12-Person Jury

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

ERIC KROHM, individually and on behalf of similarly situated individuals, *Plaintiff,* v. EPIC GAMES, INC., a Maryland corporation, *Defendant.*	)	No. 2019CH02032 Hon. **Jury Demanded**

CLASS ACTION COMPLAINT & JURY DEMAND

Plaintiff Eric Krohm ("Plaintiff"), individually and on behalf of a class of similarly situated persons, brings this Class Action Complaint against Epic Games, Inc., ("Defendant" or "Epic Games"), due to its actions and inactions resulting in a catastrophic cybersecurity vulnerability (the "Vulnerability") in Defendant's global-hit video game, Fortnite. Plaintiff alleges as follows based on personal knowledge as to his own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by his attorneys.

INTRODUCTION

1. Defendant Epic Games is the developer of Fortnite, one of the most popular video games ever produced with tens of millions of active monthly users across the globe.

2. Defendant's Fortnite video game generates hundreds of millions of dollars in annual revenue, a significant portion of which is derived from players' in-game purchases of items such as outfits, or "skins," for their in-game characters. In order to make an in-game purchase, Defendant requires players to purchase and utilize its own Fortnite currency called "Vbucks."

3. Around or before November 2018, Defendant became aware of a significant cybersecurity Vulnerability in its Fortnite video game that allowed cyber-criminals and

unauthorized third parties to hijack player accounts and access players' personally identifiable information ("PII"), credit card and payment information ("Payment Information"), and other sensitive data associated with the players' respective accounts.

4. After hijacking a respective player's Fortnite account, a cyber-criminal is then able to make in-game purchases of Vbucks in order to resell the same on the criminal black market.

5. Indeed, Defendant's Vbucks currency is a lucrative item for cybercriminals, and Defendant is fully cognizant of the substantial criminal activity surrounding the fraudulent acquisition of Vbucks.

6. In addition to exposing the PII and Payment Information of Fortnite players, the Vulnerability also enabled unauthorized parties to covertly listen in on the conversations of Fortnite players, many of which are minors, thereby constituting a severe breach of privacy.

7. Even though Defendant knew that it was storing sensitive information which was valuable and vulnerable to cyber attackers, particularly credit card and other Payment Information, Defendant nonetheless failed to take basic security precautions that could have prevented, and certainly at least mitigated, the ramifications of the Vulnerability.

8. Defendant's lax cybersecurity policies and procedures created the Vulnerability that allowed hackers to obtain access to Plaintiff's and other players' PII and Payment Information.

9. Even if certain of the PII and Payment Information made available to hackers as a result of the Vulnerability is not being *presently* used for identity theft, any such PII and Payment Information that has been stored and/or sold for *future* misuse and/or sale are likewise at highly imminent risk of unauthorized disclosure.

10. A lucrative criminal black market exists for PII and, in particular, Payment Information. These items increase in value when associated with active user accounts, which are then subject to highly targeted spam and phishing attack campaigns.

11. Further, even after being made aware of the Vulnerability by a leading cybersecurity research firm, Defendant nonetheless failed to remedy the Vulnerability within a reasonable time and failed to employ a reasonable notification protocol to alert Plaintiff and other Fortnite players of the Vulnerability.

12. To this day, Plaintiff continues to rely on his own time, efforts, and expense to monitor and assess the extent to which his valuable PII and Payment Information was compromised due to the Vulnerability, and Plaintiff will need to continually monitor his accounts into the foreseeable future.

13. On behalf of himself and the proposed Classes defined below, Plaintiff seeks equitable and monetary damages, together with costs and reasonable attorneys' fees

PARTIES

14. Defendant Epic Games, Inc., is a Maryland corporation that is headquartered in North Carolina. Epic Games markets and offers its products and services, including the subject Fortnite video game, throughout Illinois and Cook County.

15. Plaintiff Eric Krohm is a resident and citizen of the State of Illinois.

JURISDICTION AND VENUE

16. 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 intentionally markets its products and

services, including the subject Fortnite video game, in this State to Illinois residents. Tens, if not hundreds, of thousands of Illinois residents play Defendant's Fortnite game on a regular basis.

17. Venue is proper in Cook County pursuant to 735 ILCS 5/2-101, because Defendant is doing extensive business throughout Cook County and because the transaction which forms the primary basis for this lawsuit occurred in Cook County.

FACTS SPECIFIC TO PLAINTIFF

18. Defendant Epic Games is the developer of Fortnite, one of the most popular and successful video games in the United States and across the globe.

19. Like millions of other Fortnite players, Plaintiff was required to create an account with Defendant in order to play. Defendant required Plaintiff to provide certain PII in order to create his account, and also enabled and encouraged him to store his Payment Information for future purchases of Vbucks, Defendant's in-game currency for Fortnite which enables players to make in-game purchases.

20. In order to make prospective account holders more comfortable with providing their Payment Information and other PII during the registration process, Defendant expressly promised to maintain appropriate technical safeguards to protect user account holders' PII and Payment Information from accidental, unlawful, or unauthorized destruction, loss, alteration, access, disclosure, or use.

21. Plaintiff entrusted Defendant with his PII and Payment Information with the belief and understanding that Defendant would implement reasonable cybersecurity protocols to protect the same, or at least reasonably notify him of any irregularities. Plaintiff would not have otherwise provided his PII and Payment Information to Defendant.

22. Around or before November 2018, a leading cybersecurity research firm alerted Defendant to the subject Fortnite Vulnerability which allowed cyber-criminals and unauthorized third parties to access and extract PII, Payment Information, and other sensitive data associated with the player accounts.

23. The Vulnerability existed because Defendant failed to implement a basic precautionary technical measure that would have prevented unauthorized third-parties the ability to retrieve and reuse the "security tokens" associated with Plaintiff's and other user's accounts. Once armed with the security token for a given account, a hacker is able to access and utilize every feature of such account, including the ability to make purchases of Defendant's Vbucks currency using the account Payment Information.

24. Such security-token-jacking schemes are increasingly common, and any reasonably-robust cybersecurity and information technology regime must account for the ultimate disposition, including reusability, of security tokens. Defendant has failed in this regard.

25. The Vulnerability allowed unauthorized parties the ability to extract and store players' PII and Payment Information for future misuse and/or resell on the criminal black market. Thus, Plaintiff will need to constantly monitor his PII and Payment Information that has been stored for *future* misuse or sale.

26. Defendant is aware that Vbucks are a lucrative item for cybercriminals and that its players are frequently targeted by hackers and scammers seeking to fraudulently obtain Vbucks, as well as the PII and Payment Information frequently associated with Fortnite player accounts. Notably, Defendant's Fortnite title was the target of a data hack in the summer of 2018 which affected millions of its players' accounts.

27. Despite its awareness that its Fortnite title is constantly the target of hackers, Defendant nonetheless failed to implement reasonable technical measures to detect irregularities in its systems, such as the subject Vulnerability. Rather, a benevolent third-party research firm detected the Vulnerability.

28. The Vulnerability also allowed unauthorized parties the ability to covertly eavesdrop on the in-game conversations between Fortnite players.

29. Defendant's lax cybersecurity policies and procedures created the Vulnerability that allowed hackers to obtain access to Plaintiff's and other players' PII and Payment Information.

30. Defendant also failed to remedy the Vulnerability within a reasonable time after being made aware of its existence and failed to reasonably and timely notify Plaintiff and other affected Fortnite account holders. These failures not only increased the scope of the Vulnerability, but also allowed unauthorized parties additional time to extract and store PII and Payment Information for future misuse and/or sale.

31. For at least several weeks, unauthorized third parties were able to freely access, extract, misuse or sell, or store for future misuse or sale, the PII and Payment Information of millions of Defendant's customers, including Plaintiff.

32. As a result of Defendant's conduct regarding the Vulnerability, Plaintiff faces the certain costs, time, and other palpable expenses associated with continuously monitoring his accounts for the foreseeable future.

33. Despite the severity of the Vulnerability, by failing to take prompt measures to alert Plaintiff and other customers that their PII and Payment Information had been compromised, Defendant exposed consumers to an increased risk of identity theft and other harms.

34. Had Defendant informed Plaintiff of the Vulnerability within a reasonable period as required by law and/or through a reasonable manner and medium, Plaintiff and the other customers would have been able to take actions to protect their identities, credit card and debit accounts, and other potential targets from further or imminently-future misuse. Instead Defendant let its customers languish in ignorance as to the privacy harms presented by the Vulnerability.

35. Defendant's failure to comply with its own express policies and other 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.

36. Since recently becoming aware of the vulnerability, Plaintiff has taken time and effort to mitigate the risk of identity theft, including changing account passwords and constantly expending time, effort, and expense in monitoring credit and other financial information.

37. Defendant itself even recommended that Plaintiff and other Fortnite players "use[] strong passwords," *i.e.* spend additional time and effort (and expense) in securing their accounts.

38. Plaintiff has also been harmed by having his PII and Payment Information compromised and faces the imminent and impending threat of future additional harm from any future misuse or sale of his PII and Payment Information by unknown third parties.

39. Plaintiff also experiences mental anguish as a result of Defendant's Vulnerability exposing or otherwise making freely available his PII and Payment Information to third party hackers. For example, he experiences anxiety and anguish when thinking about what would happen if his identity is stolen as a result of the Vulnerability; when considering that, because his PII and Payment Information may have been stored for future misuse and sale, how he will need to constantly monitor his accounts for the foreseeable future; and when he thinks about the fact that

Defendant was aware of the Vulnerability and actively decided to keep him and the other victims of the Vulnerability in the dark.

40. The Vulnerability was caused and enabled by Defendant's violations of its own express commitments to its customers to implement appropriate technical safeguards, as well as its preexisting obligations to abide by adequate practices and industry standards in protecting customers' PII and Payment Information. Defendant wholly failed to comply with reasonable cybersecurity standards.

CLASS ALLEGATIONS

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

> **Class:** All persons whose PII and/or Payment Information was in the possession of Defendant at any time during the two-month period starting at the beginning of November 2018 through the end of December 2018.
>
> **Illinois Subclass:** All Illinois residents whose PII and/or Payment Information was in the possession of Defendant at any time during the two-month period starting at the beginning of November 2018 through the end of December 2018.

42. 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.

43. Upon information and belief, there are hundreds of thousands, if not millions, of members of the Class, making the Class so numerous that joinder of all members is impracticable. Although the exact number of Class members is currently unknown to Plaintiff, the members can easily be ascertained through Defendant's records.

44. Plaintiff's claims are typical of the claims of the Class members he 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 similar injuries as a result of Defendant's actions and inactions surrounding the subject Vulnerability and exposing their PII and Payment Information.

45. There are many questions of law and fact common to the claims of Plaintiff and the 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 implemented adequate technical, administrative, and physical safeguards to prevent the Vulnerability;

b. Whether Defendant implemented adequate technical, administrative, and physical safeguards to detect the Vulnerability;

c. Whether Defendant implemented adequate technical, administrative, and physical safeguards to reasonably mitigate the Vulnerability;

d. Whether Plaintiff and the Class members were notified of the Vulnerability within a reasonable period of time and through a reasonable method;

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 the Vulnerability;

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; and

k. When/if Defendant completely cured the Vulnerability.

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

47. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class he seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and his 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 his counsel have any interest adverse to those of the other members of the Class.

48. Defendant has acted and failed to act on grounds generally applicable to 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 Subclass)

49. Plaintiff realleges by reference the foregoing allegations as if fully set forth herein.

50. Pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq.* ("PIPA"), Defendant was required to implement and maintain reasonable security measures to protect 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. This duty required Defendant to not only implement reasonable protocols to detect and prevent the Vulnerability, but also to reasonably mitigate the same.

51. Defendant was also obligated under PIPA to notify Plaintiff and the Illinois Subclass of the Vulnerability in the most expedient time possible and without unreasonable delay.

52. Defendant's conduct alleged herein resulting in the Vulnerability, thereby failing to safeguard its customers' PII and Payment Information, and subsequent failure to adequately notify its customers, constitute a violation of PIPA.

53. Pursuant to Section 530/20 of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.* ("ICFA"), Defendant's PIPA violation is itself deemed an "unlawful practice" and a distinct violation under the ICFA.

54. As a result of Defendant's violation of the ICFA vis-à-vis its PIPA violation, Plaintiff and the Illinois Subclass have suffered actual pecuniary and non-pecuniary harms.

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

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

56. Plaintiff realleges by reference the foregoing allegations as if fully set forth herein.

57. Plaintiff and the Class members are parties to express agreements with Defendant whereby Plaintiff and the Class members provide their PII and Payment Information to Defendant in exchange for the ability to play Fortnite, as well as purchase the in-game products and service advertised by Defendant within Fortnite.

58. Such agreement expressly included the provision of reasonable technical safeguards to prevent the unauthorized disclosure of, and reasonable notification for irregularities concerning, Plaintiff's and Class members' PII and Payment Information

59. As alleged herein, Defendant's actions, inactions, and failures concerning its cybersecurity and information technology protocol, as well as its conduct leading up to, surrounding, and following the Vulnerability, constitutes a breach of contract.

60. Plaintiff and the Class members would not have provided and entrusted their PII and Payment Information to Defendant the absence of an agreement with Defendant to reasonably safeguard the same and to reasonably notify them of unauthorized disclosures or irregularities concerning the same.

61. Plaintiff and the members of the Class fully performed their obligations under their respective contracts for the utilization of and purchases associated with Defendant's Fortnite products and services.

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

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

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

64. Plaintiff realleges by reference Paragraph 1 through 47 as if fully set forth herein.

65. Plaintiff and the Class members provided their PII and Payment Information to Defendant in exchange for the ability to play Fortnite and utilize the in-game products and services.

66. To the extent that it is found that Defendant did not have express agreements with Plaintiff and the Class members, Defendant entered into implied contracts with Plaintiff and the Class members. By virtue of the requirement to provide their PII and Payment Information and Defendant's collection, storage, and use of the same, Plaintiff and the Class members and Defendant entered into implied contracts where Defendant was obligated to provide appropriate technical protections and to take reasonable other steps to secure and safeguard such PII and

Payment Information and obligated to take reasonable steps leading up to, surrounding, and following the Vulnerability.

67. As alleged herein, Defendant's actions, inactions, and failures concerning its cybersecurity and information technology protocol, as well as its conduct leading up to, surrounding, and following the Vulnerability, constitutes a breach of contract.

68. Plaintiff and the Class members would not have provided and entrusted their PII and Payment Information to Defendant in the absence of an agreement with Defendant to reasonably safeguard the same and to reasonably notify them of unauthorized disclosures or irregularities concerning the same.

69. Plaintiff and the members of the Class fully performed their obligations under their respective contracts for the utilization of and purchases associated with Defendant's Fortnite products and services.

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

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

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

72. Plaintiff realleges by reference the foregoing allegations as if fully set forth herein.

73. By virtue of enabling Plaintiff and Class members to provide their PII and Payment Information as a condition to utilizing Fortnite's in-game products and services, including Defendant's Vbucks currency, 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 and Payment Information of the Plaintiff and the Class members and to prevent the unauthorized access to and disclosures of the same.

74. As alleged herein, Defendant's actions, inactions, and failures concerning its cybersecurity and information technology protocol, as well as its conduct leading up to, surrounding, and following the Vulnerability, constitutes a breach of such duty.

75. Defendant also breached its duties in one or more of the following ways:

a. Failing to implement reasonable data privacy and cybersecurity measures to secure Plaintiff's and Class members' PII and Payment Information;

b. Failing to implement reasonable policies, procedures, and technical measures to address the disposition and reusability of security tokens;

c. Failing to reasonably notify Plaintiff and Class members that their PII and Payment Information was exposed due to the Vulnerability;

d. Failing to implement reasonable policies, procedures, and technical, administrative, and physical safeguards to detect and analyze irregularities in its information systems, such as the subject Vulnerability; and

e. Otherwise failing to act reasonably under the circumstances and being negligent and careless with regard to its conduct in preventing, detecting, and disclosing the subject Vulnerability.

76. As a direct result of Defendant's aforesaid negligent acts and omissions, Plaintiff and the Class members suffered pecuniary and non-pecuniary injury and damages, including the loss of their legally protected interest in the confidentiality and privacy of their PII and Payment Information and injury in the form of time and expense to mitigate the same.

77. Wherefore, Plaintiff prays for the relief set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself 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, 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 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: February 15, 2019

Respectfully submitted:
ERIC KROHM, individually and on behalf of a class of similarly situated individuals

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

Myles McGuire
Jad Sheikali
Timothy P. Kingsbury
McGuire Law, P.C. (Firm ID 56618)
55 W. Wacker Dr., 9th Fl.
Chicago, IL 60601
(312) 893-7002
mmcguire@mcgpc.com
jsheikali@mcgpc.com
tkingsbury@mcgpc.com

Attorneys for Plaintiff and the Putative Classes