UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

ALEXANDRU SARCA and JENNIFER SIMONI, individually and on behalf of all those similarly situated,	)	Case No. _____
Plaintiffs,	)	**CLASS ACTION COMPLAINT**
v.	)	JURY TRIAL DEMANDED
REVOLVE GROUP, INC.,	)	
Defendant.	)	

CLASS ACTION COMPLAINT
AND DEMAND FOR JURY TRIAL

Plaintiffs, Alexandru Sarca ("Sarca") and Jennifer Simoni ("Simoni") (together, "Plaintiffs"), individually and on behalf of all others similarly situated, bring this Class Action Complaint against Defendant, Revolve Group, Inc. ("Revolve" or "Defendant"), and allege, upon personal knowledge as to their own acts and experiences and, as to all other matters, upon information and belief, including the investigation of their counsel, as follows:

INTRODUCTION

1. This is a class action arising from Revolve's failure to secure the payment card data and other personal information that it collected from its customers and stored on its online shopping platform.

2. Revolve is an online fashion retailer headquartered in Cerritos, California. It operates the Revolve.com and FWRD.com e-commerce sites and sells to consumers throughout the United States, including in Illinois.

3. When a customer makes a purchase, Revolve collects and stores the customer's name, contact and address information, payment card number, and payment card expiration date (collectively, "Private Information").

4. On September 11, 2026, an unauthorized actor accessed Revolve's online shopping platform. By Revolve's own account, that actor may have obtained customers' Private Information stored on that platform, and may have done so "through automated means" (the "Data Breach").[1]

5. By Revolve's own account, it was not until September 29, 2026, eighteen days after the intrusion, that Revolve determined what customer data was involved. Revolve reported to the Texas Attorney General that the Data Breach affected 127,200 Texas residents alone.[2] Upon information and belief, the Data Breach affected approximately 1.5 million individuals nationwide.

6. Revolve did not begin notifying its customers until on or about October 29, 2026, the same day it disclosed the incident to its investors in a filing with the Securities and Exchange Commission. That was approximately thirty days after Revolve determined that payment card data was involved and forty-eight days after the intrusion. During that entire period, the affected payment cards remained active and exposed.

7. The notice Revolve sent offered its customers no credit monitoring, no identity protection, and no other remedial service. It instructed them to review their own payment card statements and to consider, at their own initiative, obtaining credit reports and placing fraud alerts or security freezes.[3]

---

[1] Revolve Group, Inc., Current Report (Form 8-K), Item 8.01 (Oct. 29, 2026), https://www.sec.gov/Archives/edgar/data/0001746618/000119312526439022/rvlv-20261029.htm (last visited Nov. 12, 2026).

[2] Office of the Texas Attorney General, Data Security Breach Reports, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Nov. 10, 2026) (entry for Revolve Group, Inc., published Oct. 30, 2026).

[3] Revolve Group, Inc., Notice of Data Breach (sample notice submitted to the California Attorney General), https://oag.ca.gov/system/files/Revolve%20-%20California%20Notification.pdf (last visited Nov. 10, 2026); *see*

8. At the same time, Revolve told its investors that the incident had caused no operational disruption and that it did not expect a material impact on its business. Revolve thus treated the Data Breach as immaterial to itself while leaving its affected customers to bear its consequences.

9. The Data Breach was the direct and foreseeable result of Revolve's failure to implement and maintain reasonable security measures for stored payment card data, to detect and stop the automated extraction of that data, and to notify its customers without unreasonable delay.

10. Plaintiffs are Revolve customers whose Private Information was compromised in the Data Breach. They bring this action on behalf of themselves, a Nationwide Class, and an Illinois Subclass, and assert claims for negligence, breach of implied contract, breach of fiduciary duty, unjust enrichment, violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, violation of the California Unfair Competition Law, and declaratory and injunctive relief.

PARTIES

Plaintiffs

11. Plaintiff Jennifer Simoni is a natural person and a citizen of the State of Illinois who resides in Skokie, Cook County, Illinois.

12. Plaintiff Simoni is a Revolve customer. She has made purchases from Revolve from her home in Illinois, has had those purchases shipped to her in Illinois, and provided her payment card information to Revolve to pay for them.

---

also Cal. Dep't of Justice, Data Security Breach Report, Revolve Group, Inc., https://oag.ca.gov/ecrime/databreach/reports/sb24-632070 (last visited Nov. 10, 2026).

13. Plaintiff Simoni received from Revolve, by U.S. Mail, a Notice of Data Breach dated October 29, 2026, informing her that her name, address, and the number and expiration date of her payment card ending in 6630 may have been acquired in the Data Breach.

14. Plaintiff Alexandru Sarca is a natural person and a citizen of the State of Illinois who resides in Cook County, Illinois.

15. Plaintiff Sarca is a Revolve customer. He has made purchases from Revolve from his home in Illinois, has had those purchases shipped to him in Illinois, and provided his payment card information to Revolve to pay for them.

16. Plaintiff Sarca received from Revolve, by U.S. Mail, a Notice of Data Breach dated October 29, 2026, informing him that his name, address, and the number and expiration date of his payment card ending in 9231 may have been acquired in the Data Breach.

Defendant

17. Defendant, Revolve Group, Inc., is a corporation organized under the laws of the State of Delaware with its principal place of business at 12889 Moore Street, Cerritos, California 90703. Revolve is a publicly traded company that, directly and through its subsidiaries, operates the Revolve.com and FWRD.com online retail sites.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d). This is a putative class action in which: (i) the proposed classes consist of more than 100 members; (ii) at least one class member, including each Plaintiff, a citizen of Illinois, is a citizen of a State different from Defendant, a citizen of Delaware and California; and (iii) the amount in controversy exceeds $5,000,000 in the aggregate, exclusive of interest and costs.

19. This Court has personal jurisdiction over Defendant because Plaintiffs' claims arise out of and relate to Defendant's contacts with Illinois. Defendant purposefully markets and sells its products to Illinois consumers through its interactive e-commerce platform, accepts orders and payment card information from Illinois consumers, and ships products to Illinois. Defendant collected Plaintiffs' Private Information from them in Illinois in the course of selling and shipping products to them in Illinois, and Plaintiffs suffered their injuries in Illinois.

20. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred here. Plaintiffs reside in Cook County, Illinois, provided their Private Information to Defendant from this District, received Defendant's notices of the Data Breach in this District, and were injured in this District.

FACTUAL ALLEGATIONS

A. Revolve Collects and Stores Its Customers' Payment Card Data

21. Revolve is an online fashion retailer. It sells its products to consumers through its e-commerce sites, including Revolve.com and FWRD.com.

22. To complete a purchase, a customer must provide Revolve with her name, billing and shipping addresses, contact information, and payment card details. Revolve's Privacy Policy confirms that Revolve collects a customer's payment card information when she makes a purchase.[4]

23. Revolve does not use that information only to complete the transaction. Its Privacy Policy states that Revolve uses the information it collects to remember a customer's information so that the customer need not enter it again on a later visit, and to record the purchases a customer

[4] Revolve Group, Inc., Privacy Policy (last updated July 21, 2026), https://www.revolve.com/privacypolicy (last visited Nov. 12, 2026).

has made. Upon information and belief, retaining its customers' payment information benefits Revolve commercially by making checkout easier and encouraging repeat purchases.

24. Revolve's Privacy Policy states that Revolve stores the information it collects "for as long as is necessary" for the purposes for which it was collected. The Privacy Policy also states that Revolve uses customer information to protect against fraud and unauthorized transactions and, in describing where customer information is processed, that Revolve will take steps to maintain an adequate level of protection for that information. The Privacy Policy does not describe the safeguards Revolve uses to protect stored payment card data, and it does not disclose that stored payment card numbers are kept in a form that an intruder could extract.

25. The Privacy Policy lists the circumstances in which Revolve may disclose customer information to third parties. None of those circumstances applies to the Data Breach.

26. By soliciting, collecting, storing, and profiting from its customers' Private Information, Revolve assumed legal and equitable duties to keep that information confidential and secure, and to protect it from unauthorized access and theft.

27. Plaintiffs and Class Members provided their Private Information to Revolve with the reasonable expectation that Revolve would comply with those duties.

B. The Data Breach

28. According to the notice Revolve sent to its customers, on September 11, 2026, an unauthorized actor accessed Revolve's online shopping platform and may have acquired certain customer information.[5]

[5] Revolve Group, Inc., Notice of Data Breach, *supra* note 3.

29. The same notice states that on September 29, 2026, Revolve determined that the affected data included customers' names, addresses, and the numbers and expiration dates of their payment cards.

30. Revolve also reported the Data Breach to the Texas Attorney General. According to that report, which was published on October 30, 2026, the Data Breach affected 127,200 Texas residents, the information affected included names and financial information such as account numbers and credit or debit card numbers, and Revolve gave notice by U.S. Mail and by posting on a website.[6] Upon information and belief, the Data Breach affected approximately 1,515,073 individuals nationwide.

31. Upon information and belief, Revolve did not detect the intrusion until on or about September 29, 2026. For approximately eighteen days, therefore, an unauthorized actor's access to Revolve's shopping platform and to its customers' stored payment card data went undetected.

32. On October 29, 2026, Revolve filed a Current Report on Form 8-K with the Securities and Exchange Commission. In that report, Revolve stated that it had become aware of unauthorized access to certain of its systems and that it believed an unauthorized actor may have obtained, through automated means, the name, contact information, payment card number, and payment card expiration date of certain customers whose payment information was saved on its e-commerce platform.[7]

33. In the same report, Revolve stated that it had notified federal law enforcement and retained outside cybersecurity experts, that the incident had not disrupted its operations, and that it did not believe the incident would have a material impact on its business.

[6] Office of the Texas Attorney General, Data Security Breach Reports, *supra* note 2.
[7] Revolve Group, Inc., Form 8-K, *supra* note 1.

34. Revolve has not disclosed when it first learned of the unauthorized activity, how the unauthorized actor gained access to its platform, what "automated means" were used to obtain its customers' Private Information, how long the unauthorized access lasted, or whether the stored payment card numbers were encrypted or otherwise rendered unreadable.

35. Revolve has not publicly identified the unauthorized actor. Upon information and belief, the Private Information of Plaintiffs and Class Members was copied and removed from Revolve's systems and remains in the possession of that actor or of those to whom it has been transferred.

C. Revolve's Delayed and Inadequate Notice

36. Revolve began notifying affected customers on or about October 29, 2026, approximately thirty days after it determined that payment card data was involved and forty-eight days after the intrusion. The notices Plaintiffs received are dated October 29, 2026.

37. Revolve submitted sample copies of its customer notice to state regulators, including the Attorneys General of California and Massachusetts.[8]

38. The notice does not explain how the Data Breach occurred, does not state how many customers were affected, and does not state whether the payment card data was encrypted.

39. The notice offers no credit monitoring, identity theft protection, or reimbursement of any kind. It tells customers to review their payment card statements, to report unauthorized charges to their card issuers, and to consider obtaining credit reports and placing fraud alerts or security freezes on their own.

40. Revolve's delay deprived Plaintiffs and Class Members of the opportunity to cancel or replace their payment cards, to monitor their accounts with heightened attention, and to take

[8] Revolve Group, Inc., sample notice submitted to the Massachusetts Attorney General, https://www.mass.gov/doc/2026-1895-revolve-group-inc/download (last visited Nov. 10, 2026).

other protective measures during the weeks when their card data was already in the hands of an unauthorized actor.

D. The Data Breach Was Foreseeable and Preventable

41. Stored payment card data is a well-known target of cybercriminals, and the risk that an online retailer's stored card data will be attacked has been recognized by regulators and by the payment card industry for many years.

42. The Payment Card Industry Data Security Standard ("PCI DSS") applies to every entity that stores, processes, or transmits payment card data. Requirement 3 of the PCI DSS requires such an entity to limit its storage of account data, to restrict the display and copying of full card numbers, and to render card numbers unreadable anywhere they are stored, through methods such as strong cryptography, truncation, or tokenization.[9]

43. The Federal Trade Commission ("FTC") has published data security guidance for businesses for many years. That guidance directs businesses to retain payment card account numbers and expiration dates only where there is a genuine business need, to encrypt sensitive information stored on their networks, to use intrusion detection systems, and to monitor outgoing traffic for unexpectedly large transfers of data.[10]

44. The FTC has also concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an unfair practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

---

[9] PCI Security Standards Council, *Payment Card Industry Data Security Standard*, v4.0.1 (June 2024), Requirement 3 (Protect Stored Account Data).

[10] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Nov. 10, 2026).

45. Revolve, a publicly traded online retailer that stores the payment card data of its customers nationwide, knew or should have known of these standards and of the consequences of failing to meet them.

46. The facts Revolve has disclosed show that it did not meet them. An unauthorized actor was able to obtain, through automated means, the full payment card numbers and expiration dates of, upon information and belief, approximately 1.5 million customers, and that activity went undetected for approximately eighteen days. Upon information and belief, that could not have occurred unless Revolve failed to do one or more of the following:

(a) render stored payment card numbers unreadable through encryption, tokenization, or truncation, or adequately protect the means of reversing those protections;

(b) restrict access to, and the display and retrieval of, full payment card numbers and expiration dates;

(c) implement controls capable of detecting and blocking the automated, high-volume retrieval of customer and payment data;

(d) monitor its systems and outgoing traffic so as to promptly detect unauthorized access and the removal of data; and

(e) limit its retention of payment card data to what was necessary.

47. Had Revolve implemented and maintained reasonable security measures consistent with industry standards and FTC guidance, the Data Breach would have been prevented or, at a minimum, detected and stopped before its customers' Private Information was taken.

E. The Value of the Stolen Data and the Harm to Plaintiffs and Class Members

48. Payment card data has a ready market among criminals. According to Experian, credit card details sell on the dark web for $10 to $240, with the price depending in part on how complete the data is.[11]

49. The data taken in the Data Breach is unusually complete. It pairs each payment card number with the cardholder's name, address, contact information, and card expiration date. Upon information and belief, that combination is sufficient to attempt fraudulent card-not-present transactions with merchants that do not require additional verification.

50. The same data also exposes Plaintiffs and Class Members to targeted phishing and social engineering. A criminal who knows a person's name, contact information, and payment card details, and who knows that the person is a Revolve customer, can credibly impersonate Revolve or the person's card issuer in order to obtain further information.

51. Fraudulent use of stolen payment data does not always occur immediately. Stolen data may be held, sold, and resold before it is used, so that the risk to Plaintiffs and Class Members will continue well beyond the date of Revolve's notice.

52. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer injuries, including: (i) the theft of their Private Information; (ii) the loss of the confidentiality and the diminished value of that information; (iii) unauthorized charges and the time and effort required to dispute them; (iv) the time, inconvenience, and expense of cancelling and replacing payment cards, updating recurring payments, and monitoring accounts; (v) a present and continuing risk of fraud and identity theft; (vi) the loss of

[11] Ben Luthi, *Here's What Your Data Sells for on the Dark Web*, Experian (June 30, 2025), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Nov. 10, 2026).

the benefit of their bargain with Revolve; and (vii) the continued exposure of their Private Information, which remains in Revolve's possession and subject to further breaches so long as Revolve fails to adopt adequate security measures.

F. Plaintiff Simoni's Experience

53. Plaintiff Simoni has been a Revolve customer for several years. As a condition of purchasing products from Revolve, she provided Revolve with her name, address, contact information, and payment card information.

54. Plaintiff Simoni provided her Private Information to Revolve with the expectation that Revolve would keep it confidential and secure. Had she known that Revolve would not adequately protect her payment card data, she would not have purchased from Revolve on the same terms.

55. Plaintiff Simoni received Revolve's Notice of Data Breach, dated October 29, 2026, by U.S. Mail at her home in Skokie, Illinois. The notice informed her that on September 11, 2026 an unauthorized actor accessed Revolve's online shopping platform, and that on September 29, 2026 Revolve determined that the data that may have been acquired contained her name and address, as well as the card number and expiration date for her payment card ending in 6630.

56. The notice offered Plaintiff Simoni no credit monitoring, identity theft protection, or reimbursement. It advised her to review her payment card statements for unauthorized charges, to report any such charges to her card issuer, and to consider obtaining credit reports and placing fraud alerts or security freezes herself. It did not tell her when Revolve first learned of the unauthorized activity or how the unauthorized actor obtained her information.

57. Since receiving the notice, Plaintiff Simoni has regularly reviewed her credit reports for signs that her information has been misused, and she is considering placing a security freeze on her credit files.

58. Plaintiff Simoni plans to make a major purchase in the coming year for which she will need access to her credit. As Revolve's own notice explains, a security freeze must be placed separately with each credit reporting company and must be lifted before a creditor can review the consumer's credit report. The Data Breach therefore requires Plaintiff Simoni to continue to spend time and money, monitoring and protecting her credit.

59. Plaintiff Simoni has spent several hours responding to the Data Breach, including reviewing her account statements for unauthorized activity and investigating the incident. This is time she would otherwise have spent on other activities.

60. Since the Data Breach, Plaintiff Simoni has experienced a noticeable increase in suspicious emails, text messages, and telephone calls.

61. Plaintiff Simoni is careful with her Private Information. To her knowledge, the payment card affected by the Data Breach has not been compromised in any other data breach.

62. Plaintiff Simoni's Private Information remains in Revolve's possession. She has a continuing interest in ensuring that it is protected from further breaches.

G. Plaintiff Sarca's Experience

63. Plaintiff Sarca has been a Revolve customer for several years. As a condition of purchasing products from Revolve, he provided Revolve with his name, address, contact information, and payment card information.

64. Plaintiff Sarca provided his Private Information to Revolve with the expectation that Revolve would keep it confidential and secure. Had he known that Revolve would not

adequately protect his payment card data, he would not have purchased from Revolve on the same terms.

65. Plaintiff Sarca received Revolve's Notice of Data Breach, dated October 29, 2026, by U.S. Mail at his home in Cook County, Illinois. The notice informed him that on September 11, 2026 an unauthorized actor accessed Revolve's online shopping platform, and that on September 29, 2026 Revolve determined that the data that may have been acquired contained his name and address, as well as the card number and expiration date for his payment card ending in 9231.

66. The notice Plaintiff Sarca received is identical in substance to the notice Plaintiff Simoni received. It offered him no credit monitoring, identity theft protection, or reimbursement, and it did not tell him when Revolve first learned of the unauthorized activity or how the unauthorized actor obtained his information.

67. Plaintiff Sarca has spent several hours responding to the Data Breach, including reviewing his account statements for unauthorized activity and investigating the incident. This is time he would otherwise have spent on other activities.

68. Plaintiff Sarca's Private Information remains in Revolve's possession. He has a continuing interest in ensuring that it is protected from further breaches.

CLASS ALLEGATIONS

69. Plaintiffs bring this action under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3), and, as appropriate, (c)(4), on behalf of themselves and the following classes:

Nationwide Class: All individuals residing in the United States whose Private Information was accessed or acquired by an unauthorized party in the data security incident that Revolve disclosed on or about October 29, 2026.

Illinois Subclass: All members of the Nationwide Class who resided in Illinois at the time of the Data Breach.

70. The Nationwide Class and the Illinois Subclass are referred to collectively as the "Class," and their members as "Class Members."

71. Excluded from the Class are Defendant, its officers, directors, and employees, any entity in which Defendant has a controlling interest, Defendant's affiliates, legal representatives, successors, and assigns, counsel for the parties, and any judicial officer presiding over this matter and the members of his or her immediate family and judicial staff.

72. Plaintiffs reserve the right to modify the class definitions, or to propose additional subclasses, as discovery and further investigation warrant.

73. Numerosity. The members of the Class are so numerous that joinder is impracticable. Revolve reported to the Texas Attorney General that the Data Breach affected 127,200 Texas residents alone and, upon information and belief, it affected approximately 1,515,073 individuals nationwide. Revolve has not publicly disclosed the number of affected Illinois residents but, upon information and belief, the Illinois Subclass numbers in the thousands. Class Members can be identified from Revolve's own records, including the records it used to send its notices.

74. Commonality and Predominance. Common questions of law and fact exist as to all Class Members and predominate over any questions affecting only individual members. These common questions include:

(a) whether Revolve owed a duty to Plaintiffs and Class Members to safeguard their Private Information;

(b) whether Revolve failed to implement and maintain reasonable security measures for stored payment card data;

(c) whether Revolve's security measures complied with industry standards, FTC guidance, and applicable law;

(d) whether Revolve failed to detect the Data Breach within a reasonable time;

(e) whether Revolve notified Plaintiffs and Class Members of the Data Breach without unreasonable delay;

(f) whether Revolve's conduct was negligent, breached its implied contracts, or was unfair or unlawful under the statutes pleaded below; and

(g) whether Plaintiffs and Class Members are entitled to damages, restitution, and injunctive relief, and in what measure.

75. Typicality. Plaintiffs' claims are typical of those of the Class. Plaintiffs and every Class Member provided Private Information to Revolve in connection with a purchase, had that information compromised in the same Data Breach, and were injured by the same course of conduct.

76. Adequacy. Plaintiffs will fairly and adequately protect the interests of the Class. Their interests do not conflict with those of other Class Members, and they have retained counsel experienced in class action litigation who will prosecute this action vigorously.

77. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The damages suffered by individual Class Members are small relative to the burden and expense of individual litigation against a well-resourced defendant. Individual actions would also risk inconsistent adjudications of identical questions. Plaintiffs are

aware of no difficulty in the management of this action that would preclude its maintenance as a class action.

78. Injunctive and Declaratory Relief. Revolve has acted or refused to act on grounds that apply generally to the Class, so that final injunctive relief and corresponding declaratory relief are appropriate with respect to the Class as a whole.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Illinois Subclass)

79. Plaintiffs repeat and reallege paragraphs 1 through 78 as if fully set forth herein.

80. Revolve solicited, collected, and stored the Private Information of Plaintiffs and Class Members for its own commercial benefit. Revolve therefore owed Plaintiffs and Class Members a duty to exercise reasonable care in safeguarding that information, including by rendering stored payment card data unreadable, restricting access to it, monitoring for unauthorized access, and deleting data it no longer needed.

81. Revolve's duty also arose from statute. The Illinois Personal Information Protection Act requires a data collector that owns or licenses, or maintains or stores, records that contain personal information concerning an Illinois resident to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. 815 ILCS 530/45(a). Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits the unfair practice of failing to employ reasonable data security. These duties exist independently of any contract between Revolve and its customers.

82. Revolve further owed Plaintiffs and Class Members a duty to notify them of the Data Breach in the most expedient time possible and without unreasonable delay, so that they could take steps to protect themselves.

83. It was foreseeable that a failure to use reasonable care in securing stored payment card data would result in the theft of that data and in injury to the customers to whom it belonged. Plaintiffs and Class Members were the foreseeable and probable victims of Revolve's inadequate security practices.

84. Plaintiffs and Class Members had no ability to protect the Private Information that was in Revolve's possession. Revolve alone was in a position to prevent the Data Breach.

85. Revolve breached its duties by, among other things, failing to implement and maintain reasonable security measures for stored payment card data, failing to detect and stop the automated extraction of that data, failing to detect the Data Breach for approximately eighteen days, and failing to notify Plaintiffs and Class Members for approximately thirty days after determining that their payment card data was involved.

86. Revolve's violations of Section 5 of the FTC Act and the Illinois Personal Information Protection Act are evidence of its negligence. Plaintiffs and Class Members are within the class of persons those statutes were intended to protect, and the harm they suffered is the type of harm those statutes were intended to prevent. To the extent California law applies, Revolve's violations give rise to a presumption of negligence under Cal. Evid. Code § 669.

87. But for Revolve's breaches of its duties, the Private Information of Plaintiffs and Class Members would not have been compromised.

88. As a direct and proximate result of Revolve's negligence, Plaintiffs and Class Members have suffered and will continue to suffer the injuries described above, and are entitled to recover actual, consequential, and nominal damages in an amount to be proven at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Illinois Subclass)

89. Plaintiffs repeat and reallege paragraphs 1 through 78 as if fully set forth herein.

90. Revolve offered to sell products to Plaintiffs and Class Members and required them to provide their Private Information for that purpose. Plaintiffs and Class Members accepted that offer, purchased products from Revolve, and provided their Private Information.

91. In doing so, Plaintiffs and Class Members entered into implied contracts with Revolve under which Revolve agreed to safeguard their Private Information, to use it only for legitimate business purposes, and to notify them promptly if it was compromised.

92. These terms were implied by the parties' conduct and by the nature of the transaction. No reasonable customer would save a payment card to a retailer's website without the understanding that the retailer would take reasonable steps to protect it, and Revolve could not reasonably have understood otherwise.

93. The implied contracts are further evidenced by Revolve's Privacy Policy, which describes the limited circumstances in which Revolve will disclose customer information, none of which includes disclosure to an unauthorized actor.

94. Plaintiffs and Class Members fully performed their obligations under the implied contracts, including by paying for the products they purchased.

95. Revolve breached the implied contracts by failing to safeguard the Private Information of Plaintiffs and Class Members and by failing to provide timely and adequate notice of the Data Breach.

96. As a direct and proximate result of Revolve's breaches, Plaintiffs and Class Members have suffered the injuries described above, including the loss of the benefit of their bargain, and are entitled to actual, consequential, and nominal damages in an amount to be proven at trial.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Illinois Subclass)

97. Plaintiffs repeat and reallege paragraphs 1 through 78 as if fully set forth herein.

98. By collecting the payment card data of Plaintiffs and Class Members, and by retaining custody of that data after their purchases were complete, Revolve undertook to act as the guardian of their Private Information. Plaintiffs and Class Members placed their trust and confidence in Revolve, and Revolve, which alone controlled the security of its systems, held a position of superiority and influence with respect to that information.

99. Revolve thereby became a fiduciary with respect to the Private Information entrusted to it, and owed Plaintiffs and Class Members duties to act for their benefit in safeguarding that information, to notify them promptly and fully of any compromise, and to maintain complete and accurate records of what information it stored and where.

100. Revolve breached its fiduciary duties by failing to protect the systems containing the Private Information of Plaintiffs and Class Members, and by failing to diligently discover, investigate, and give notice of the Data Breach within a reasonable time.

101. As a direct and proximate result of Revolve's breaches of fiduciary duty, Plaintiffs and Class Members have suffered the injuries described above and are entitled to damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Illinois Subclass)

102. Plaintiffs repeat and reallege paragraphs 1 through 78 as if fully set forth herein.

103. This claim is pleaded in the alternative to Count II, to the extent the Court finds that no contract governs the subject matter of this dispute.

104. Plaintiffs and Class Members conferred benefits on Revolve. They paid Revolve for its products, and they provided Revolve with their Private Information, including payment card data that Revolve retained for its own commercial purposes.

105. Revolve knew of and accepted those benefits. A portion of the payments Revolve received was, or should have been, used to pay for reasonable data security.

106. Revolve enriched itself by saving the costs it reasonably should have spent on data security measures adequate to protect the Private Information of Plaintiffs and Class Members. Plaintiffs and Class Members suffered as a direct and proximate result.

107. Had Plaintiffs and Class Members known that Revolve would not adequately secure their Private Information, they would not have provided their payment card information to Revolve and would not have purchased from Revolve on the same terms.

108. Under these circumstances, it would violate fundamental principles of justice, equity, and good conscience for Revolve to retain the benefits conferred on it.

109. Revolve should be compelled to disgorge into a common fund, for the benefit of Plaintiffs and Class Members, the proceeds it unjustly retained, and to make restitution.

COUNT V
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS 505/1, *ET SEQ.*
(On Behalf of Plaintiffs and the Illinois Subclass)

110. Plaintiffs repeat and reallege paragraphs 1 through 78 as if fully set forth herein.

111. Plaintiffs and the members of the Illinois Subclass are "consumers" within the meaning of 815 ILCS 505/1(e), and Revolve's sale of merchandise to them constitutes "trade" and "commerce" within the meaning of 815 ILCS 505/1(f).

112. The Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA") prohibits unfair or deceptive acts or practices in the conduct of any trade or commerce, including the concealment, suppression, or omission of any material fact with the intent that others rely on it. 815 ILCS 505/2.

113. Revolve is a "data collector" within the meaning of the Illinois Personal Information Protection Act ("PIPA"), 815 ILCS 530/5, because it handles, collects, and otherwise deals with nonpublic personal information.

114. PIPA requires a data collector that owns or licenses, or maintains or stores, records that contain personal information concerning an Illinois resident to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. 815 ILCS 530/45(a). PIPA also requires a data collector that owns or licenses personal information concerning an Illinois resident to notify the resident of a breach in the most expedient time possible and without unreasonable delay. 815 ILCS 530/10(a). Revolve owns or licenses the Private Information it collects from its customers.

115. The data taken in the Data Breach is "personal information" within the meaning of 815 ILCS 530/5, because it consists of an individual's name in combination with a credit or debit card number. Upon information and belief, that data was not encrypted or redacted, or the means

of reading it were acquired in the Data Breach, because Revolve has acknowledged that the unauthorized actor may have obtained its customers' card numbers and expiration dates.

116. Revolve violated PIPA by failing to implement and maintain reasonable security measures to protect the Private Information of Plaintiffs and the Illinois Subclass, and by waiting approximately thirty days after determining that payment card data was involved, and forty-eight days after the intrusion, to begin notifying them.

117. A violation of PIPA constitutes an unlawful practice under ICFA. 815 ILCS 530/20.

118. Independently of PIPA, Revolve engaged in unfair acts and practices in violation of ICFA by:

(a) failing to implement and maintain reasonable security measures for the payment card data it collected from its customers and stored;

(b) omitting and failing to disclose to its customers the material fact that its security measures were inadequate to protect stored payment card data, with the intent that customers rely on that omission in providing their payment card information and making purchases; and

(c) failing to provide timely and adequate notice of the Data Breach.

119. Revolve's practices offend the public policy expressed in PIPA and in Section 5 of the FTC Act, are immoral, unethical, oppressive, and unscrupulous, and caused substantial injury to consumers that consumers could not reasonably have avoided and that is not outweighed by any countervailing benefit to consumers or competition.

120. Revolve's unfair and unlawful practices occurred in the course of trade and commerce and were directed to consumers in Illinois, including Plaintiffs, who provided their Private Information to Revolve, and received and paid for Revolve's products, in Illinois.

121. As a direct and proximate result of Revolve's violations of ICFA, Plaintiffs and the members of the Illinois Subclass suffered actual damage, including the loss of the benefit of their bargain, and the time and expense of responding to the Data Breach.

122. Plaintiffs and the Illinois Subclass seek actual damages, punitive damages, injunctive relief, and reasonable attorney's fees and costs under 815 ILCS 505/10a.

COUNT VI
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200, *ET SEQ.*
(On Behalf of Plaintiffs and the Nationwide Class)

123. Plaintiffs repeat and reallege paragraphs 1 through 78 as if fully set forth herein.

124. Revolve is a "person" within the meaning of Cal. Bus. & Prof. Code § 17201.

125. The California Unfair Competition Law ("UCL") applies to Revolve's conduct toward Plaintiffs and the Nationwide Class because that conduct and the security failures emanated from California. Revolve is headquartered in Cerritos, California. Upon information and belief, Revolve's decisions concerning the collection, storage, and security of customer payment data, its oversight of the systems on which that data was stored, its investigation of the Data Breach, and its decisions concerning the timing and content of its notices were all made in and directed from California.

126. Revolve engaged in unlawful business practices within the meaning of the UCL by violating Section 5 of the FTC Act, 15 U.S.C. § 45, as described above.

127. Revolve engaged in unfair business practices within the meaning of the UCL by failing to implement and maintain reasonable security measures for stored payment card data and by delaying notice of the Data Breach. That conduct is contrary to the legislatively declared policies of California and of the United States favoring the protection of consumers' personal information, is immoral, unethical, oppressive, and unscrupulous, and caused substantial injury to

consumers that they could not reasonably have avoided and that is not outweighed by any countervailing benefit.

128. As a direct and proximate result of Revolve's unlawful and unfair business practices, Plaintiffs and the Nationwide Class suffered injury in fact and lost money or property, including the portion of the price they paid to Revolve that should have been devoted to adequate data security.

129. Plaintiffs and the Nationwide Class seek restitution and injunctive relief under Cal. Bus. & Prof. Code § 17203. To the extent this Count seeks equitable relief, it is pleaded in the alternative to Plaintiffs' claims for damages. Damages alone cannot remedy the continuing risk posed by Revolve's retention of Plaintiffs' and Class Members' Private Information under inadequate security.

COUNT VII

DECLARATORY AND INJUNCTIVE RELIEF, 28 U.S.C. § 2201

(On Behalf of Plaintiffs and the Nationwide Class)

130. Plaintiffs repeat and reallege paragraphs 1 through 78 as if fully set forth herein.

131. An actual controversy exists between Plaintiffs and the Class, on the one hand, and Revolve, on the other, concerning Revolve's duties to safeguard the Private Information that remains in its possession and the adequacy of its present security measures.

132. Revolve continues to hold the Private Information of Plaintiffs and Class Members. In its Form 8-K, Revolve stated only that it is working to identify and implement enhanced security measures. It has not stated that any such measures are in place, has not disclosed what they are, and has not stated whether stored payment card numbers are now rendered unreadable. Plaintiffs and Class Members therefore remain at risk of a further compromise of their Private Information.

133. Plaintiffs seek a declaration that Revolve owed and continues to owe a legal duty to secure the Private Information of Plaintiffs and Class Members, and that Revolve breached that duty.

134. Plaintiffs further seek injunctive relief requiring Revolve to: (i) render all stored payment card data unreadable through strong encryption or tokenization; (ii) implement controls to detect and block automated extraction of customer data; (iii) delete payment card data it no longer has a legitimate business need to retain; (iv) submit to periodic independent audits of its data security; and (v) provide credit monitoring and identity theft protection services to Plaintiffs and Class Members at its own expense.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, Jennifer Simoni and Alexandru Sarca, individually and on behalf of all others similarly situated, respectfully request that this Court enter judgment in their favor and against Defendant, Revolve Group, Inc., as follows:

A. Certifying this action as a class action under Federal Rule of Civil Procedure 23, appointing Plaintiffs as class representatives, and appointing their counsel as class counsel;

B. Declaring that Defendant's conduct violated the laws set forth above;

C. Awarding Plaintiffs and Class Members actual, consequential, statutory, punitive, and nominal damages, as allowed by law, in an amount to be determined at trial;

D. Awarding restitution and disgorgement of the amounts by which Defendant was unjustly enriched;

E. Awarding the declaratory and injunctive relief described above;

F. Awarding pre-judgment and post-judgment interest as allowed by law;

G. Awarding reasonable attorney's fees, costs, and expenses, and service awards to Plaintiffs, as allowed by law; and

H. Granting such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

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

Dated: November 12, 2026

Respectfully submitted,

s/Bogdan Enica
Bogdan Enica, Esq.
Access Law Group
20283 State Rd. 7
Boca Raton, FL 33498
Telephone: (305) 306-4989
Email: bogdan@accesslaw.us

Dragos Butucea-Boscoianu, Esq.
Access Law Group
1480 Renaissance Dr., Suite 308
Park Ridge, IL 60068
Telephone: (312) 880-7279
Email: drey@accesslaw.us

Counsel for Plaintiffs and the Putative Class