughout America. Defendant employs numerous customer service representatives to interact with customers, and craftsmen and craftswomen to work on and repair jewelry.

17. Common practice for employers, Defendant must keep its employees' Sensitive Information in its system. Defendant accomplishes this by keeping the Sensitive Information electronically—even in its email systems.

18. As an employer, Defendant is required to ensure that such sensitive, personal information is not disclosed or disseminated to unauthorized third parties without Employees' express, written consent, as further detailed below.

B. The Data Breach.

19. On or around April 28, 2023, Defendant issued a Notice of Data Event, notifying employees of an incident involving potential unauthorized access to personal information. Defendant provided this Data Breach Notification to an undisclosed number of members ("April 28, 2023, Data Breach Notice"). The April 2023 Data Breach Notice informed the affected members that:

> On November 10, 2022, Leo Hamel Fine Jewelers became aware of suspicious activity affecting certain systems within our network. We immediately took steps to secure our systems and launch an investigation with the assistance of third-party computer specialists, to confirm the full nature and scope of the activity and to restore functionality to the affected systems. The investigation determined that an unknown actor gained access to certain Leo Hamel Fine Jewelers systems beginning on November 6, 2022, and may have viewed or taken information stored in those areas. We then undertook a comprehensive and time-intensive review of the potentially impacted files to determine if they contained sensitive information and to whom it related. Once this review was complete, we reviewed our records to locate address information for potentially affected individuals so that notice could be provided. On March 24, 2023, the review for address information was completed and we determined that your information was contained within the potentially impacted files.
>
> The information related to you that may have been affected includes your name and Social Security number.

20. On information and belief, Defendant has not posted any Notice of Data Breach on its website. Defendant provided members the April 2023 Data Breach Notice which informed the affected members that:

Leo Hamel Fine Jewelers, Inc. ("Leo Hamel Fine Jewelers") writes to notify you of a recent event that may have impacted some of your information. We are providing you with information about the event, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

On November 10, 2022, Leo Hamel Fine Jewelers became aware of suspicious activity affecting certain systems within our network. We immediately took steps to secure our systems and launch an investigation with the assistance of third-party computer specialists, to confirm the full nature and scope of the activity and to restore functionality to the affected systems. The investigation determined that an unknown actor gained access to certain Leo Hamel Fine Jewelers systems beginning on November 6, 2022, and may have viewed or taken information stored in those areas. We then undertook a comprehensive and time-intensive review of the potentially impacted files to determine if they contained sensitive information and to whom it related. Once this review was complete, we reviewed our records to locate address information for potentially affected individuals so that notice could be provided. On March 24, 2023, the review for address information was completed and we determined that your information was contained within the potentially impacted files.

The information related to you that may have been affected includes your name and Social Security number.

Safeguarding the privacy of information in our care and the security of our network are among our highest priorities. Upon learning of this event, we moved quickly to investigate and respond. Assess the security of our systems, and notify potentially affected individuals. We also notified the Federal Bureau of Investigations of this event. As part of our ongoing commitment to the security of information within our care, we are reviewing our existing policies and procedures regarding cybersecurity and evaluating additional measures and safeguards to protect against this type of event in the future. We also implementing additional network security measures to further enhance our network security.

Although we are unaware of any misuse of your information as a result of this incident, as an added precaution, we are offering you complimentary access to twelve (12) months of identity monitoring services through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud

> Consultation, and Identity Theft Restoration. For details of this offer and activation instructions, please review the information contained in the attached *Steps You Can Take to Help Protect Your Information*.

21. The April 2023 Data Breach Notice identified the following data points: employee name, and Social Security number.

22. Defendant failed to put in place proper security protocols to protect against the unauthorized release of employee information and failed to properly train its employees on such protocols, resulting in the unauthorized release of private data. As a result of Defendants failures, Plaintiff and the Class Employees' Sensitive Information was accessed and viewed by unknown and unauthorized third parties and is, or likely will be, for sale on the dark web. This means that the Data Breach was successful: unauthorized individuals accessed Plaintiff and the Class employees' unencrypted, unredacted information set forth above.

23. Plaintiff received data breach notification letters from Defendant on or about May 8, 2023, informing them of the Data Breach and that their Sensitive Information was present in the affected Leo Hamel Fine Jewelers, Inc. systems. The Data Breach notification indicated the following information may have been compromised employee name and Social Security number.

24. This kind of Sensitive Information is highly valued by 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. Social Security numbers are especially valuable to identity thieves.

C. <u>Plaintiff's Exposure and Mitigation Efforts</u>

Plaintiff Foster

25. As a direct result of the Data Breach, Plaintiff Foster has engaged in mitigation efforts and expended time and resources. Plaintiff Foster now checks his credit reports as well as his banking statements and credit card statements on a daily

basis. This is time Plaintiff Foster otherwise would have spent performing other activities, such as his job or leisure activities.

26. Following the Data Breach, on or around February 2023, Plaintiff Foster was notified by the Internal Revenue Service ("IRS"), that fraudulent federal tax returns were filed in his name.

27. As a direct result of the Data Breach, Plaintiff Foster has spent approximately 15 hours on the phone, spanning multiple days, with the IRS in attempts to remedy any damage done by the fraudster. As of the date of this filing, Plaintiff Foster's IRS issues have still yet to be rectified due to the fraudster's actions.

28. As a direct result of the Data Breach, Plaintiff Foster has hired a tax attorney at $500.00 a month, on a 14-month contract totaling $7,000.00, to assist Plaintiff Foster in remedying his tax issues with the IRS.

29. Knowing that thieves stole his Sensitive Information and knowing that his Sensitive Information may now or in the future be available for sale on the dark web has caused Plaintiff Foster great anxiety. He is now very concerned about fraudulent tax returns filed in his name and identity theft in general. This Data Breach has given Plaintiff Adams hesitation about using electronic services and reservations about conducting other online activities requiring his personal information.

30. Plaintiff Foster suffered actual injury from having his Sensitive Information exposed as a result of the Data Breach including, but not limited to: (a) actual instances of identity fraud; (b) damages to and diminution in the value of his Sensitive Information—a form of intangible property that Plaintiff Foster entrusted to Defendant as a condition for employment; (c) loss of his privacy; (d) imminent and impending injury arising from the increased risk of fraud and identity theft; and (e) the time and expense of his mitigation efforts as a result of the Data Breach.

31. As a result of the Data Breach, Plaintiff Foster will continue to be at heightened risk for financial fraud, and identity theft, and the attendant damages, for years to come.

D. Defendant Knew or Should Have Known of the Risk Because large employers are Particularly Susceptible to Cyber Attacks.

32. The number of U.S. data breaches surpassed 1,000 in 2016—a record high and a 40 percent increase in the number of data breaches from the previous year.[1] In 2017, 1,579 breaches were reported—a new record high and a 44.7 percent increase in just one year.[2] That trend continues.

33. Defendant knew and understood unprotected or exposed Sensitive Information in the custody of employers, such as Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Sensitive Information through unauthorized access. Indeed, when compromised, highly confidential related data is among the most sensitive and personally consequential. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impacts the economy as a whole.[3]

34. Data breaches continue to rapidly increase. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[4]

35. As an employer provider, Defendant knew, or should have known, the importance of safeguarding Sensitive Information entrusted to it by Plaintiff and Class

---

[1] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html (last accessed May 8, 2023).

[2] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf (last accessed May 8, 2023).

[3] *Id.*

members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

E. Defendant Acquires, Collects, and Stores Plaintiff and Class Employees' PII.

36. Defendant acquires, collects, and stores a massive amount of its Employees' protected confidential information and other personally identifiable data.

37. As a condition of engaging in employment, Defendant requires its employees to entrust them with highly confidential Sensitive Information.

38. By requiring, obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Employees' Sensitive Information, Defendant assumed legal and equitable duties, and knew or should have known it was responsible for protecting Plaintiff's and Class Employees' Sensitive Information from disclosure.

39. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their Sensitive Information. Plaintiff and Class members relied on Defendant to keep their Sensitive Information confidential and securely maintained, to use this information for business purposes only, to only allow authorized disclosures of this information, and prevent unauthorized disclosure of the information.

F. The Value of PII and the Effects of Unauthorized Disclosure.

40. Defendant was well aware of the highly private nature of the Sensitive Information it collects and its significant value to those who would use it for wrongful purposes.

41. Sensitive Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can commit an array of crimes including identify theft, medical fraud, and financial fraud.[5] Indeed, a robust "cyber black market" exists in

[5] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed May 9, 2023).

which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

42. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363, according to the Infosec Institute. This is because an individual's health history (e.g., ailments, diagnosis, surgeries, etc.) cannot be changed.[6]

43. The ramifications of Defendant's failure to keep Plaintiff' and Class Employees' Sensitive Information secure are long lasting and severe. Once Sensitive Information is stolen, fraudulent use of that information and damage to victims may continue for years.

44. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Sensitive Information and of the foreseeable consequences if its data security systems were breached, including the significant costs that would be imposed on its members as a result of a breach.

G. Defendant Failed to Comply with FTC Guidelines.

45. The Federal Trade Commission ("FTC") promulgates numerous guides for businesses highlighting 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.[7]

46. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[8] The guidelines note that businesses should protect the personal customer information they

[6] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at:* https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last accessed May 9, 2023).

[7] Federal Trade Commission, *Start With Security*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed May 9, 2023).

[8] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed May 9, 2023).

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.

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

48. The FTC brings 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. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

49. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Employees' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

50. Defendant was at all times fully aware of its obligation to protect Plaintiff' and Class Employees' Sensitive Information because of Defendant's position as a trusted and experience employer. Defendant was also aware of the significant repercussions that would result from its failure to do so.

H. <u>Defendant Failed to Comply with Industry Standards.</u>

51. Defendant failed to implement several basic cybersecurity safeguards that can be implemented to improve cyber resilience and require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture

[9] FTC, *Start With Security*, *supra* note 16.

including: (a) the proper encryption of PII; (b) educating and training employees on how to protect PII; and (c) correcting the configuration of software and network devices.

52. Private cybersecurity firms have also identified the businesses as being particularly vulnerable to cyber-attacks, both because of the value of the PII they maintain and because employees have been slow to adapt and respond to cybersecurity threats.[10] These private cybersecurity firms have also promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of PII.

53. Despite the abundance and availability of information regarding the threats and cybersecurity best practices to defend against those threats, Defendant chose to ignore them. These best practices were known, or should have been known by Defendant, whose failure to heed and properly implement industry standards directly led to the Data Breach and the unlawful exposure of Sensitive Information.

I. Plaintiff and Class members Suffered Damages.

54. The ramifications of Defendant's failure to keep Plaintiff's and Class Employees' Sensitive Information secure are long lasting and severe. Once that kind of Sensitive Information 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.[11]

55. The Sensitive Information belonging to Plaintiff and Class members is private, sensitive in nature, and left inadequately protected by Defendant—who did

[10] Stickman Cyber, *Why Cybersecurity In The Workplace Is Everyone's Responsibility, available at:* https://www.stickmancyber.com/cybersecurity-blog/why-cybersecurity-in-the-workplace-is-everyones-responsibility (last accessed May 9, 2023).

[11] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed May 9, 2023).

not obtain Plaintiff's or Class Employees' consent to disclose such Sensitive Information to any other person as required by applicable law and industry standards.

56. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff's and Class Employees' Sensitive Information from unauthorized access, 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 Plaintiff's and Class Employees' Sensitive Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

57. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect member data.

58. Defendant could have prevented the intrusions into its systems and, ultimately, the theft of Sensitive Information if Defendant had remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field.

59. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class members are now in imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to dedicate time and resources which they otherwise would have dedicated to other life demands, such as work and family, to mitigate the actual and potential impact of the Data Breach on their lives.

60. 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."[12]

61. In the breach notification letter, Defendant made an offer of 12–months of identity monitoring services to its members that had their social security numbers breached. This is wholly inadequate to compensate Plaintiff and Class members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Employees' Sensitive Information.

62. As a direct result of the Defendant's failures to prevent the Data Breach, Plaintiff and Class members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Sensitive Information;
b. Out–of–pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
c. Lost opportunity costs and lost wages associated with efforts expended and loss of productivity from addressing and attempting to mitigate actual and future consequences of the Data Breach, including but not limited to researching how to prevent, detect, contest, and recover from identity theft and fraud;
d. The continued risk to their Sensitive Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Sensitive Information in its possession; and

[12] 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 (last accessed May 9, 2023).

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members.

63. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring their Sensitive Information is secure, remains secure, and is not subject to further misappropriation and theft.

J. <u>Defendant's Delay in Identifying & Reporting the Breach Caused Additional Harm.</u>

64. It is axiomatic that:

> The 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.[13]

65. 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, insurance invoices, 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).[14]

[13] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire¸ *available at:* https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million (last accessed May 9, 2023).

[14] Consumer Reports, *The Data Breach Next Door: Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too*, January 31, 2019, *available at:* https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last accessed May 9, 2023).

66. Although their Sensitive Information was improperly exposed on or around November 6, 2022, Plaintiff and Class members were not notified of the Data Breach until on or around April 28, 2021, depriving Plaintiff and Class members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

67. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, there is an increased risk of fraud for Plaintiff and Class members.

CLASS ACTION ALLEGATIONS

68. This action has been brought and may be maintained as a class action pursuant to California Code of Civil Procedure section § 382 because there is a well–defined community of interest among the persons who comprise the readily ascertainable class defined below and because the Plaintiff are unaware of any difficulties likely to be encounter in managing this case as a class action.

69. The Plaintiff bring this class action on behalf of themselves and the following proposed class initially defined as:

> All residents of the State of California whose Sensitive Information stored or possessed by Leo Hamel Fine Jewelers, Inc. was subject to the Data Breach announced by Leo Hamel Fine Jewelers, Inc. on or about April 28, 2023. (the "Class").

70. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has 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; Class Counsel; and all judges assigned to hear any aspect of this litigation, as well as their staff and immediate family members.

71. Pursuant to Rule of Court 3.765(b), Plaintiff reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

72. **Numerosity:** The Class is so numerous that joinder of all members is impracticable. Defendant has identified hundreds of members whose Sensitive Information may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records. A precise number of class members can be ascertained through appropriate discovery and from records maintained by Defendant.

73. **Commonality and Predominance:** Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class members. These include but are not limited to, the following:

a. Whether Plaintiff's and the Class Employees' Sensitive Information was accessed and/or viewed by one or more unauthorized persons in the Data Breach alleged above;
b. Whether Defendant's publishing Plaintiff's and Class Employees' Sensitive Information to unauthorized persons was permissible without the prior written authorization of the Plaintiff or the Class members;
c. When and how Defendant should have learned and actually learned of the Data Breach;
d. Whether Defendant's response to the Data Breach was adequate;
e. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their Sensitive Information;
f. Whether Defendant breached that duty;
g. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class Employees' Sensitive Information;
h. Whether Defendant acted negligently in connection with the

monitoring and/or protecting of Plaintiff's and Class Employees' Sensitive Information;

i. Whether Defendant knew or should have known that they did not employ reasonable measures to keep Plaintiff's and Class Employees' Sensitive Information secure and prevent loss or misuse of that Sensitive Information;

j. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

k. Whether Defendant caused Plaintiff and Class members damages;

l. Whether Defendant violated the law by failing to promptly notify Class members their Sensitive Information was compromised;

m. Whether Plaintiff and Class members are entitled to actual damages, nominal and/or statutory damages, credit monitoring, other monetary relief, and/or equitable relief;

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

o. Whether Defendant violated the California Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq*. (§ 1798.150(a));

p. Whether Defendant violated the Information Act (Cal. Civ. Code § 56, *et seq*.); and

q. Whether Defendant violated the California Consumer Privacy Act ("CCPA") (Cal. Civ. Code § 1798.150, *et seq*.).

74. There are no defenses of a unique nature that may be asserted against the Plaintiff individually, as distinguished from the other members of the class, and the relief sought is common to the class.

75. **Typicality:** Plaintiff's claims are typical of those of other Class members because all had their Sensitive Information compromised because of the Data Breach, due to Defendant's virtually identical conduct.

76. **Adequacy of Representation:** Plaintiff will fairly and adequately represent and protect the interests of the Class members in that Plaintiff's interests are

aligned with the class. Plaintiff have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiff seek no relief adverse to Class members. In addition, Plaintiff retained counsel experienced in data breach and complex consumer class action litigation. Neither Plaintiff nor their counsel have any interests which might cause them not to vigorously pursue this claim.

77. **Superiority:** 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 Defendant. 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.

78. The prosecution of separate actions by individual members of the class would create a risk of inconsistent or varying adjudications with respect to individual members of the class, and a risk that any adjudications with respect to individual members of the class would, as a practical matter, either be dispositive of the interests of other members of the class not party to the adjudication or substantially impair or impede their ability to protect their interests.

79. Class certification is also warranted for purposes of injunctive and declaratory relief because the defendant has acted, or refused to act, on grounds generally applicable to the class, so that final injunctive and declaratory relief are appropriate with respect to the class as a whole.

CAUSES OF ACTION

First Cause of Action
Negligence
(On Behalf of Plaintiff and the Class)

80. Plaintiff incorporate by reference the prior paragraphs as if fully set forth herein.

81. Defendant's own negligent conduct created a foreseeable risk of harm to Plaintiff and Class members. Defendant's negligence included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's negligence also included its decision not to comply with (1) industry standards, and/or best practices for the safekeeping and encrypted authorized disclosure of the Sensitive Information of Plaintiff and Class members; or (2) Section 5 of the FTC Act.

82. First, Defendant 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 its security protocols to ensure Sensitive Information in Defendant's possession was adequately secured and protected, and that employees tasked with maintaining such information were adequately trained on relevant cybersecurity measures. Defendant also had a duty to put proper procedures in place to prevent the unauthorized dissemination of Plaintiff's and Class Employees' Sensitive Information.

83. As a condition of receiving services, Plaintiff and Class members were obligated to provide Defendant directly with their Sensitive Information. As such, Plaintiff and the Class members entrusted their Sensitive Information to Defendant with the understanding Defendant would safeguard their information.

84. Defendant was in a position to protect against the harm suffered by Plaintiff and Class members as a result of the Data Breach. However, Plaintiff and Class

members had no ability to protect their Sensitive Information in Defendant's possession.

85. Defendant had full knowledge of the sensitivity of the Sensitive Information, and the types of harm Plaintiff and Class members could, would, and will suffer if the Sensitive Information were wrongfully disclosed.

86. Defendant admitted that certain systems containing Plaintiff's and Class Employees' Sensitive Information were wrongfully compromised and accessed by unauthorized third persons, and that the Data Breach occurred due to Defendant's actions and/or omissions.

87. Plaintiff and Class members were the foreseeable and probable victims of Defendant's negligent and inadequate security practices and procedures that led to the Data Breach. Defendant knew or should have known of the inherent risks in collecting and storing the highly valuable Sensitive Information of Plaintiff and Class members, the critical importance of providing adequate security of that Sensitive Information, the current cyber security risks being perpetrated, and that Defendant had inadequate employee training, monitoring and education and IT security protocols in place to secure the Sensitive Information of Plaintiff and Class members.

88. Defendant negligently, through its actions and/or omissions, and unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Employees' Sensitive Information while the data was within Defendant's possession and/or control by failing to comply with and/or deviating from standard industry rules, regulations, and practices at the time of the Data Breach.

89. The harm the Data Breach caused is the type of harm privacy laws were intended to guard against. And Plaintiff and Class members are within the class of persons California privacy laws were intended to protect.

90. Defendant negligently failed to comply with privacy laws by failing to protect against and prevent the dissemination of Plaintiff's and Class Employees' Sensitive Information to unauthorized third parties.

91. Third, Defendant's violations of Section 5 of the FTC Act constitute negligence. 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 Defendant, of failing to use reasonable measures to protect Sensitive Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

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

93. Plaintiff and Class members are within the class of persons the FTC Act was intended to protect.

94. The harm the Data Breach caused, and continues to cause, is the type of harm the FTC Act was intended to guard against. The FTC pursues 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 Class members.

95. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent unauthorized dissemination of Plaintiff's and Class Employees' Sensitive Information.

96. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiff and Class members the existence and scope of the Data Breach.

97. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class members, Plaintiff's and Class Employees' Sensitive Information would not have been compromised.

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

99. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered, and continue to suffer, injuries and damages arising from the Data Breach, including, but not limited to: damages from lost time and efforts to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, filing police reports, and damages from identity theft, which may take months—if not years—to discover, detect, and remedy.

100. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered, and will continue to suffer, the continued risks of exposure of their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its continued possession.

Second Cause of Action
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

101. Plaintiff incorporate by reference the prior paragraphs as if fully set forth herein.

102. Plaintiff and Class members had a legitimate expectation of privacy with respect to their Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

103. Defendant owed a duty to its members, including Plaintiff and Class members, to keep their Sensitive Information confidential.

104. The unauthorized release of Sensitive Information, especially Social Security numbers, is highly offensive to a reasonable person.

105. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class members disclosed their Sensitive Information to Defendant as part of their use of Defendant's services, but privately, with the intention that the Sensitive Information would be kept confidential and 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.

106. The Data Breach constitutes an intentional interference with Plaintiff's and Class Employees' 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.

107. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

108. Acting with knowledge, Defendant had notice and knew its inadequate cybersecurity practices would cause injury to Plaintiff and Class members.

109. As a proximate result of Defendant's acts and omissions, Plaintiff and Class Employees' Sensitive Information was disclosed to, and used by, third parties without authorization, causing Plaintiff and Class members to suffer damages.

110. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class members in that the Sensitive Information maintained by Defendant

may be breached again—leading to further viewing, distributing, and use of updated and additional Sensitive Information by unauthorized persons.

111. 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 Class members.

Third Cause of Action
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

112. Plaintiff incorporate by reference the prior paragraphs as if fully set forth herein.

113. Plaintiff and Class members were required to provide their Sensitive Information, including their names, Social Security numbers, addresses, dates of birth, telephone numbers, email addresses, and various other information to Defendant as a condition of their use of Defendant's services.

114. Plaintiff and Class members were paid money by Defendant in exchange for services, along with Defendant's promise to protect their Sensitive Information and other Sensitive Information from unauthorized disclosure.

115. In their written privacy policies, Defendant expressly promised Plaintiff and Class members that it would only disclose protected information and other Sensitive Information under certain circumstances, none of which relate to the Data Breach.

116. Defendant promised to comply with privacy standards, and to make sure Plaintiff's and Class Employees' Sensitive Information would remain protected.

117. Implicit in the agreement between Plaintiff and Class members on the one hand, and the Defendant on the other, regarding providing protected Sensitive Information, was Defendant's obligation to: (a) use such Sensitive Information for business purposes only; (b) take reasonable steps to safeguard that Sensitive Information; (c) prevent unauthorized disclosures of the Sensitive Information; (d) provide Plaintiff and Class members with prompt and sufficient notice of any and

all unauthorized access and/or theft of their Sensitive Information; (e) reasonably safeguard and protect the Sensitive Information of Plaintiff and Class members from unauthorized disclosure or uses; and (f) retain the Sensitive Information only under conditions that kept such information secure and confidential.

118. Without such implied contracts, Plaintiff and Class members would not have provided their Sensitive Information to Defendant.

119. Plaintiff and Class members fully performed their obligations under the implied contract with Defendant. However, Defendant did not.

120. Defendant breached the implied contracts with Plaintiff and Class members by failing to:

a. Reasonably safeguard and protect Plaintiff's and Class Employees' Sensitive Information, which was compromised as a result of the Data Breach; and

b. Identify and respond to suspected or known security incidents;

121. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class members have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to: damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, filing police reports, and damages from identity theft, which may take months if not years to discover, detect, and remedy.

Fourth Cause of Action
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

122. Plaintiff incorporate by reference the prior paragraphs as if fully set forth herein.

123. In light of their special relationship, Defendant became the guardian of Plaintiff's and Class Employees' Sensitive Information. Defendant became a fiduciary, created by its undertaking and guardianship of Plaintiff's and Class Employees' Sensitive Information, to act primarily for the benefit of Plaintiff and Class members. This duty included the obligation to safeguard Plaintiff's and Class Employees' Sensitive Information, and to timely notify them in the event of a data breach.

124. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of its relationship. Defendant breached its fiduciary duties owed to Plaintiff and Class members by failing to:

a. Properly encrypt and otherwise protect the integrity of the system containing Plaintiff's and Class Employees' protected confidential information and other Sensitive Information;

b. Timely notify and/or warn Plaintiff and Class members of the Data Breach; and

c. Otherwise failing to safeguard Plaintiff's and Class Employees' Sensitive Information.

125. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered, and will suffer, injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity to control how their Sensitive Information is used; (c) the compromise, publication, and/or theft of their Sensitive Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (e) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Sensitive Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate

and adequate measures to protect its Employees' Sensitive Information in continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

126. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class members have suffered, and will continue to suffer, other forms of injury and/or harm, and other economic and non–economic losses.

Fifth Cause of Action
Breach of Confidence
(On Behalf of Plaintiff and the Class)

127. Plaintiff incorporate by reference the prior paragraphs as if fully set forth herein.

128. At all times during Plaintiff's and Class Employees' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Employees' Sensitive Information that Plaintiff and Class members provided to Defendant.

129. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by terms and expectations that Plaintiff's and Class Employees' Sensitive Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

130. Plaintiff and Class members provided their respective Sensitive Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Sensitive Information to be disseminated to any unauthorized parties.

131. Plaintiff and Class members also provided their Sensitive Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Sensitive Information from unauthorized disclosure, such as

following basic principles of protecting its networks and data systems, including Defendant's employees' systems.

132. Defendant required and voluntarily received, in confidence, Plaintiff's and Class Employees' Sensitive Information with the understanding that the Sensitive Information would not be disclosed or disseminated to the public or any unauthorized third parties.

133. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class Employees' Sensitive Information, Plaintiff's and Class Employees' Sensitive Information was disclosed to, and misappropriated by, unauthorized third parties beyond Plaintiff's and Class Employees' confidence, and without their express permission.

134. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class members have suffered, and will continue to suffer damages.

135. But for Defendant's disclosure of Plaintiff's and Class Employees' Sensitive Information in violation of the parties' understanding of confidence, Plaintiff's and Class Employees' Sensitive Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Employees' Sensitive Information, as well as the resulting damages.

136. The injury and harm Plaintiff and Class members suffered, and continue to suffer, was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Employees' Sensitive Information. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class Employees' Sensitive Information had numerous security and other vulnerabilities placing Plaintiff's and Class Employees' Sensitive Information in jeopardy.

137. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will suffer injury, including but not

limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their Sensitive Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and (g) the diminished value of Defendant's services they received.

138. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non–economic losses.

Sixth Cause of Action
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*.--Unfair Business Practices
(On Behalf of Plaintiff and the Class)

139. Plaintiff incorporate by reference the prior paragraphs as if fully set forth herein.

140. Defendant violated Cal. Bus. & 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 Plaintiff and Class members.

141. Defendant 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 Class Employees' Sensitive Information with knowledge the information would not be adequately protected; and by storing Plaintiff's and Class Employees' Sensitive Information in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which require Defendant to take reasonable methods of safeguarding the Sensitive Information of Plaintiff and Class members.

142. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

143. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff and Class members were injured and lost money or property, including but not limited to the loss of Plaintiff's and Class Employees' legally protected interest in the confidentiality and privacy of their Sensitive Information, nominal damages, and additional losses as described herein.

144. Defendant knew or should have known Defendant's computer systems and data security practices were inadequate to safeguard Plaintiff's and Class Employees' Sensitive Information and that the risk of a data breach or theft was highly likely. Defendant's 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 Plaintiff and Class members.

145. Plaintiff, on behalf of the Class, seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and Class members of money or property Defendant may have acquired by means of Defendant's unlawful, and unfair business practices, restitutionary disgorgement of all monies that accrued to Defendant because of Defendant's 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.

Seventh Cause of Action
Violation of California's Information Practices Act of 1977
Cal. Civ. Code § 1798, *et seq*.
(On Behalf of Plaintiff and the Class)

146. Plaintiff incorporate by reference the prior paragraphs as if fully set forth herein.

147. Defendant was legally obligated to "establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the [Information Practices Act of 1977], to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury." (Cal. Civ. Code § 1798.21.)

148. Defendant failed to establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the Information Practices Act of 1977 regarding Plaintiff's and Class Employees' Sensitive Information.

149. Defendant failed to ensure the security and confidentiality of records containing Plaintiff's and Class Employees' Sensitive Information.

150. Defendant failed to protect against anticipated threats and hazards to the security and integrity of records containing Plaintiff's and Class Employees' Sensitive Information.

151. As a result of these failures, Plaintiff 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 continuing increased risk of identity theft, and identify fraud risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their Sensitive Information, (iv) deprivation of the value of their private and Sensitive Information, 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.

152. Plaintiff and Class members are also entitled to injunctive relief under California Civil Code § 1798.47.

Eighth Cause of Action
Violation of California Consumer Records Act ("CCRA")
Cal. Civ. Code § 1798.80, *et seq*.
(On Behalf of Plaintiff and the Class)

153. Plaintiff incorporate by reference the prior paragraphs as if fully set forth herein.

154. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay."

155. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82(b).)

156. Any person or business required to issue a security breach notification under the CCRA shall meet the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

i. The name and contact information of the reporting person or business subject to this section;

ii. A list of the types of personal information that were or are

reasonably believed to have been the subject of a breach;

iii. If the information is possible to determine at the time the notice is provided, then any of the following:
    1. The date of the breach;
    2. The estimated date of the breach; or
    3. The date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

vi. The toll–free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

157. The Data Breach described herein constituted a "breach of the security system" of Defendant.

158. As alleged above, Defendant unreasonably delayed informing Plaintiff and Class members about the Data Breach, affecting their Personal Information, after Defendant knew the Data Breach had occurred.

159. Defendant failed to disclose to Plaintiff and Class members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Personal Information when Defendant knew or reasonably believed such information had been compromised.

160. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

161. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiff and Class members would impede its investigation.

162. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and Class members were deprived of prompt notice of the Data Breach, and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff and Class members because their stolen information would have had less value to identity thieves.

163. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and Class members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

164. Plaintiff and Class members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to the damages suffered by Plaintiff and Class members as alleged above and equitable relief.

Ninth Cause of Action
Violation of CCPA
Cal. Civ. Code § 1798.150, *et seq*.
(On Behalf of Plaintiff and the Class)

165. Plaintiff and Class Members incorporate by reference the prior paragraphs as if fully set forth herein.

166. Defendant is a corporation organized or operated for profit or financial benefit of its owners with annual gross revenues of approximately $5 million. Defendant collects consumers' PII as defined in Cal. Civ. Code § 1798.140

167. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and Class Members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

168. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's and Class Members PII. As detailed herein, Defendant failed to do so. As a direct and proximate result of Defendant's acts, Plaintiff's and Class Members' PII, including Social Security numbers, and names were subjected to unauthorized access and exfiltration, theft or disclosure.

169. Plaintiff and Class Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards customer's PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold current and past employee's PII including Plaintiff's and Class Members' PII. Plaintiff and Class Members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

170. Pursuant to Cal. Civ. Code § 1798.150(b), on May 10, 2023, Plaintiff mailed CCPA notice letter to Defendant's registered service agents via overnight post, detailing the specific provisions of CCPA that Leo Hamel Fine Jewelers, Inc. has and continues to violate. If Defendant cannot cure within 30 days, and Plaintiff believe such cure is not possible under these facts and circumstances, then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

Declaratory Judgement

171. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the personal information under the CCPA.

172. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant and third parties with similar inadequate security measures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and all Class members, request

judgment against the Defendant, and that the Court grant the following:

A. An order certifying the Class as defined herein, and appointing Plaintiff and their Counsel to represent the Class;

B. Granting injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein,

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws,

iii. requiring Defendant to delete, destroy, and purge the personal information of Plaintiff and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members,

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal information of Plaintiff and Class Employees' personal information,

v. prohibiting Defendant from maintaining Plaintiff's and Class Employees' personal information on a cloud-based database,

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering

Defendant to promptly correct any problems or issues detected by such third-party security auditors,

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring,

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures,

ix. requiring Defendant to conduct regular database scanning and securing checks,

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal information, as well as protecting the personal information of Plaintiff and Class members,

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach,

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

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

xiv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential personal information to third parties, as well as the steps affected individuals must take to protect themselves,

xv. requiring Defendant to design, maintain, and test its computer systems to ensure that PI in its possession is adequately secured and protected,

xvi. requiring Defendant disclose any future data disclosures in a timely and accurate manner; and

xvii. requiring Defendant to provide ongoing credit monitoring and identity theft repair services to Class members.

C. An award of compensatory, statutory, and nominal in an amount to be determined;

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

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

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demand a trial by jury.

Respectfully submitted,

Date: May 10, 2023

SWIGART LAW GROUP, APC

Joshua B. Swigart