NO

EXHIBITS

CASE NO. 2018CH12352

DATE: 10/2/2018

CASE TYPE: Class Action

PAGE COUNT: 14

CASE NOTE

12-Person Jury

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

SHANICE KLOSS, individually and on behalf of similarly situated individuals, *Plaintiff,* v. EVENTBRITE, INC., d/b/a TICKETFLY, a Delaware corporation, *Defendant.*	No. 2018CH12352 Hon. **Jury Demanded**

CLASS ACTION COMPLAINT & JURY DEMAND

Plaintiff, Shanice Kloss ("Plaintiff"), individually and on behalf of a class of similarly situated persons, brings this Class Action Complaint against Defendant Eventbrite Inc., d/b/a Ticketfly ("Defendant" or "Eventbrite"), as a result of its conduct concerning a recent data breach ("Data Breach" or "Data Hack") that compromised private personal information of the Plaintiff and other members of the putative class due to Defendant's failure to implement a reasonably adequate cybersecurity prevention, detection, and response protocol. Plaintiff alleges as follows based on personal knowledge as to her own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by her attorneys.

INTRODUCTION

1. On or before May 30, 2018, Eventbrite was the target of a Data Hack on its information technology ("IT") systems.

2. This Data Breach resulted in unauthorized outside parties gaining access to Eventbrite's customers' sensitive and confidential personal information, including their names, home and business addresses, phone numbers, email addresses, and password values ("PII"). Despite the fact that Eventbrite was storing sensitive information that it knew was of value to, and

vulnerable to, cyber attackers, Eventbrite failed to take basic security precautions that could have prevented the disclosure of its customers' PII.

3. Eventbrite's lax cybersecurity procedures allowed hackers to obtain access to Plaintiff's and other customers' PII. This PII should have been secured by adequate levels of protection and should not have been susceptible to unauthorized access via the ransomware attack employed in the subject Data Breach.

4. In a ransomware attack, hackers exploit vulnerabilities in an organization's administrative, technical, and/or physical cybersecurity safeguards to install damaging software, *i.e.* malware, onto the organization's IT systems, which may disable the entire network, extract confidential data, or accomplish other nefarious objectives. The hackers then demand a ransom from the target in exchange for removing the malware.

5. Defendant was subject to such a ransomware attack, *i.e.* the Data Hack, and failed to prevent, detect, or otherwise act in a reasonable manner or within a reasonable time, resulting in Plaintiff and other employees' PII being compromised.

6. To this day, Defendant has failed to notify Plaintiff that her PII was compromised in the Data Breach. On information and belief, Defendant has failed to implement any breach notification process *whatsoever* following the Data Breach.

PARTIES

7. Defendant Eventbrite, Inc., is a Delaware Corporation that is transacting business in Cook County, Illinois and maintains its headquarters in California. Defendant Eventbrite transacts business in Illinois under the d/b/a Ticketfly.

8. At all relevant times, Plaintiff Shanice Kloss has been a resident and citizen of the State of Illinois.

JURISDICTION AND VENUE

9. This Court may assert personal jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 in accordance with the Illinois Constitution and the Constitution of the United States because Defendant is doing business within this State and because Plaintiff's claims arise out of Defendant's unlawful in-state actions, as Plaintiff used Defendant's services in Illinois, and Defendant failed to take reasonable precautions to guard against, respond to, and detect cyberattacks in this State.

10. Venue is proper in Cook County pursuant to 735 ILCS 5/2-101, because Defendant is doing business in Cook County and, thus, resides there under § 2-102, and because Plaintiff purchased her event tickets from Defendant in Cook County.

FACTS SPECIFIC TO PLAINTIFF

11. On or around May 30, 2018, Defendant was the target of a Data Hack when third-party hackers ("Hackers") employed a ransomware attack on its IT systems. Defendant was not able to thwart Data Hack, resulting in exposure of the PII of over twenty-five million (25,000,000) of its customers ending up in the hands of criminals. [1]

12. On information and belief, Eventbrite was notified by the Hackers prior to the Data Hack that its IT systems contained a vulnerability. Nonetheless, Eventbrite failed to take reasonable measures following such communication to either discover and mitigate the vulnerability or follow-up with the source of the communication.[2]

[1] <https://motherboard.vice.com/en_us/article/j5kd4b/ticketfly-hack-breach-26-million-users-emails-home-addresses> (last accessed September 30, 2018).
[2] *Id.*

13. On or around May 31, 2018, the Hackers briefly defaced Eventbrite's website while simultaneously releasing the PII of millions of Eventbrite customers to the public domain. The Data Hack resulted in the shutdown of Eventbrite's IT systems for a number of days.[3]

14. Despite the severity of the Data Breach, Eventbrite failed to reasonably implement a breach notification protocol. Aside from a passive support page[4] and a single Tweet[5] on social media, Eventbrite failed to take measures to alert Plaintiff that her PII had been compromised in the Data Breach.

15. It was not until September 13, 2018, after coming across Eventbrite's Tweet from June 6, 2018 at 11:50 p.m., did Plaintiff learn of the Data Breach.

16. Prior to learning of the Data Hack, Plaintiff used Eventbrite's ticket-purchasing service multiple times using the same email address, "s.kloss21@gmail.com," with each purchase.

17. Upon learning of the Data Breach, Plaintiff utilized a forensic online tool[6] developed by a non-profit organization to enable users to determine if their information was included in a given breach incident. Here, when Plaintiff inputted her email address into the tool, she received confirmation that her PII had been exposed in the subject Eventbrite Data Breach.

18. Defendant's failure to implement a reasonable cybersecurity protocol that included adequate technical, administrative, and physical controls allowed the Hackers to access its IT system, and ultimately, directly access Plaintiff's and other customers' PII. For example, an adequate intrusion detection and prevention system would have alerted Eventbrite to the presence of hackers, administrative controls would have prepared Eventbrite's staff to mitigate the

---

[3] *Id.*
[4] <https://support.ticketfly.com/s/article/41507> (last accessed September 30, 2018).
[5] <https://twitter.com/ticketfly/status/1004616518884192256> (last accessed September 30, 2018).
[6] <https://haveibeenpwned.com> (last accessed and cross-checked with subject email address on September 30, 2018).

ransomware attack, and technical measures such as adequate firewalls would have prevented access to hashed password values.

19. Notably, Defendant not only failed to protect Plaintiff's and other customers' PII, but also failed to inform them of the Data Breach in a reasonable manner and without undue delay. Without identifying any justification, and in violation of the law, Defendant failed to promptly and adequately notify Plaintiff of the Data Breach.

20. Given the current prevalence of cybersecurity awareness, especially in light of constant, high profile data breaches, Defendant knew of the risks inherent in capturing, storing, and using the PII of its customers and the consequences of the exposure of such PII to unauthorized third parties, as well as the importance of promptly notifying affected parties in the event of a breach incident.

21. Had Defendant informed Plaintiff of the Data Breach within a reasonable period of time as required by law and/or through a reasonable manner and medium, Plaintiff and the other members of the putative class would have been able to take actions to protect their identities, accounts, and other potential targets from further misuse. Instead Defendant let its customers languish in ignorance as to the real risk of irreversible privacy harms presented by the unauthorized parties who had gained access to their PII.

22. Plaintiff believed that Defendant would take reasonable measures to secure her PII. Had Plaintiff known that Defendant would fail to take reasonable safeguards to protect and secure her PII, she would not have agreed to purchase tickets through Defendant, or she would have at least acted differently upon weighing the risk in having her PII left vulnerable to attack.

23. Defendant's failure to comply with reasonable data security standards provided Defendant a benefit in the form of saving on the costs of compliance, but at the expense and severe

detriment of Defendant's own customers, including Plaintiff, whose PII has been exposed in the Data Breach or otherwise placed at serious and ongoing risk of imminent misuse, fraudulent charges, and identity theft.

24. Since recently becoming aware of the Data Breach, Plaintiff has taken time and effort to mitigate her risk of identity theft, including monitoring her credit and other financial information to guard against fraudulent attempts to open credit cards or other financial accounts in her name.

25. Plaintiff has also been harmed by having her PII compromised and faces the imminent and impending threat of future additional harm from the increased threat of identity theft and fraud due to her PII being sold, misappropriated, or otherwise misused by unknown parties.

26. Plaintiff has also experienced mental anguish as a result of the Data Breach. For example, she experiences anxiety and anguish when thinking about what would happen if her identity is stolen as a result of the Data Breach; when wondering how long and to how many parties her PII was exposed before the Data Breach was even discovered by Defendant; and when she thinks about the fact that Defendant was aware of the Data Breach and actively decided to keep her and the other victims of the Data Breach ignorant of the fact that their PII had been compromised.

27. The Data Breach was caused and enabled by Defendant's knowing violation of its obligations to abide by adequate practices and industry standards in protecting customers' PII. Eventbrite wholly failed to comply with reasonable cybersecurity standards and allowed its customers' PII to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Data Breach.

28. Defendant also avoided the cost of notifying, individually, over twenty-five million (25,000,000) of its customers, including Plaintiff.

CLASS ALLEGATIONS

29. Plaintiff brings Counts I through IV, as set forth below, on behalf of herself and a Class and Subclass (together, the "Class") of similarly situated individuals pursuant to 735 ILCS § 5/2-801. The Class and Subclass are defined as follows:

> **Class:** All persons whose Personal Information was in the possession of Defendant, or any of its subsidiaries, at any point during the Data Breach.
>
> **Illinois Subclass:** All Illinois residents whose Personal Information was in the possession of Defendant, or any of its subsidiaries, at any point during the Data Breach.

30. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant; and any immediate family member of such officer or director.

31. Upon information and belief, there are over twenty-five million (25,000,000) members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of Class members is currently unknown Plaintiff, the members can easily be ascertained through Defendant's records and with the help of third-party forensic investigators Defendant claims to be working with.

32. Plaintiff's claims are typical of the claims of the Class members she seeks to represent because the factual and legal bases of Defendant's liability to Plaintiff and the other Class members are the same and because Defendant's conduct has resulted in similar injuries to Plaintiff and to the Class members. As alleged herein, Plaintiff and the other Class members have all suffered damages as a result of Defendant's failure to maintain reasonable security safeguards with respect to its handling and storage of employees' sensitive PII.

33. There are many questions of law and fact common to the claims of Plaintiff and the other Class members, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant adequately safeguarded Plaintiff and the Class members' PII;

b. Whether Plaintiff and the Class members were notified of the Data **Breach** within a reasonable period of time and through a reasonable method;

c. Whether Defendant willfully, recklessly, and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class members' PII;

d. Whether there was an unauthorized disclosure of the Class members' PII;

e. Whether implied or express contracts existed between Defendant and the Class members;

f. Whether Plaintiff and the Class members sustained damages as a result of Defendant's failure to adequately safeguard their PII;

g. Whether Defendant's PII storage and protection protocols and procedures were reasonable under industry standards;

h. Whether Defendant's cybersecurity prevention, detection, and notification protocols were reasonable under industry standards;

i. Whether Defendant misrepresented the safety and security of the Class members' PII maintained by Defendant;

j. When Defendant became aware of the unauthorized access to Plaintiff's and the Class members' PII;

k. Whether Defendant's conduct violated the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*; and

34. Absent a class action, most Class members would find the cost of litigating their claims to be prohibitively expensive and would have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation

in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

35. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class she seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the other Class members and have the financial resources to do so. Neither Plaintiff nor her counsel have any interest adverse to those of the other members of the Class.

36. Defendant has acted and failed to act on grounds generally applicable to the Plaintiff and the other Class members, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

COUNT I
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*
(On behalf of Plaintiff and the Illinois Subclass)

37. Plaintiff realleges and incorporates by reference the foregoing allegations as if fully set forth herein.

38. Pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq.*, Defendant was required to implement and maintain reasonable security measures to protect the Plaintiff's and Illinois Subclass members' PII, and to notify them regarding any unauthorized disclosure in the most expedient time possible and without unreasonable delay.

39. Defendant's unlawful conduct alleged herein in failing to safeguard its customers' PII, and subsequent failure to timely notify its customers that such PII had been compromised, constitute violations of the Illinois Personal Information Protection Act.

40. Pursuant to Section 530/20 of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.* ("ICFA"), a violation of the Illinois Personal Information Protection Act, as alleged herein, is itself deemed an "unlawful practice" and violation under the ICFA, and Defendant has therefore violated the ICFA.

41. Plaintiff and the Illinois Subclass members have suffered injury in fact and actual damages, as alleged herein, as a result of Defendant's unlawful conduct and violations of the ICFA.

42. Wherefore, Plaintiff prays for relief as set forth below.

COUNT II
Breach of Contract
(On behalf of Plaintiff and the Class)

43. Plaintiff realleges and incorporates by reference the foregoing allegations as if fully set forth herein.

44. Plaintiff and the Class members are parties to express agreements with Defendant whereby Plaintiff and the Class members provide their PII to Defendant in exchange for tickets to events from Defendant, including the provision of reasonable safeguards to prevent the unauthorized disclosure of Plaintiff's and Class members' PII.

45. Defendant's failure to implement an adequate and reasonable data privacy and cybersecurity protocol which included adequate prevention, detection, and notification procedures constitutes a breach of contract.

46. Plaintiff and the Class members would not have provided and entrusted their PII to Defendant as a condition of a sales contract with Defendant, or would have sought other alternatives with Defendant's competitors or otherwise sought concessions, in the absence of an agreement with Defendant to reasonably safeguard their PII and to reasonably notify them of unauthorized disclosures.

47. Plaintiff and the members of the Class fully performed their obligations under their contract for the purchase of tickets from Defendant.

48. Defendant breached the contracts it made with Plaintiff and the Class members by failing to safeguard and protect their PII, and by failing to notify them in a timely and accurate manner that that their PII was compromised as a result of the Data Breach.

49. The damages expressed herein as sustained by Plaintiff and the Class members were the direct and proximate result of Defendant's breaches of contract.

50. Wherefore Plaintiff prays for the relief set forth below.

COUNT III
Breach of Implied Contract
(On behalf of Plaintiff and the Class) (in the alternative to Count II)

51. Plaintiff realleges and incorporates by reference Paragraph 1 through 42 as if fully set forth herein.

52. Plaintiff and the Class members were required to provide Defendant their PII as a condition of the sales of tickets to events. To the extent that it is found that Defendant did not have an express contract with Plaintiff and the Class members, Defendant entered into implied contracts with Plaintiff and the Class members whereby, by virtue of such requirement to provide their PII, Plaintiff and the Class members and Defendant entered into implied contracts whereby Defendant was obligated to take reasonable steps to secure and safeguard such PII and obligated to take reasonable steps following an unauthorized disclosure of the same.

53. Defendant's failure to implement an adequate and reasonable data privacy and cybersecurity protocol which included adequate prevention, detection, and notification procedures constitutes a breach of an implied contract between Defendant and the Class members.

54. Plaintiff and the Class Members would not have provided and entrusted their PII to Defendant in order to obtain their tickets to events from Defendant, and certainly not at the offered

rate, in the absence of an agreement with Defendant to reasonably safeguard their PII and to reasonably notify them of unauthorized disclosures

55. Plaintiff and the members of the Class fully performed their obligations under their implied contracts with Defendant.

56. Defendant breached the implied contracts it made with Plaintiff and the Class members by failing to safeguard and protect their PII, and by failing to notify them in a timely and accurate manner that that their PII was compromised as a result of the Data Breach.

57. The damages expressed herein as sustained by Plaintiff and the Class members were the direct and proximate result of Defendant's breaches of contract.

58. Wherefore Plaintiff prays for the relief set forth below.

COUNT IV
Negligence
(On behalf of Plaintiff and the Class)

59. Plaintiff realleges and incorporates by reference the foregoing allegations as if fully set forth herein.

60. As a condition of employment, Defendant required Plaintiff and Class members to provide their PII.

61. At all relevant times, Defendant had a duty, or assumed a duty, to implement reasonable data privacy and cybersecurity protocol, including adequate prevention, detection, and notification procedures, in order to safeguard the PII of the Plaintiff and the Class members and to prevent the unauthorized access to and disclosures of the same.

62. Defendant breached the aforementioned duty in, including but not limited to, one or more of the following ways:

a. Failing to implement reasonable data privacy and cybersecurity measures to secure its or Plaintiff's and Class members' email accounts, including failing to require adequate multifactor authentication and encryption;

b. Failing to implement a reasonable data privacy and cybersecurity protocol, including adequate procedures for preventing cybersecurity threats and/or detecting such threats in a timely manner;

c. Failing to notify Plaintiff and Class member's that their PPII had been disclosed to nefarious hackers within a reasonable period of time and/or through a reasonable manner or method;

d. Failing to reasonably comply with applicable state and federal law concerning its data privacy and cybersecurity protocol, including the substance and manner of its unreasonably-delayed notification to Plaintiff and Class members concerning the Data Breach; and

e. Otherwise failing to act reasonably under the circumstances and being negligent with regards to its conduct in preventing, detecting, and disclosing the subject Data Breach.

63. Defendant knew, or should have known, that its data privacy and cybersecurity protocol failed to reasonably protect Plaintiff and the Class members' PII.

64. As a direct result of Defendant's aforesaid negligent acts and omissions, Plaintiff and the Class members suffered injury and damages, including the loss of their legally protected interest in the confidentiality and privacy of their PII, the loss of the benefit of their bargain in purchasing tickets from Defendant, pecuniary injury in the form of time and expense to mitigate the disclosure and/or significantly increased risk of exposure of PII to nefarious third parties.

65. Wherefore Plaintiff prays for the relief set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class and Subclass set forth above, respectfully requests the Court order relief and enter judgement against Defendant:

A. Certifying the Class and Subclass identified above and appointing Plaintiff as Class representative and the undersigned counsel as Class counsel;

B. Awarding Plaintiff and the Class and Subclass appropriate relief, including actual, statutory, compensatory, and/or punitive damages;

C. Requiring Defendant to furnish identity fraud monitoring and mitigation services for a reasonable period of time;

D. Granting injunctive relief requiring Defendant to implement commercially reasonable security measures to properly guard against any and all future cyberattacks and to provide prompt, reasonable notification in the event of such an attack;

E. Requiring Defendant to pay Plaintiff's and the Class members' reasonable attorneys' fees, expenses, and costs; and

F. Any such further relief as this Court deems reasonable and just.

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury on all issues so triable.

Dated: October 2, 2018

Respectfully submitted:

SHANICE KLOSS, individually and on behalf of a class of similarly situated individuals

By: /s/ Jad Sheikali
One of Plaintiff's Attorneys

Jad Sheikali
William Kingston
McGUIRE LAW, P.C. (Firm ID 56618)
55 W. Wacker Dr., 9th Fl.
Chicago, IL 60601Tel:
(312) 893-7002
jsheikali@mcgpc.com
wkingston@mcgpc.com

Attorneys for Plaintiff and the Putative Classes