IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

HEBER BRAN, individually and on behalf of all others similarly situated, Plaintiff, v. VTECH ELECTRONICS NORTH AMERICA, L.L.C., a Delaware limited liability company, and VTECH HOLDINGS LIMITED, a Hong Kong company, Defendants.	Case No.: 1:15-cv-10891

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Heber Bran brings this Class Action Complaint and Demand for Jury Trial ("Complaint") against Defendants VTech Electronics North America, L.L.C. ("VTech") and VTech Holdings Limited ("VTech Holdings") because of their failure to safeguard the sensitive information of millions of its customers, including the sensitive information of millions of children. Plaintiff alleges as follows upon personal knowledge as to himself and his own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

NATURE OF THE ACTION

1. VTech Holdings is the leading manufacturer of electronic toys for children. VTech Holdings' flagship electronic devices, including its "kid-friendly" tablet computers, allow children to browse the Internet, communicate with other digital devices, and download education-related software applications, e-books, learning games, and other educational content. VTech distributes VTech Holdings' devices to consumers throughout the United States.

2. In order to use VTech devices, parents are required to register for an account with VTech and provide it with, among other things, their names, home addresses, email addresses, and passwords (collectively, their "Sensitive Information"). Children can then create their own profiles for the devices by providing VTech with their names, passwords, dates of birth, gender, and, in certain circumstances, photographs. During this process, VTech promises to protect and keep their information secure.

3. When consumers like Plaintiff Bran purchase VTech's learning devices and related services (like e-books, games, or other learning applications for use on its devices), they do not merely purchase the product or service. Rather, they purchase an indivisible bundle of goods and services that includes not only the good or service but also data privacy and security.

4. Unfortunately, VTech did not—despite its customers' expectations and its own promises—utilize industry-standard data security measures to protect its customers' Sensitive Information. Ultimately, that failure led to the theft of the private information of millions of Americans, including millions of children twelve years old and younger. Specifically, on November 24, 2015, VTech discovered that its databases had been hacked and that nearly five million parent accounts and over six million related children's profiles had been compromised. Even worse, according to recent reports, children's communication logs and profile photos were also compromised.

5. Had VTech informed consumers that it would use inadequate security measures, customers (like Plaintiff Bran) would not have purchased its products or services.

6. Some security threats are unavoidable in a rapidly-developing technological environment, but VTech's failure to implement industry-standard data security protocols jeopardized its customers' Sensitive Information, fell far short of its promises, and diminished

the value of the products and services it provided. In other words, because VTech failed to disclose its gross security inadequacies to Plaintiff and a class of consumers defined below, it delivered to them fundamentally less useful and less valuable products and services than the ones they paid for.

7. Accordingly, Plaintiff Bran brings suit on behalf of himself and all others similarly situated to seek redress for VTech's unlawful conduct.

PARTIES

8. Plaintiff Heber Bran is a natural person and citizen of the Commonwealth of Massachusetts.

9. Defendant VTech Electronics North America, L.L.C. is a Delaware limited liability company with its headquarters located at 1156 West Shure Drive, Suite 200, Arlington Heights, Illinois 60004. VTech Electronics North America, L.L.C. is registered with the Illinois Secretary of State as entity number 00195197. VTech Electronics North America, L.L.C. conducts business throughout this District, the State of Illinois, and the United States.

10. Defendant VTech Holdings Limited is a Hong Kong company with its headquarters located at 23/F, Tai Ping Industrial Centre, Block 1, 57 Ting Kok Road, Tai Po, New Territories, Hong Kong. VTech Holdings Limited conducts business throughout this District, the State of Illinois, and the United States.

JURISDICTION AND VENUE

11. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because (a) at least one Class member is a citizen of a different state than Defendants, (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and (c) none of the exceptions under that subsection apply to this action.

12. This Court has personal jurisdiction over Defendants because they conduct significant business in this District, and the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated from this District. Additionally, this Court has personal jurisdiction over Defendant VTech Electronics North America, L.L.C. because it is headquartered in this District.

13. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to the Complaint occurred in this District and because Defendant VTech Electronics North America, L.L.C. maintains its headquarters and principal place of business in this District.

CHOICE OF LAW

14. Illinois law governs the substantive legal issues in the instant matter. VTech's operative Terms and Conditions state that its terms shall be governed and construed in accordance with the laws of the State of Illinois and that any disputes arising out of, or relating to, its terms or use of its services will be subject to the exclusive jurisdiction of the courts located within Cook County in the State of Illinois.

COMMON FACTUAL ALLEGATIONS

I. An Overview Of VTech.

15. VTech claims to be the world's leading manufacturer of children's "electronic learning products."[1] Several of VTech's flagship products, such as its "kid-friendly" InnoTab tablet computers, allow children to purchase and download education-related applications or content to their devices through its proprietary software application called the Learning Lodge.

16. Before using these products or accessing its Learning Lodge, parents must first

[1] *VTech Corporate Profile*, VTech Holdings Limited, https://www.vtech.com/en/about-us/ (last visited Dec. 2, 2015).

register for an account with VTech and provide it with their own Sensitive Information. Parents can then have their children create profiles on these devices by providing VTech with their own Sensitive Information: names, dates of birth, gender, and passwords.

17. As discussed in the next Section, VTech recognizes the sensitivity of this information and, in light of that, promises to protect and keep it secure. As such, when consumers (like Plaintiff Bran) purchase products or services from VTech, they not only purchase the products or services themselves, but also pay for VTech's promise to protect and keep its customers' Sensitive Information secure. If VTech had revealed to its customers that it would not protect their or their children's Sensitive Information, they would not have purchased or used its products or services.

II. VTech's Customers Justifiably Expected That Their Sensitive Information Would Be Secured.

18. Parents purchased VTech's learning tablets because they provided children with a supposedly safe way to connect to the Internet and access VTech's education-related content, and also because they expected that VTech, as the leading children's electronics manufacturer, would protect the Sensitive Information it collected from them and their children. These minimal expectations are both reasonable and justified, especially as applied to VTech. That is because VTech itself created these expectations by promising parents that it would, at a minimum, protect their and their children's Sensitive Information.

19. In order to use its devices, parents are required to register for an account with VTech and provide it with their Sensitive Information. Children can then create their own profiles for these devices by providing VTech with their Sensitive Information, including their names, passwords, dates of birth, gender, and, in certain circumstances, photographs.

20. During this process, parents must affirmatively agree to VTech's Terms and

Conditions.[2] VTech prominently displays its data security promises in its terms, including that it is committed "to protect[ing parents' and children's] privacy and personal information" and "uses reasonable precautions to keep [their] personal information secure."[3] VTech's Privacy Policy, which is incorporated into its terms, goes on to say:

> The security of your personal information is important to VTech, and VTech is committed to handling your information carefully. In most cases, if you submit your PII to VTech directly through the Web Services it will be transmitted encrypted to protect your privacy using HTTPS encryption technology. Any Registration Data submitted in conjunction with encrypted PII will also be transmitted encrypted. Further, VTech stores your PII and Registration Data in a database that is not accessible over the Internet.
>
> * * *
>
> [Unless otherwise stated in the Privacy Policy, a]ny information we collect from you about your children is treated and handled in the same manner as the information we collect about you.

21. In light of these representations, VTech knew that parents in the market for "kid-friendly" Internet connected tablets would expect that their information (and, more importantly, their children's information) would be protected using, at a bare minimum, industry standard practices. Unfortunately, and as described below, VTech breached its promises and failed to protect the Sensitive Information it was trusted with.

III. VTech Failed To Deliver The Security That It Promised And Parents Expected.

22. On November 24, 2015, VTech discovered that its databases had been remotely accessed and hacked, and that nearly five million parent accounts and over six million related children's profiles—including Plaintiff Bran's and the Class's Sensitive Information—had been compromised. Worse yet, early reports suggest that children's communication logs and profile

---

[2] If the user does not register for an account with VTech, a substantial portion of the device's functionality is disabled.

[3] The relevant excerpts of VTech's operative Privacy Policy have been reproduced here. The full Privacy Policy can be located on its tablets.

photos were also compromised.

23. According to VTech, it only discovered the breach after receiving an email from a journalist on November 23, 2015 asking about the incident. After receiving that email, VTech conducted an internal investigation, detected some irregular activity on its servers, and then conducted a comprehensive check of the affected services. Only after that did VTech learn that its customers' data (including their Sensitive Information and information concerning their children) was compromised. Put another way, VTech was not even aware its systems had been hacked and its customers' personal information compromised until after it was notified by a third party.

24. According to VTech, hackers were able to access its systems containing millions of parents' and children's extremely Sensitive Information, including photographs and communication logs, because "[r]egretfully[, its] database was not as secure as it should have been."[4] It is important to emphasize that VTech's customer databases *were* remotely accessed, given its explicit promise in its Privacy Policy that it "stores . . . PII and Registration Data in a database that is not accessible over the Internet."[5]

25. VTech recognizes that this breach exposes exposed customers' Sensitive Information to, among other things, an increased risk of misuse by unauthorized third parties (*e.g.*, identity theft) and recommends—through an online statement about the breach published on its website—that affected customers immediately change other online accounts that share the same now-compromised credentials used to register their VTech accounts.

26. In addition to exposing affected customers' Sensitive Information to this

---

[4] *Data Breach On VTech Learning Lodge Update*, VTech Holdings Limited, http://www.vtech.com/en/media/faq-about-data-breach-on-vtech-learning-lodge/ (last visited Dec. 1, 2015).

[5] *See* Note 3, *supra.*

increased risk, the data breach demonstrated that VTech had not been providing its customers with the promised (and paid-for) data security services that VTech set out through its data privacy and security statements.

27. VTech's shoddy data security practices were discussed at length in the first article published about the breach, which included the following:[6]

> [A leading data security researcher] analyzed the data and found 4,833,678 unique email addresses with their corresponding passwords. The passwords were not stored in plaintext, but "hashed" or protected with an algorithm known as MD5, which is considered trivial to break. (If you want to check whether you're among the victims, you can do it on [the researcher's] website Have I Been Pwned.)
>
> Moreover, secret questions used for password or account recovery were also stored in plaintext, meaning attackers could potentially use this information to try and reset the passwords to other accounts belonging to users in the breach—for example, Gmail or even an online banking account.
>
> "That's very negligent," [the researcher] said. "They've obviously done a really bad job at storing passwords."
>
> For [the researcher], however, the most worrisome element of the breach is the fact that it contains data about kids, and that it's possible to link the kids' database back to the parents, making it possible to figure out a kid's full name and home address.
>
> "When it includes their parents as well—along with their home address—and you can link the two and emphatically say 'Here is 9 year old Mary, I know where she lives and I have other personally identifiable information about her parents (including their password and security question),' I start to run out of superlatives to even describe how bad that is," [he] wrote in a blog post he published on Friday.
>
> * * *
>
> According to [the researcher], it appears that parents still can't trust VTech. Apart from the breach, he also found a number of awful security practices during a "cursory review" of how the company handles data on its sites.
>
> [He] said that VTech doesn't use SSL web encryption anywhere, and transmits data such as passwords completely unprotected. (SSL is a technology used to protect data

[6] *One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids | Motherboard*, http://motherboard.vice.com/read/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids (last visited Dec. 3, 2015).

> sent between a user and a website, and it's typically visualized with a green lock on the URL bar.) [He] also found that the company's websites "leak extensive data" from their databases and APIs—so much that an attacker could get a lot of data about the parents or kids just by taking advantage of these flaws.

28. In another article describing the attack, Vice News reported:

> [The hacker] then quickly found out the [VTech] site was vulnerable to the ancient, yet still very effective, hacking technique known as SQL injection.
>
> The hacker then quickly obtained the maximum level or administrative privileges on the server, known as "root" in technical jargon, and realized he could basically do whatever he wanted.
>
> * * *
>
> At that point [the hacker] started poking around, pivoted to other VTech servers, and was able to find some data. At some point, the hacker said, he found the two databases containing the personal data of millions of parents and thousands of children.

29. Based on these reports, it is evident that VTech never implemented the security it promised. Specifically, it has been revealed that:

- Passwords were stored as simple hashes, without "salt";
- Secret questions for password and account recovery were stored in plaintext;
- Children accounts were linked to home addresses and other identifying information;
- VTech did not use encryption in the transmission of collected data (i.e., no SSL);
- VTech did not encrypt stored private communications and pictures;
- VTech's services were susceptible to SQL injection;
- VTech stored customer data in an Internet-accessible database;
- VTech shared and transmitted collected customer data with an unauthorized party (VTech Holdings); and
- VTech did not implement basic user authentication (e.g., allowing anyone "root"

access).

30. Unfortunately, VTech never told consumers that it was not securing parent and children data—it took a massive data breach for that information to come to light.

IV. By Concealing Its Deficient Data Protection Practices From Consumers, VTech Was Able To Both Sell More Of And Command Higher Prices For Its Products and Services.

31. Consumers place value in data privacy and security, and they consider those things when making purchasing decisions.

32. In fact, it is widely accepted that consumers are willing to pay higher prices to do business with merchants who better protect their privacy. Consumer technology markets have likewise demonstrated that consumers value their privacy and security and incorporate data security practices into their purchases. For example, companies have begun providing consumers with "cloaking services" that allow them to browse the Internet anonymously for a fee. Likewise, companies now offer services that, in exchange for a monthly fee, will offer online services designed to protect data privacy.

33. Consumers are especially interested in ensuring the security of their login credentials (*i.e.*, usernames, passwords, and email addresses). This has lead to the development of a market where consumers can buy software and services to securely store and manage their Sensitive Information.

34. Because of the value consumers place on data privacy and security, products and services with better security practices command higher prices than those without. Indeed, if consumers did not value their data security and privacy, profit-seeking corporations (like VTech) would have no reason to tout their privacy and security credentials to current and prospective customers.

35. These value propositions reflect the fact that consumers view technology companies who promise to adequately secure customer data as being far more useful—and valuable—than those with substandard protections.

36. As a result, a technology-related product or service with substandard data security and privacy protections is less useful and valuable than a product or service using adequate security protocols, and is, in reality, a different product and service entirely.

37. And even though consumers will pay a premium for secure products and services, there is no reason that *any* purchasing consumer would assign *any* value to VTech's online products and services at issue here, considering that each (i) was marketed exclusively for children's use (including use that involves the transmission of children's personal information over the Internet, such as names and pictures), (ii) lacked industry standard data security safeguards, and (iii) were not even safeguarded in line with VTech's own Terms and incorporated Privacy Policy.

38. Stated simply, had consumers—and parents, in particular—known the truth about VTech's data security practices—e.g., that it did not use industry standard protections and stored its customers' (and its customers' children's) data in a manner that was accessible via the internet—none would have purchased or chosen to use VTech's products or services.

FACTS SPECIFIC TO PLAINTIFF HEBER BRAN

39. In late 2014, Plaintiff Bran purchased a VTech InnoTab Learning Tablet for his then-five year old child.

40. Before he or his child could use the tablet, Plaintiff Bran was required to register for an account with VTech by providing it with his Sensitive Information, including his name, home address, email address, and password.

41. In addition to providing detailed personal information to VTech, Plaintiff Bran was required to read and agree to VTech's Terms and Conditions, including the data security promises described in Section II above.

42. Plaintiff Bran subsequently purchased education-related software applications, e-books, learning games, or other educational content from VTech's Learning Lodge app store.

43. Thereafter, Plaintiff Bran's child used the tablet and, through such use, submitted Sensitive Information to VTech (e.g., name, birthdate, password, and gender).

44. Because he purchased products and services from a well-known, supposedly reputable children's toy manufacturer, Plaintiff Bran believed that VTech would use reasonable and accepted methods of securing his and his child's Sensitive Information, and VTech confirmed that belief with the representations discussed in Section II.

45. Accordingly, when Bran purchased VTech's InnoTab Learning Tablet and related apps from VTech, he paid for the products, services, and data privacy and security measures, wherein VTech promised to protect his and his child's Sensitive Information.

46. These components—the products, services, and data security—were material parts of his purchase. Thus, without the security protections that VTech promised and that Plaintiff Bran justifiably believed he would receive as part of his purchase (both for himself and for his child), the purchased products and services as a whole were substantially less useful and valuable to him.

47. Had VTech disclosed (before the actual data breach) that it was not actually implementing adequate security protocols, Plaintiff Bran would—through reading VTech's privacy statements or learning through the media—have been aware of VTech's *actual* data security practices.

48. Accordingly, had VTech disclosed its lax security practices prior to his purchase, he would not have purchased the tablet in the first place or would have tried to return it before completing the tablet's registration process.

49. Additionally, Plaintiff Bran took (and continues to take) considerable precautions to protect the unauthorized dissemination of his and his child's Sensitive Information. Unfortunately, as a result of VTech's failure to implement its promised and paid-for security practices, Plaintiff Bran's Sensitive Information was disseminated without his consent and the value of that information was quantifiably reduced.

50. As a result, Plaintiff Bran has suffered damages in (i) an amount equal to the difference in value between the products and services paid for and the products and services delivered, and (ii) the value of his personal data and lost property in the form of his breached and compromised Sensitive Information. Additionally, as a result of VTech's data breach, Plaintiff Bran and his child are now at an increased risk that unauthorized third parties will misuse their Sensitive Information.

CLASS ALLEGATIONS

51. **Class Definitions**: Plaintiff Bran brings this action pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2), and (b)(3) on behalf of himself and a class and subclass of similarly situated individuals, defined as follows:

> **Class**: All individuals in the United States whose Sensitive Information was compromised during the data breach announced by VTech in or around November 2015.
>
> **Overpayment Subclass**: All Class members who purchased (i) VTech products that connect to its Learning Lodge app store and/or (ii) apps, games, e-books, or other content from VTech's Learning Lodge.

Excluded from the Class and Overpayment Subclass (collectively referred to as the "Class",

unless otherwise indicated) are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and their current or former employees, officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; (6) the legal representatives, successors, and assigns of any such excluded persons; and (7) any individual who contributed to the unauthorized access of Defendants' database.

52. **Numerosity**: The exact size of the Class is unknown and not available to Plaintiff at this time, but it is clear that individual joinder is impracticable. On information and belief, there are millions of people in the Class, making joinder of each individual member impracticable. Ultimately, members of the Class will be easily identified through Defendants' records.

53. **Commonality and Predominance**: Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual members:

(a) whether Defendants failed to protect and keep customers' Sensitive Information secure, as promised;

(b) whether Defendants' conduct described herein constitutes a violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505;

(c) whether Defendants' conduct described herein constitutes a breach of contract; and

(d) whether Defendants were unjustly enriched through their unlawful conduct described herein.

54. **Typicality**: Plaintiff's claims are typical of the claims of the other members of the Class. Plaintiff and members of the Class sustained damages as a result of Defendants' uniform wrongful conduct during transactions with Plaintiff and the Class.

55. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex class actions. Plaintiff has no interest antagonistic to those of the Class, and Defendants have no defenses unique to Plaintiff.

56. **Policies Generally Applicable to the Class**: This class action is appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward members of the Class, and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' practices challenged herein apply to and affect members of the Class uniformly, and Plaintiff's challenge of those practices hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

57. **Superiority**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy given that joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective

relief from Defendants' misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort and expense will be fostered and uniformity of decisions ensured.

FIRST CAUSE OF ACTION
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
815 ILCS 505
(On behalf of Plaintiff and the Overpayment Subclass)

58. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

59. The Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA") (815 ILCS §§ 505/1, *et seq.*) protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

60. The ICFA prohibits any unlawful, unfair, or fraudulent business acts or practices including the employment of any deception, fraud, false pretense, false promise, false advertising, misrepresentation, or the concealment, suppression, or omission of any material fact.

61. The ICFA applies to Defendants' actions and conduct as described herein because it protects consumers in transactions that are intended to result, or which have resulted, in the sale of goods or services.

62. Defendants are each a "person" as defined under section 505/1(c) of the ICFA.

63. Plaintiff and each member of the Overpayment Subclass is a "consumer" as defined under section 505/1(e) of the ICFA.

64. Defendants' tablets are "merchandise" within the meaning of section 505/1(b) and the sale of their tablets is considered "trade" or "commerce" under the ICFA.

65. Defendants violated the ICFA by omitting material facts about their tablets. Specifically, Defendants failed to disclose that they were:

- Storing passwords as simple hashes without salt;
- Storing secret questions for password and account recovery in plaintext;
- Linking children's accounts to home address and other identifying information;
- Failing to use encryption for the transmission of collected data (i.e., no SSL);
- Failing to encrypted stored data;
- Failing to protect against SQL injection;
- Storing customer data in an Internet-accessible database;
- Sharing and transmitting collected customer data with an unauthorized party (VTech Holdings); and
- Failing to implement basic user authentication (e.g., by limiting who can gain "root" access).

66. Defendants were aware or should have been aware that they were not implementing security protections as outlined above.

67. Defendants omitted the material fact that their tablets do not offer any security protections in both their advertising and warnings on the tablet's physical packaging.

68. Defendants knew and were aware that if they prominently disclosed on the tablet's physical packaging that they do not offer any data security protections, they would have to sell the tablets at a substantially lower price.

69. Defendants created their advertisements and marketing materials with the intent that Plaintiff and the Overpayment Subclass members would rely on the information provided, but omitted the material fact that the tablets do not offer adequate security protections.

70. Had Defendants not engaged in the deceptive omission of material facts described above, Plaintiff and the members of the Overpayment Subclass would have been presented with an informed choice as to whether or not to buy the tablets and would have also been presented with the disclosures necessary to modify their use of (and their children's use of) the tablets to avoid a breach of their privacy.

71. Defendants' material omissions to Plaintiff and members of the Overpayment Subclass constitute unfair and deceptive acts or practices in violation of the ICFA. Plaintiff would not have purchased the VTech tablets if the Defendants disclosed that they were not secure.

72. Plaintiff and the Overpayment Subclass members were damaged by Defendants' conduct directed towards consumers. Defendants chose not to disclose that their tablets were not secure because Defendants wanted to create demand for and to sell the tablets. Had Defendants disclosed their true security practices, Plaintiff and the Overpayment Subclass either would have not purchased the tablets or would have paid substantially less for them (i.e., the value of tablets *without* adequate security protections is worth substantially less than the value of tablets *with* adequate protection).

73. As a direct and proximate result of Defendants' violation of the ICFA, Plaintiff and each Overpayment Subclass member have suffered harm in the form of monies paid for Defendants' products. Plaintiff, on behalf of himself and the Overpayment Subclass, seeks an order (1) requiring Defendants to cease the unfair practices described herein; (2) awarding

damages, interest, and reasonable attorneys' fees, expenses, and costs to the extent allowable; and/or (3) requiring Defendants to restore to Plaintiff and each Overpayment Subclass member any money acquired by means of unfair competition (restitution).

SECOND CAUSE OF ACTION
Breach of Contract
(On behalf of Plaintiff and the Class)

74. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

75. In order to register for an account to use its service, VTech required that Plaintiff Bran read and agree to its Terms and Conditions and Privacy Statement, and in it, VTech's representations regarding its security protocols.

76. Plaintiff Bran was required to read VTech's Terms and Conditions and Privacy Statement (including its representations regarding privacy and data security), before registering for an account with VTech.

77. Plaintiff Bran assented to the Terms and Conditions and Privacy Statement.

78. Together, the Terms and Conditions and Privacy Statement constitute a valid and enforceable contract between Plaintiff Bran and VTech governing his use and purchase of its products and services.

79. Plaintiff Bran's contract was for VTech's products and services, which included security protections for his Sensitive Information.

80. As part of this contract, VTech was obliged to implement adequate security protocols to protect Plaintiff Bran's and the Class's Sensitive Information.

81. Plaintiff Bran was required to read these representations and considered them in making his decision to sign up for an account through VTech. Had VTech represented that it

would not use industry standard security measures, Plaintiff Bran would not have purchased them.

82. Plaintiff Bran performed his obligations under the contract by, among other things, paying his purchase price for VTech's products and/or services and abiding by the Terms and Conditions and Privacy Policy.

83. The data breach revealed that VTech breached the material term of its contract with Plaintiff Bran to protect his Sensitive Information.

84. In the eyes of the marketplace and consumers such as Plaintiff Bran, manufacturers of children's products and services that do not use industry standard data security protocols offer products and services that are fundamentally less useful and valuable than do manufacturers and online service providers that offer products and services that use industry-standard security protections.

85. Consumers, including Plaintiff Bran and the Class, value their privacy. Products and services (like VTech's) that offer greater data security protections offer consumers greater usefulness and utility than products and services with substandard security practices. Consumers will, if given the choice between two otherwise identical products and services, choose the ones with industry-standard security practices over ones with substandard security practices.

86. Because of this consumer preference for data security, a manufacturer and online service with industry-standard security protocols commands higher market prices than ones with substandard security protocols (to the extent ones that use substandard security protocols can sell their products and services at all).

87. Plaintiff Bran believed he would receive adequate protection for his Sensitive Information as part of his purchase price, and those security protections were valuable to him.

88. To Plaintiff Bran, the as-promised products and services offer significantly more utility than the products and services delivered, which lacked meaningful security protections. Thus, to Plaintiff Bran, the products and services promised and paid-for were substantially more valuable than the unsecure products and services delivered.

89. Plaintiff Bran paid for, but never received, the valuable security protections to which he was entitled, and which would have made his VTech products and services significantly more useful to him.

90. As a result of VTech's misconduct and breach of contracts described herein, Plaintiff Bran and the members of the Class suffered and will continue to suffer injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses. Looking forward, and recognizing the risk caused by devastating data breaches like VTech's, Plaintiff and members of the Class will have to incur expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; and increased risk of future harm.

91. Plaintiff and the Overpayment Subclass suffered actual damages, including an amount equal to the difference in the free-market value of the secure products and services they paid for and the insecure products and services they received.

92. Accordingly, Plaintiff, on behalf of himself and the other Class members, seeks an order declaring that VTech's conduct constitutes breach of contract, and awarding Plaintiff and the Class and Overpayment Subclass damages as described above.

THIRD CAUSE OF ACTION
Unjust Enrichment/Restitution
(*In the Alternative to Breach of Contract*)
(On Behalf of Plaintiff and the Overpayment Subclass)

93. Plaintiff incorporates the foregoing allegations as if fully set forth herein, excluding paragraphs 74–92.

94. If the Court finds Plaintiff's and members of the Overpayment Subclass's contracts with VTech invalid, non-existent, or otherwise unenforceable, Plaintiff and members of the Overpayment Subclass may be left without any adequate remedy at law.

95. Plaintiff and members of the Overpayment Subclass conferred a monetary benefit on VTech in the form of fees paid for its products or services (which included the protection of Plaintiff's and the Overpayment Subclass's Sensitive Information).

96. VTech appreciated or had knowledge of the benefits conferred upon it by Plaintiff and members of the Overpayment Subclass.

97. The fees for products and services that Plaintiff and members of the Overpayment Subclass paid to VTech were supposed to be used by VTech, in part, to pay for the administrative costs of data management and security.

98. As a result of VTech's conduct, Plaintiff and the Overpayment Subclass suffered actual damages, including an amount equal to the difference in the free-market value of the secure products and services they paid for and the insecure products and services they received.

99. Further, had VTech informed Plaintiff Bran and the Overpayment Subclass that it would use inadequate security measures to protect their or their children's Sensitive Information, Plaintiff Bran and the Overpayment Subclass would not have purchased VTech's products or services.

100. Accordingly, under principles of equity and good conscience, VTech should not be permitted to retain the money belonging to Plaintiff and members of the Overpayment Subclass, because VTech failed to implement (or adequately implement) the data management and security measures that Plaintiff and members of the Overpayment Subclass paid for.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Heber Bran, on behalf of himself and the Class and the Overpayment Subclass, respectfully requests that this Court issue an order:

A. Certifying this case as a class action on behalf of the Class and Overpayment Subclass defined above, appointing Plaintiff Bran as representative of the Class and Overpayment Subclass, and appointing his counsel as class counsel;

B. Declaring that Defendants' actions, as described herein, constitute (i) violations of the ICFA, (ii) breach of contract, and (iii) unjust enrichment (in the alternative to breach of contract);

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class and Overpayment Subclass members, including, *inter alia*: (i) an order prohibiting Defendants from engaging in the wrongful and unlawful acts described herein; and (ii) requiring Defendants to protect all data collected through the course of their business in accordance with industry-standards;

D. Awarding appropriate damages and restitution to Plaintiff and the Class and Overpayment Subclass in an amount to be determined at trial;

E. Awarding Plaintiff and the Class and Overpayment Subclass their reasonable litigation expenses and attorneys' fees;

F. Awarding Plaintiff and the Class and Overpayment Subclass pre- and post-judgment interest, to the extent allowable; and

G. Awarding such other and further relief as equity and justice may require.

JURY DEMAND

Plaintiff requests a trial by jury of all claims that can be so tried.

Respectfully Submitted,

HEBER BRAN, individually and on behalf of all others similarly situated,

Dated: December 3, 2015

By: /s/ Benjamin S. Thomassen
One of Plaintiff's Attorneys

Jay Edelson
jedelson@edelson.com
Alexander T.H. Nguyen*
anguyen@edelson.com
Benjamin S. Thomassen
bthomassen@edelson.com
EDELSON PC
350 North LaSalle Street, 13th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

**Pro hac vice* admission to be sought.