UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

KEN TITTLE, on Behalf of Himself and All Others Similarly Situated, Plaintiffs, v. VTECH ELECTRONICS NORTH AMERICA, LLC, Defendant.	§ § § § § § § § § § § § §	Case No. CLASS ACTION COMPLAINT **JURY TRIAL DEMANDED**

Plaintiff Ken Tittle, by his attorneys and on behalf of himself and all others similarly situated (the "Class"), brings this action against Defendant VTech Electronics North America, LLC ("Defendants" or "VTech" or the "Company"). Plaintiff allege in this Complaint the following upon knowledge with respect to each of their own acts, and upon facts obtained through an investigation conducted by his counsel, which included, inter alia: (a) review and analysis of defendants' public documents and statements relevant to the instant action; (b) review and analysis of the marketing materials utilized by defendant in connection with the marketing and sales of the products subject of the Complaint; (c) information readily obtainable on the Internet; and (d) interviews of witnesses with personal knowledge of the relevant facts, and upon information and belief as to all other matters based upon, inter alia, an investigation conduct by itself and through its attorneys.

Plaintiffs believe that further substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery. Additional facts supporting the allegations contained herein are known only to defendant or are exclusively within its control.

NATURE OF THE ACTION

1. This is a class action on behalf of a class of persons and entities that acquired certain products from VTech. VTech manufactures and distributes electronic devices aimed toward children and children's learning. In order to fully utilize the devices, VTech requires that consumers provide VTech with personal information, including sensitive information such as their children's identity, by means of online registration.

2. On or about November 14, 2015, an unauthorized party gained entry into the VTech databases and obtained the personal and sensitive information of Plaintiffs and the Class. VTech has acknowledged that its security of this data was wholly inadequate. This admission, is in reality, an understatement of the gross negligence committee by VTech in acquiring and storing sensitive information of the Class.

3. This action asserts claims arising not only from damages caused by the disclosure of Plaintiff's and the members of the Class' sensitive personal information caused by VTech's failure to safeguard the information it demanded, and acquired of Plaintiff and the Class, in order to use the subject products, but also for the damages caused to the Plaintiff and the Class for having purchased the VTech products that they otherwise would not have had they known of VTech's inadequate data security.

PARTIES

4. Plaintiff Ken Tittle is a citizen of the State of Washington. During the Class Period, Mr. Tittle purchased an InnoTab 2 and two VTech Innotab 3S tablets, all of which are designed, manufactured and distributed by VTech. Mr. Tittle registered with, utilized and made purchases through, the Learning Lodge service offered by VTech. Moreover, Mr. Tittle registered for, and utilized the Kid Connect service through the products he purchased. In so

doing, Mr. Tittle provided to VTech personal and sensitive data about himself and his family, including his children.

5. Defendant VTech Electronics North America, LLC is an Illinois limited liability company with its principal place of business at 1155 W Dundee Road, Suite 130, Arlington Heights, IL 60004. VTech further maintains National Registered Agents, Inc. as a registered agent located at 208 SO LASALLE ST, SUITE 814, Chicago, IL 60604.

JURISDICTION AND VENUE

6. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000 and Plaintiff, and other members of the proposed Class, are citizens of a state different from Defendant.

7. This Court has personal jurisdiction over VTech because the Company is an Illinois LLC with its principal place of business in this district, has registered with the Illinois Secretary of State to conduct business in the State of Illinois, has substantial or continuous and systematic contacts through its headquarters located in Arlington Heights, Illinois.

8. Moreover, VTech has consented to, and selected, this jurisdiction and venue in a "Privacy Policy" it contends by its terms that Plaintiff and the members of the Class are subject.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 in that many of the acts and transactions giving rise to this action occurred in this district and because defendant:

a. is authorized to conduct business in this district and has intentionally availed itself of the laws and markets within this district through the promotion, marketing, distribution and sale of its products in this district;

b. does substantial business in this district;

c. maintains its headquarters in this district; and

d. is subject to personal jurisdiction in this district.

COMMON FACTUAL ALLEGATIONS

10. This is a class action on behalf of a class consisting of all persons and entities, other than defendants and its officers and directors, who purchased within the United States products and devices marketed and sold by VTech under various model names[1] through November 29, 2015 (the "Class Period") that utilized software and services including either The Learning Lodge or Kid Connect (collectively "the Products") seeking to recover damages caused by defendants' unlawful conduct and violations of various state consumer protection laws (the "Class"), and for failure to secure and safeguard its customers' personal data, including the personal information of children that it solicited, and for failing to expediently inform Plaintiff and the Class that VTech had experienced a data breach and that the Plaintiffs' personal information had been acquired by a an unauthorized person. Plaintiff further brings these claims for loss of use of the products purchased as VTech has suspended services necessary for the full use of the Products.

11. VTech designs, manufactures, and sells electronic learning products for children of all ages, including preschool and grade school children, including learning systems, kids' laptops, tablets, and multi-functional handheld touch learning systems and other electronic playsets.

12. VTech markets and distributes the Products throughout the United States.

13. The Products utilize software features and programs obtained online and distributed by VTech. Such software includes learning apps and apps that provide for additional

[1] The Products subject of this action include, but are not limited to, InnoTab tablets, including models InnoTab 3, InnoTab 3S Plus, InnoTab 3S, InnoTab3S Plus and the InnoTab Max, and the Tote & Go Laptop, MobiGo, V.Reader, and ABC Learning Classroom products.

features advertised by VTech that are key to the Products value and usability such as Kid Connect software which allows parents and children to interact with one another through text messages sent online to certain of the Products.

14. To obtain and use such software, VTech required Plaintiff and members of the Class to provide their personal information to VTech. VTech further solicited information concerning their children so that the software could be personalized for the children. VTech stored this information on servers that it owned, operated and/or controlled.

15. VTech further marketed online services as part of the benefit of more expensive product models. For example, VTech marketed the Kid Connect feature and service as a key benefit to purchasing the more expensive InnoTab models Innotab 3S Plus and Innotab Max. The Kid Connect feature enabled parents to interact with their children by enabling communications between the Innotab tablet and a cell phone such that parents and children could communicate by way of pictures, "stickers," and text and voice messages and a group "bulletin board." The Kid Connect service also required Plaintiff and members of the Class to provide their personal information to VTech, as well as their children's personal information. The communications sent and received through the Kid Connect service were transmitted to and from servers owned, operated and/or controlled by VTech. These servers further stored the communications sent via the Kid Connect service.

16. Plaintiff and the members of the Class did transmit each of their, and their children's, personal information to VTech in connection with utilizing The Learning Lodge service.

17. Plaintiff and certain members of the Class also acquired premium VTech products, including the Innotab 3S Plus and the Innotab Max, at prices greater than those of

lesser VTech products, in order to take advantage of the Kid Connect features and services that were not available to lesser VTech products (the "Kid Connect Class"). Plaintiff and certain members of the Class transmited each of their, and their children's, personal information to VTech in order to utilize the Kid Connect service. Moreover, Plaintiff and these class members, by using Kid Connect, caused to be transmitted to VTech, sensitive and personal data intended only for use and store by themselves personally.

18. In purchasing and using the Products, and associated online services, Plaintiff and Class members expected VTech to adequately safeguard the personal communications made through the Kid Connect service and limit the information stored by VTech to that which was only necessary to receive and transmit the communications. These expectations were not only established through a consumers' reasonable expectation of privacy and data safeguards now clearly established in under the law, but also by the representations of VTech concerning limitations of the data it collected, data retention policies and safeguards it had in place.

19. Unbeknownst to Plaintiff and members of the Class, VTech was acquiring information unreasonably beyond the scope necessary to carry out the core functions of the services it offered. Moreover, VTech's security was entirely inadequate and was, instead, nothing but incompetent, let alone sufficient given the sensitive nature of the information it was soliciting and storing from Plaintiff and the Class.

20. VTech has acknowledged that on November 14, 2015, its Learning Lodge and Kid Connect databases were hacked. The hack exposed over 11 million accounts, comprising 4.8 million customer (parent) accounts and 6.3 million related kid profiles. Among the 6.3 million related kid profiles, 1.2 million of them were Kid Connect enabled. The information obtained by the third party hacker included parent account informing including name, email

address, secret questions and answers for password retrieval, kids profiles including name, genders and birthdates that are readily associated with the parents' information, childrens' profile photos, Kid Connect messages and chats between children and their parents and bulletin board postings.

21. On November 29, 2015, VTech suspended the Kid Connect and Learning Lodge services, along with a number of associated websites. As a result of these service, Plaintiff and the members of the Class have been denied the use of the Products it purchased, as all Products rely upon the Learning Lodge services, and the Kid Connect Products subject of the Kid Connect Class were marketed, and sold at higher prices, due to having the Kid Connect service access.

22. VTech has admitted that its "Learning Lodge, Kid Connect and PlanetVTech databases were not as secure as they should have been." According to numerous reports, VTech's security was grossly inadequate. Security researcher Troy Hunt concluded in a blog post covering his external review of VTech's online and database security, VTech demonstrated a "total lack of care [ ] in securing this data. It's taken me not much more than a cursory review of publicly observable behaviours to identify serious shortcomings that not only appear as though they could be easily exploited . . . ." The active oversight by VTech of the security of its databases was also inadequate. The third party intruder managed to download more than 190GB worth of photos and data without VTech ever becoming aware. VTech only became aware of the intrusion after security journalists, who were informed of the intrusion by the hacker, repeatedly made efforts to inform VTech of the breach.

23. The security breach, and the failure to promptly discover and block the Data Breach, was the result of VTech's grossly inadequate information systems and security oversight. These failures enabled the perpetrators to obtain customers' personal sensitive

information stored by VTech. VTech's failures further put the Class members and their children at serious risk of ongoing fraud and identity theft.

24. The personal information of consumers, including Plaintiff and Class members, is valuable. In this instance it is also highly sensitive as reflected by broad laws governing business obtaining information from, and concerning, children.

25. The FTC warns consumers to pay particular attention to how they keep personally identifying information and other sensitive data. As the FTC notes, "[t]hat's what thieves use most often to commit fraud or identity theft."

26. The information stolen from VTech is extremely valuable to thieves or other miscreants. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."

27. Personal information such as that stolen in VTech's data breach is highly coveted by and a frequent target of hackers. Legitimate organizations and the criminal underground alike recognize the value of such data. Otherwise, they would not pay for or maintain it, or aggressively seek it. Criminals seek personal and financial information of consumers because they can use biographical data to perpetuate more and larger thefts. Obtaining children's information and family associations provides even greater benefit as such data is ripe for storing and utilizing at later times when Plaintiff and the Class is less likely to be on-guard (particularly children who may be unable to appreciate, or even recall, the data breach).

28. Hackers use personal information to create stolen identities to use in financial fraud and other crimes. Other prospective criminals have also been known to seek and utilize

information about children, including family relationships and other matters familiar to children, in carrying out other crimes.

29. The data breach was caused and enabled by Defendant's knowing violation of its obligations to abide by best practices and industry standards in protecting customers' personal information. The Company grossly failed to comply with security standards and allowed its customers' data 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 that occurred.

30. Defendant's failure to comply with reasonable security standards provided the Company with short-term and fleeting benefits in the form of saving on the costs of compliance, but at the expense and to the severe detriment of its own customers – including Class members here – who have been subject to the breach or otherwise have had their personal information placed at serious and ongoing risk.

31. The Company allowed widespread and systematic theft of its customers' personal information. Defendant's actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect customers' financial information.

PLAINTIFF'S FACTUAL ALLEGATIONS

32. In late 2012 or early 2013, Mr. Tittle purchased an InnoTab 2. In March 2014, Mr. Tittle purchased two VTech Innotab 3S tablets. All of these products are designed, manufactured and distributed by VTech. Mr. Tittle registered with, utilized and made purchases through, the Learning Lodge service offered by VTech. Moreover, Mr. Tittle registered for, and utilized the Kid Connect service through the products he purchased. In so doing, Mr. Tittle provided to VTech personal and sensitive data about himself and his family, including his

children. Mr. Tittle also provided VTech with his personal credit card information so that he could utilize the services to make purchases from VTech.

33. In making his purchase, Mr. Tittle relied upon the numerous representations and marketing materials regarding the quality of the products and the services that it provided.

34. Mr. Tittle further relied upon a reasonable expectation that VTech would implement adequate safeguards of the data he provided to VTech and the limitations of the scope of data and information that VTech would capture and store. Plaintiff further believed, and relied upon, that VTech would maintain the personal information contained provided to it by Plaintiff in a reasonably secure manner, and would also maintain reasonable limitations of the scope of data and information that VTech captured and stored.

35. Plaintiff's personal information, along with his children's, has been compromised as a result of the VTech data breach. Plaintiff was harmed by having his personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to the data breach.

36. Plaintiff also purchased Kids Connect Products and paid a premium over other devices so that he could utilize the Kids Connect service. VTech has suspended said service and denied Plaintiff and members of the Kids Connect Class utilization of said services.

37. Had Plaintiff been aware of the grossly inadequate security measures implemented by VTech, Plaintiff would not have purchased the Products or would paid substantially less given the decrease in the value of said Products purchased.

CLASS ACTION ALLEGATIONS

38. Pursuant to Fed. R. Civ. P. 23, Plaintiff brings his claims that the Company violated state data breach statutes (Count I) on behalf of separate statewide classes in and under

the respective data breach statutes of the States of Alaska, Arkansas, Arizona, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, North Carolina, North Dakota, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, Wisconsin and Wyoming, and the District of Columbia. These classes are defined as follows:

> **Statewide Data Breach Statute Classes:**
>
> All residents of [name of State or District of Columbia] who purchased a VTech product that utilizes the Learning Lodge or Kids Connect Service in the United States through November 29, 2014.

39. Pursuant to Fed. R. Civ. P. 23, Plaintiff brings separate claims for breach of implied contract (Count III), negligence (Count IV), unjust enrichment (Count V), and violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.* (Count VI), on behalf of the respective statewide classes in and under the laws of each respective State of the United States and the District of Columbia as set forth in Counts III, IV, V) These classes for each of the foregoing claims are defined as follows:

> **Statewide [Breach of Implied Contract, Negligence, Unjust Enrichment] Class:**
>
> All residents of [name of State or District of Columbia] who purchased a VTech product that utilizes the Learning Lodge or Kids Connect Service in the United States through November 29, 2014.

40. Plaintiff further seeks to represent, and assert a claim for violation of the same statutes on behalf of a subclass of Kids Connect Product purchasers, defined as:

> All residents of [name of State or District of Columbia] who purchased a VTech product that utilizes the Kids Connect Service, including but not limited to the Innotab 3S Plus and Innotab Max, in the United States through November 29, 2014 (the "Kids Connect Subclass").

41. Plaintiff further seeks to represent, and assert a claim for violation of Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*. (Count II), Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.* (Count VI) and for Declaratory Judgment (Count VII), on behalf of himself, a subclass consisting of residents of the State of Washington who purchased the Products, and a nationwide class, defined as:

> All Class members who reside in the United States of America and purchased a VTech product that utilizes the Learning Lodge or Kids Connect Service and registered with VTech for the the Learning Lodge or Kids Connect Service through November 29, 2014. (the "Nationwide Class").

42. Excluded from each of the above Classes are VTech, including any entity in which VTech has a controlling interest, is a parent or subsidiary, or which is controlled by VTech, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of VTech. Also excluded are the judges and court personnel in this case and any members of their immediate families.

43. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class wide basis using the same exclusive and common evidence as would be used to prove those elements in individual actions alleging the same claims.

44. All members of the purposed Classes are readily ascertainable. VTech has access to addresses and other contact information for thousands of members of the Class, which can be

used for providing notice to many Class members. In fact, VTech has notified Plaintiff and the Class members by e-mail through such a list it maintains.

45. Numerosity. Plaintiff does not know the exact number of Class members but believe that the Class comprises thousands if not tens of thousands of consumers throughout these United States. As such, Class members are so numerous that joinder of all members is impracticable.

46. Commonality and predominance. Well-defined, nearly identical legal or factual questions affect all Class members. These questions predominate over questions that might affect individual Class members. These common questions include, but are not limited to, the following:

a. Whether there was an unauthorized disclosure by Defendant of Class members' personal and/or financial information;

b. Whether Defendants enabled an unauthorized disclosure of Class members' personal and/or financial information;

c. Whether Defendant misrepresented the safety and security of Class members' personal and/or financial information maintained by Defendant;

d. Whether Defendant implemented and maintained reasonable procedures and practices appropriate for maintaining the safety and security of Class members' personal and/or financial information;

e. When Defendant became aware of an unauthorized disclosure of Class members' personal and/or financial information;

f. Whether Defendant unreasonably delayed notifying Class members of an unauthorized disclosure of Class members' personal and/or financial information;

g. Whether Defendant intentionally delayed notifying Class members of an unauthorized disclosure of Class members' personal and/or financial information;

h. Whether Defendant's conduct was negligent;

i. Whether Defendant's conduct was deceptive;

j. Whether Defendant's conduct was knowing, willful, intentional, and/or malicious;

k. Whether Defendant's conduct constitutes breach of an implied contract;

l. Whether the representations of Defendant made in connection with the marketing of the Products and associated services were deceptive;

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

n. Whether Plaintiff and the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

47. Typicality. Plaintiff's claims are typical of the claims of the Class. Plaintiff and all Class members were injured through the Company's misconduct described above and assert the same claims for relief. The same events and conduct that give rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each Class member is a person that has suffered harm as a direct result of the same conduct (and omissions of material facts) engaged in by Defendant and resulting in the data breach.

48. Adequacy. Plaintiff will fairly and adequately protect Class members' interests. Plaintiff has no interests antagonistic to Class members' interests, and Plaintiff has retained counsel that has considerable experience and success in prosecuting complex class action and consumer protection cases.

49. Superiority. A class action is superior to all other available methods for fairly and efficiently adjudicating the claims of Plaintiff and the Class members. Plaintiff and the Class members have been harmed by the Company's wrongful actions and inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to the Company's wrongful actions and inaction.

50. A class action is an appropriate method for the fair and efficient adjudication of this controversy. There is no special interest in the members of the Class individually controlling the prosecution of separate actions. The loss of money and other harm sustained by many individual Class members will not be large enough to justify individual actions, especially in proportion to the significant costs and expenses necessary to prosecute this action. The expense and burden of individual litigation makes it impossible for many members of the Class individually to address the wrongs done to them. Class treatment will permit the adjudication of claims of Class members who could not afford individually to litigate their claims against the Company. Class treatment will permit a large number of similarly situated persons to prosecute their common claims in a single form simultaneously, efficiently, and without duplication of effort and expense that numerous individual actions would entail. No difficulties are likely to be encountered in the management of this class action that would preclude its maintenance as a class action, and no superior alternative exists for the fair and efficient adjudication of this controversy. Furthermore, Defendant transacts substantial business in and perpetuated its unlawful conduct throughout the United States, including Illinois. Defendant will not be prejudiced or inconvenienced by the maintenance of this class action in this forum.

51. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(a) and (b)(3). The above common questions of law or fact predominate over any questions affecting individual

members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

52. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because the Company has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

53. The expense and burden of litigation will substantially impair the ability of Plaintiff and Class members to pursue individual lawsuits to vindicate their rights. Absent a class action, Defendant will retain the benefits of its wrongdoing despite its serious violations of the law.

COUNT I
Violations of State Data Breach Statutes
(On behalf of Plaintiff and the separate statewide data breach statute classes.)

54. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

55. Legislatures in the states and jurisdictions listed below have enacted data breach statutes. These statutes generally require that any person or business conducting business within the state that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system to any resident of the state whose personal information was acquired by an unauthorized person, and further require that the disclosure of the breach be made in the most expedient time possible and without unreasonable delay.

56. Defendant's data breach constitutes a breach of the security system of the Company within the meaning of the below state data breach statutes and the data breached is protected and covered by the below data breach statutes.

57. Plaintiff's and Class members' names, addresses, phone numbers and email addresses constitute personal information under and subject to the below state data breach statutes.

58. Defendant unreasonably delayed in informing the public, including Plaintiff and members of the statewide Data Breach Statute Classes ("Class," as used in this Count I), about the breach of security of Plaintiff's and Class members' confidential and non-public personal information after Defendant knew or should have known that the data breach had occurred.

59. Defendant failed to disclose to Plaintiff and Class members without unreasonable delay and in the most expedient time possible, the breach of security of Plaintiff's and Class members' personal and financial information when the Company knew or reasonably believed such information had been compromised.

60. Plaintiff and members of the Class suffered harm directly resulting from the Company's failure to provide and the delay in providing Plaintiff and Class members with timely and accurate notice as required by the below state data breach statutes. Plaintiff suffered the damages alleged above as a direct result of the Company's delay in providing timely and accurate notice of the data breach.

61. Had Defendants provided timely and accurate notice of the Company's data breach, Plaintiff and Class members would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by the Company in providing notice. Plaintiff and Class members could have avoided utilizing the Products and the services, and could have contacted their banks to cancel their cards, or could otherwise have tried to avoid the harm caused by the Company's delay in providing timely and accurate notice.

62. The Company's failure to provide timely and accurate notice of Defendant's data breach violated the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), et seq.;

b. Ark. Code Ann. § 4-110-105(a), et seq.;

c. Ariz. Rev. Stat. § 44-7501, et seq.;

d. Cal. Civ. Code § 1798.83(a), et seq.;

e. Colo. Rev. Stat. Ann § 6-1-716(2), et seq.;

f. Conn. Gen. Stat. Ann. § 36a-701b(b), et seq.;

g. Del. Code Ann. Tit. 6 § 12B-102(a), et seq.;

h. D.C. Code § 28-3852(a), et seq.;

i. Fla. Stat. Ann. § 501.171(4), et seq.;

j. Ga. Code Ann. § 10-1-912(a), et seq.;

k. Haw. Rev. Stat. § 487N-2(a), et seq.;

l. Idaho Code Ann. § 28-51-105(1), et seq.;

m. Ill. Comp. Stat. Ann. 530/10(a), et seq.;

n. Iowa Code Ann. § 715C.2(1), et seq.;

o. Kan. Stat. Ann. § 50-7a02(a), et seq.;

p. Ky. Rev. Stat. Ann. § 365.732(2), et seq.;

q. La. Rev. Stat. Ann. § 51:3074(A), et seq.;

r. Md. Code Ann., Commercial Law § 14-3504(b), et seq.;

s. Mass. Gen. Laws Ann. Ch. 93H § 3(a), et seq.;

t. Mich. Comp. Laws Ann. § 445.72(1), et seq.;

u. Minn. Stat. Ann. § 325E.61(1)(a), et seq.;

v. Mont. Code Ann. § 30-14-1704(1), et seq.;

w. Neb. Rev. Stat. Ann. § 87-803(1), et seq.;

x. Nev. Rev. Stat. Ann. § 603A.220(1), et seq.;

y. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), et seq.;

z. N.J. Stat. Ann. § 56:8-163(a), et seq.;

aa. N.C. Gen. Stat. Ann. § 75-65(a), et seq.;

bb. N.D. Cent. Code Ann. § 51-30-02, et seq.;

cc. Okla. Stat. Ann. Tit. 24 § 163(A), et seq.;

dd. Or. Rev. Stat. Ann. § 646A.604(1), et seq.;

ee. Pa. 73 Stat. § 2301, et sq.;

ff. R.I. Gen. Laws Ann. § 11-49.2-3(a), et seq.;

gg. S.C. Code Ann. § 39-1-90(A), et seq.;

hh. Tenn. Code Ann. § 47-18-2107(b), et seq.;

ii. Tex. Bus. & Com. Code Ann. § 521.053(b), et seq.;

jj. Utah Code Ann. § 13-44-202(1), et seq.;

kk. Va. Code. Ann. § 18.2-186.6(B), et seq.;

ll. Wash. Rev. Code Ann. § 19.255.010(1), et seq.;

mm. Wis. Stat. Ann. § 134.98(2), et seq.; and

nn. Wyo. Stat. Ann. § 40-12-502(a), et seq.

63. Plaintiff and members of each of the statewide Data Breach Statute Classes seek all remedies available under their respective state data breach statutes, including but not limited to a) damages suffered by Plaintiff and Class members as alleged above, b) equitable relief, including injunctive relief, and c) reasonable attorney fees and costs, as provided by law.

COUNT II
Violation of the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.
(On behalf of Plaintiff and the Nationwide Class.)

64. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

65. Plaintiff and members of the PIPA Nationwide Class ("Class" as used in this Count II) provided their financial and personal information to Defendant in order to fully utilize the Products, including making purchases through the apps and using the communications services offered therein.

66. The Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*. ("PIPA") requires that businesses that maintain or store personal information and financial data such as that provided by Plaintiffs and the Class must provide immediate notification to the owners or licensees of such data in the event of a security breach, and cooperate with the owners and licensees thereafter. Specifically, PIPA provides, in relevant part:

> Sec. 10. Notice of Breach.
>
> (b) Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. . . .

67. Under 815 ILCS 530/5, VTech is, and at all relevant times was, a Data Collector in that it is a private corporation or retail operator that for any purpose "handles, disseminates, or otherwise deals with nonpublic personal information." Specifically, VTech was a Data Collector that maintained or stored, but did not own or license, the computerized data that included the personal information of Plaintiff and the members of the Class.

68. The personal information obtained from Plaintiff and the members of the Class by Defendant was "Personal information" under 815 ILCS 530/5 as it contained each class members' first name or initial, and last name, in combination with a credit or debit card number.

69. At all relevant times, the Plaintiff and members of the Class were the owners or licensees of their respective Personal Information.

70. As alleged herein, Defendant was subject of a "breach of the security of the system data" owned, operated or controlled by Defendant. 815 ILCS 530/5.

71. Defendant, as a Data Collector that maintained or stored, but did not own or license, computerized data the personal information of Plaintiff and the members of the class, and had suffered a breach of its security of the system data, was required pursuant to 815 ILCS 530/10(b) to notify the Plaintiff and members of the Class immediately of the breach of Defendant's system data containing Plaintiff and the members of the Class' Personal information upon discovery of the breach by Defendants. Defendant was further required to cooperate with the Plaintiff and each member of the Class.

72. Defendant violated 815 ILCS 530/10(b), as alleged herein.

73. It was foreseeable that Defendant's failure to comply with PIPA would subject Plaintiff and the PIPA Nationwide Class to risk that their information would be further compromised by unscrupulous third parties, and Defendant's unlawful conduct did, in fact, result in that occurring.

74. The losses and damages sustained by Plaintiff and Class members as described herein were the actual and proximate result of the Company's breaches of the implied contracts between Defendant and Plaintiff and members of the Class.

COUNT III
Breach of Implied Contract
(On behalf of Plaintiff and the separate statewide breach of implied contract classes.)

75. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

76. When Plaintiff and members of the Breach of Implied Contract Classes ("Class" as used in this Count III) provided their financial and personal information to Defendant in order to register for Defendant's services necessary to utilize the Products, Plaintiff and members of the Class entered into implied contracts with the Company pursuant to which the Company agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members that their data had been breached and compromised.

77. Defendant solicited and invited Plaintiff and members of the Class to acquire the Products, and register and utilize the associated services offered by Defendant, by among other things, contributing their personal information and using their credit or debit cards. Plaintiff and members of the Class accepted the Company's offers, submitted their personal and financial information, and used their credit or debit cards to make purchases from Defendant during the period of the Company's data breach.

78. The purchase of the Products and registration and utilization of the associated service offered by VTech was made pursuant to the mutually agreed upon implied contract with the Company under which the Company agreed to safeguard and protect Plaintiff's and Class members' personal and financial information, including Plaintiff's and Class members' credit or debit cards, and to timely and accurately notify them that such information was compromised and breached.

79. Plaintiff and Class members would not have purchased the Products or provided and entrusted their financial and personal information to Defendant in order to register and utilize the associated services in the absence of the implied contract between them and the Company.

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

81. Defendant breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the personal and financial information of Plaintiff and members of the Class and by failing to provide timely and accurate notice to them that their personal and financial information was compromised in and as a result of the Company's data breach.

82. The losses and damages sustained by Plaintiff and Class members as described herein were the direct and proximate result of The Company's breaches of the implied contracts between Defendant and Plaintiff and members of the Class.

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

COUNT IV
Negligence
(On behalf of Plaintiff and the separate statewide negligence classes.)

84. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

85. Defendant owed numerous duties to Plaintiff and members of the separate statewide Negligence Classes ("Class" as used in this Count IV). Defendant's duties included the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting personal and financial data in its possession;

b. to protect the Plaintiff and Class members' personal and financial data using reasonable and adequate security procedures and systems that are compliant and consistent with industry-standard practices governing highly sensitive personal information; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class members of the data breach.

86. Defendant owed a duty of care not to subject Plaintiff and the members of the Class, and their accompanying personal and financial data, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices. Defendant solicited, gathered, and stored Plaintiff and the Class members' personal information and financial data to facilitate sales transactions.

87. Defendant knew, or should have known, of the risks inherent in collecting and storing personal information and financial data and the importance of adequate security. Defendant received warnings from within and outside the company that hackers routinely attempted to access such information without authorization. Defendant also knew about numerous, well-publicized data breaches throughout the United States.

88. Defendant knew, or should have known, that its computer systems did not adequately safeguard Plaintiff and the Class members' personal and financial data.

89. Because Defendant knew that a breach of its systems would damage millions of its customers, including Plaintiff and the Class members, it had a duty to adequately protect their personal Information and financial data.

90. Defendant had a special relationship with Plaintiff and the Class members. Plaintiff's and Class members' willingness to entrust Defendant with their personal information and financial data was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the personal Information and financial data that it stored on them from attack.

91. Defendant's conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Personal Information. Defendant's misconduct included failing to: (1) secure its databases and external access to such databases, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) sufficiently encrypt the personal information and financial data of Plaintiff and members of the Class, (5) employ adequate network segmentation, (6) implement adequate system and event monitoring, and (7) implement the systems, policies, and procedures necessary to prevent this type of data breach.

92. Defendant also had independent duties under state laws that required Defendant to reasonably safeguard Plaintiff's and the Class members' personal information and financial data and promptly notify them about the data breach.

93. Defendant breached the duties it owed to Plaintiff and Class members in numerous ways, including:

a. by creating a foreseeable risk of harm through the misconduct previously described;

b. by failing to implement adequate security systems, protocols and practices sufficient to protect their personal information and financial both before and after learning of the data breach;

c. by failing to comply with the minimum industry data security standards during the period of the data breach; and

d. by failing to timely and accurately disclose that their personal information and financial data had been improperly acquired or accessed.

94. But for Defendant's wrongful and negligent breach of the duties it owed Plaintiffs and Class members, their personal information and financial data either would not have been compromised or they would have been able to prevent some or all of their damages.

95. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligent conduct. Accordingly, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT V
Unjust Enrichment
(On behalf of Plaintiff and the separate statewide unjust enrichment classes.)

96. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

97. Plaintiff and members of the separate statewide Unjust Enrichment Classes ("Class" as used in this Count V) conferred a monetary benefit on Defendant in the form of monies paid for the purchase of the Products during the Class Period.

98. Defendant appreciates or has knowledge of the benefits conferred directly upon it by Plaintiff and members of the Class through the purchase of the Products.

99. Defendant markets the Products as utilizing the online services subject of the data breach, and, in fact, required Plaintiff and members of the Class to provide the sensitive personal and financial information to Defendant in order to fully utilize the Products by means of the associated services.

100. The monies paid for the purchase of goods by Plaintiff and members of the Class to Defendant during the period of the Company's data breach were supposed to be used by the Company, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and members of the Class.

101. Defendant failed to provide reasonable security, safeguards and protection to the personal and financial information of Plaintiff and Class members and as a result, Plaintiff and Class members overpaid the Company for the goods purchased through use of their credit and debit cards during the period of the Company's data breach.

102. Moreover, the Plaintiff and members of the Class have been denied full utilization of the Products and associated services as the Company has suspended the services, thereby denying Plaintiff and members of the Class the full benefit of the bargain entered into when Plaintiff and the Class purchased the Products.

103. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and members of the Class, because the Company failed to provide adequate safeguards and security measures to protect Plaintiff's and Class members' personal and financial information that they paid for but did not receive. Moreover, Plaintiff and the Class members are now being denied use of the services that were associated with, and required, by the Products.

104. As a result of the Company's conduct as set forth in this Complaint, Plaintiff and members of the Class suffered damages and losses as stated above, including monies paid for the Products that Plaintiff and Class members would not have purchased had the Company disclosed the material fact that it lacked adequate measures to safeguard customers' data and had the Company provided timely and accurate notice of the data breach, and including the difference between the price they paid for the Company's goods as promised and the actual diminished value of its goods and services.

105. Plaintiff and the Class have conferred directly upon Defendant an economic benefit in the nature of monies received and profits resulting from sales and unlawful overcharges to the economic detriment of Plaintiff and the Class.

106. The economic benefit, including the monies paid and the overcharges and profits derived by the Company and paid by Plaintiff and members of the Class, is a direct and proximate result of the Company's unlawful practices as set forth in this Complaint.

107. The financial benefits derived by the Company rightfully belong to Plaintiff and members of the Class.

108. It would be inequitable under established unjust enrichment principles in the District of Columbia and all of the 50 states for the Company to be permitted to retain any of the financial benefits, monies, profits and overcharges derived from the Company's unlawful conduct as set forth in this Complaint.

109. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds received by the Company.

110. A constructive trust should be imposed upon all unlawful or inequitable sums received by the Company traceable to Plaintiff and the Class.

111. Plaintiff and the Class have no adequate remedy at law.

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

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

113. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

114. Defendant's offered and advertised the services associated with the Products to induce the Plaintiff and members of the Nationwide Class to purchase the Products as well as utilize the services associated with the Products, which included services that enabled Plaintiff and members of the Class to make additional purchases from Defendant. Defendant intended for Plaintiff and the other members of the Nationwide Class to rely on Defendant's to protect, secure, and prevent access from unauthorized third parties the personal and financial information furnished to it by Plaintiff and the Nationwide Class as Plaintiff and the Class utilized the Products and associated services.

115. Defendant knowingly concealed, suppressed and consciously omitted material facts to Plaintiff and other members of the Nationwide Class knowing that consumers would rely on the advertisements and packaging to purchase the Products.

116. At the time Defendant made and disseminated the statements alleged herein, it knew or should have known that the statements were untrue or misleading

117. Instead of truthfully disclosing material facts concerning the scope of the data it collected, and the inadequate security it utilized in protecting said data, Defendant's knowingly, and intentionally, maintained an insecure database and online services system that, along with inadequate oversight of its information systems, was inadequate to effectively protect Plaintiff

and the Nationwide Class members' financial and personal information from being compromised.

118. Defendant's either willfully failed to follow industry best practices concerning data theft or was negligent in preventing such data theft from occurring, and concealed, omitted and misrepresented this fact from Plaintiff and the Nationwide Class.

119. Defendant benefited from maintaining an insecure and susceptible network and database system that exposed its customers' personal and financial information to theft by not having to make significant one-time and going expenditures to purchase, implement and maintain adequate measures that that would have prevented the data from being compromised, or limited the extent of the breach through early detection. Defendant further benefitted by storing and maintaining data and information submitted by Plaintiff and the Nationwide Class in connection with their use of the Products' associated services by utilizing said data not to effectuate the services but to profit from scraping said data in order to analyze it for competitive purposes and/or sell it to third parties.

120. Defendant's fraudulent and deceptive acts and omissions were intended to induce Plaintiff and the other Nationwide Class members' reliance on Defendant's deception that their personal and financial information was secure and protected when using debit and credit cards to make purchases from Defendant. Defendant's acts and omissions were also intended to induce Plaintiff and the Nationwide Class members' to purchase the Products by believing that the use of said products was safe and private, and that any data collected was collected for purposes of effectuating the services and was stored in a secure environment.

121. Plaintiff and the members of the Nationwide Class were deceived by Defendant's failure to properly implement adequate, commercially reasonable security measures to protect their personal and private financial information.

122. Plaintiff and the Nationwide Class members were induced as a result of Defendants' unlawful conduct to provide their personal and financial information to Defendants in connection with registering for, and using, the online services associated with the Products. Moreover, the Plaintiff and Nationwide Class members were induced into purchasing the Products.

123. Defendant's violated 815 ILCS 505/1, *et seq.*, by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff's and the other Nationwide Class members' personal and financial information, and by marketing and selling the Product using false and misleading representations, along with omissions, concerning the safety of the Products and the services associated therewith, in violation of 815 ILC 505/2.

124. Defendant's failure to maintain reasonable and appropriate means to protect consumers' personal and financial information, and failure to promptly notify consumers of the security breach, constitutes unfair acts or practices under Federal Trade Commission Act, 15 U.S.C. § 45(a) because substantial injury to Class members was not reasonably avoidable by consumers and is not offset by countervailing benefits to consumers or competition. 815 ILCS 505/2

125. Defendant's failure to promptly and adequately notify affected customers of the Data Breach also served as an unlawful practice as it failed to act in accordance with Illinois law that governed its corporate conduct as to all consumers. As set forth in Count II, Defendant violated Section 10(b) of the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et*

seq. The violation of 815 ILCS 530/10(b) is deemed "an unlawful practice" under Illinois' Consumer Fraud and Deceptive Business Practices Act. 815 ILCS 530/20.

126. Plaintiff and the Nationwide Class members have suffered injury in fact and actual damages.

127. The foregoing acts, omissions and practices directly, foreseeably and proximately caused Plaintiff and other members of the Class to suffer an ascertainable loss and damages in the form of, inter alia, paying more money for the Product than they would have, and/or by purchasing the Product which they would not have purchased, if the benefits of taking the Product had not been misrepresented, in amounts to be determined at trial. It was foreseeable that Defendant's willful indifference or negligent course of conduct in handling its customers' personal and financial information would subject Plaintiff and the Nationwide Class to risk that their information would be compromised by unscrupulous third parties, and Defendant's unlawful conduct did, in fact, result in the Data Breach which has harmed Plaintiff and the Nationwide Class.

128. Moreover, it was foreseeable that Plaintiff and the Nationwide Class would rely upon the misrepresentations and omissions made by Defendant in connection with the marketing and advertising of the Products.

129. As a result of Defendants' violations of the Illinois Consumer Fraud Act, Plaintiff and the Nationwide Class have suffered actual damages including, including, among others, costs incurred with the increased risk of identity theft including present and future costs of credit monitoring services, control of the property rights in their personal and financial information, the denial of the services they paid for when purchasing the Products as a result of the Defendant's

suspension of associated services, as well as having been induced to purchase the Products that they either would not have purchased at all, or would have paid substantially less for. .

130. The fraudulent and deceptive acts of Defendant were the result of Defendant's wanton or reckless conduct and/or reckless indifference to the interest of others. Accordingly, an award of punitive damages is appropriate.

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

COUNT VII
Declaratory Judgment
(On behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Separate Statewide Negligence and Breach of Implied Contract Classes)

132. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

133. As previously alleged, Plaintiff and members of the Breach of Implied Contract classes entered into an implied contract that required Defendant to provide adequate security for the personal information and financial data it collected from their credit and debit card transactions. As previously alleged, Defendant owes duties of care to Plaintiff and the members of the Nationwide class or, alternatively, the separate statewide Negligence classes, that require it to adequately secure personal information and financial data.

134. Defendant still possesses the personal information and financial data regarding Plaintiff and the Class members.

135. After the data breach, Defendant announced changes that it claimed would improve data security. These changes, however, have not fix many systemic vulnerabilities in Defendant's computer online storage and database network.

136. Accordingly, Defendant has still has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class members. In fact, now that Defendant's lax approach

towards information security has become public, the personal information and financial data in Defendant's possession is even more vulnerable. Actual harm has arisen in the wake of the Company's data breach regarding its contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Breach of Implied Contract and Negligence Classes. Defendant maintains that its security measures will become adequate even though its changes are insufficient to meet Defendant's contractual obligations and legal duties.

137. Moreover, Defendant continues to maintain the personal information of Plaintiff and the members of the Class, and will continue to maintain such information, as well as gather additional information from Plaintiff and the Class, if the Plaintiff and the members of the Class continue utilizing the Products that they purchased, as Defendant requires that it obtain such information in an ongoing basis in order to deliver the services associated with the Products. Accordingly, Plaintiff and members of the Class will continue to experience harm without Declaratory Judgment, or otherwise be stripped of the entire value of the Product as the Products otherwise become unusable as intended.

138. Plaintiff, therefore, seeks a declaration (a) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (b) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to: (1) ordering the Defendant to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors; (2) ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

(3) ordering that Defendant's audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Defendant segments customer data by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems; (5) ordering that Defendant's purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services; (6) ordering that Defendant's conduct regular database scanning and securing checks; (7) ordering that Defendant routinely and continually conducts internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (8) ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendant customers must take to protect themselves; and (9) imposing restrictions on the scope, both nature of and period of retention, of the data and information collected by Defendants in order to provide the services associated with the Products.

Defendant

PRAYER FOR RELIEF

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

A. certifying this case as a class action pursuant to Fed. R. Civ. P. 23(a), (b)(2) and (b)(3), and, pursuant to Fed. R. Civ. P. 23(g), appoint the named Plaintiff to be Class representative and their undersigned counsel to be Class counsel;

B. requiring Defendants to make whole any losses suffered by Plaintiff and Class members;

C. requiring Defendants to pay for three years of credit card fraud monitoring services;

D. enjoining Defendants from further engaging in the unlawful conduct complained of herein and requiring Defendant to implement and maintain adequate security measures to ensure the security of Plaintiff and the members of the Class' personal information and financial data that remains in the possession of Defendant;

E. awarding Plaintiff and the Classes appropriate relief, including actual, statutory, and punitive damages, restitution and disgorgement;

F. awarding pre-judgment and post-judgment interest;

G. requiring Defendants to pay for notifying the Class of the pendency of this action;

H. establishing a fluid recovery fund for distribution of unclaimed funds;

I. requiring Defendant to pay Plaintiff's and Class members reasonable attorneys' fees, expenses, and the costs of this action; and

J. providing all other and further relief as this Court deems necessary, just, and proper.

DEMAND FOR TRIAL BY JURY

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

Dated: December 3, 2015

Respectfully submitted:

By: /s/ Matthew T. Hurst
Matthew T. Hurst, Esq.

Laurence M. Rosen, Esq.
Phillip Kim, Esq.
THE ROSEN LAW FIRM, P.A.
275 Madison Ave., 34th Floor
New York, NY 10016
Telephone: (212) 686-1060
Facsimile: (212) 202-3827
lrosen@rosenlegal.com
pkim@rosenlegal.com

Christopher S. Hinton, Esq.
THE HINTON LAW FIRM
275 Madison Ave., 34th Fl.
New York, New York 10016
Telephone: (646) 723-3377
Facsimile: (914) 530-2954

Matthew T. Hurst, Esq.
HEFFNER HURST
30 North LaSalle Street, 12th Floor
Chicago, Illinois 60602
Telephone: (312) 346-3466
Facsimile: (312) 346-2829
mhurst@heffnerhurst.com

Counsel to Plaintiff