United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

WASHINGTON, DC 20510–6125

WEBSITE: http://commerce.senate.gov

March 29, 2017

The Honorable Maureen Ohlhausen
Acting Chairwoman
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

Dear Chairwoman Ohlhausen:

Over the past few years, there have been several instances in which security vulnerabilities in internet-connected toys have led to the exposure of children's sensitive personal information. While the growth in connected toys has created important educational benefits for children, I am concerned that connected toys also pose significant privacy and security risks that the Federal Trade Commission (FTC) must address more effectively.

The Children's Online Privacy Protection Act (COPPA), implemented and enforced by the FTC through the COPPA Rule, is intended to protect children under age 13 by requiring companies to obtain explicit parental consent before collecting online information from their children.[1] In so doing, the COPPA Rule also requires covered companies to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[2] In 2013, the FTC revised the COPPA Rule to broaden the definition of children's personal information to include children's photos, videos, audio recordings, and geolocation information. The FTC also expanded the rule to include mobile applications as covered operators of websites and online services that collect and use personal information from children.[3]

In 2015, a data breach involving connected devices manufactured by VTech exposed the personal information of more than six million children globally – including children's names, genders, dates of birth, and photographs.[4] While the VTech breach was troubling enough, in recent years, security researchers have also identified vulnerabilities with other connected devices for children.[5]

---

[1] 15 U.S.C. §§ 6501-6508. The FTC enforces the law through 16 C.F.R. Part 312.

[2] 16 C.F.R. § 312.8.

[3] 16 C.F.R. § 312.2.

[4] *See One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids*, Motherboard (Nov. 27, 2015).

[5] *Hackers Can Hijack Wi-Fi Hello Barbie to Spy on Your Children*, The Guardian (Nov. 26, 2015); *R7-2015-27 and R7-2015-24: Fisher-Price Smart Toy® & hereO GPS Platform Vulnerabilities (FIXED)*, Rapid7 (Jan. 25, 2016).

Last December, I released a report titled, "Children's Connected Toys: Data Security and Privacy Concerns."[6] The report revealed the failure by some toymakers to secure collected consumer data and questioned whether toymakers are adequately prioritizing the security of children's information. I recommended that the FTC, as the country's principal consumer protection agency, carefully monitor the connected toy space and exercise the FTC's authority when appropriate.

In addition, last month, there were reports that a security breach of a database belonging to Spiral Toys – the inventor and technology provider of CloudPets toys – potentially exposed the information of hundreds of thousands of consumers, including voice recordings exchanged between children and parents. I wrote to Spiral Toys requesting information about the breach, the specific steps the company took to assist consumers impacted by the breach, and what the company has done to ensure the protection of its collected data in the future. For your reference, I have attached my letter and the company's response.

Please explain what actions the FTC has taken in response to these recent data breaches, which have exposed the personal information of millions of children. Specifically, I would like to know what actions the FTC has taken under the COPPA Rule to protect the personal data of children using connected toys. In addition, if the FTC believes it lacks sufficient authority under the COPPA Rule to protect children using connected toys, please let me know what steps the FTC plans to take to revise the rule.

Please provide a response by April 19, 2017. Thank you in advance for your assistance with this important matter.

Sincerely,

Bill Nelson

BILL NELSON
Ranking Member

Enclosure

cc: The Honorable John Thune, Chairman

---

[6] Senate Committee on Commerce, Science, and Transportation, *Children's Connected Toys: Data Security and Privacy Concerns*, 114th Congress (Dec. 14, 2016).

United States Senate
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
WASHINGTON, DC 20510–6125
WEBSITE: http://commerce.senate.gov

March 7, 2017

Mark Meyers
Chairman and Chief Executive Officer
Spiral Toys
30077 Agoura Court, Suite 230
Agoura Hills, CA 91301

Dear Mr. Meyers:

In light of the recent breach of a Spiral Toys' database containing information about hundreds of thousands of users collected from its internet-connected CloudPets toys, I write to you with questions regarding the overall data privacy and security practices of Spiral Toys.

According to a report from a security researcher, hackers appear to have accessed and exposed Spiral Toy's database that contained more than 800,000 email addresses and hashed passwords.[1] Not only was the information accessed, but records also reportedly show that the data was ransomed by the hackers on multiple occasions. Because Spiral Toys created no requirements for password strength, the hackers could have easily cracked many passwords by simply checking the data against common passwords. This information could then be used to access and download the private voice recordings of children and parents.[2]

The 2015 VTech breach that exposed the personal information of more than six million children globally should have served as a wakeup call for toymakers who were not adequately protecting the consumer information they collect.[3] I also released a report last year that raised concerns over the privacy risks associated with internet-connected toys and called on toymakers to invest in technology that ensures they are always a step ahead of increasingly sophisticated hackers.[4]

---

[1] *Data from Connected CloudPets Teddy Bears Leaked and Ransomed, Exposing Kids' Voice Messages*, Troy Hunt (Feb. 28, 2017).

[2] *Id.*

[3] *See One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids*, Motherboard (Nov. 27, 2015).

[4] Senate Committee on Commerce, Science, and Transportation, *Children's Connected Toys: Data Security and Privacy Concerns*, 114th Congress (Dec. 14, 2016).

The breach of Spiral Toys raises serious questions concerning how well your company protects the information it collects, especially information collected from children. Additionally, the incident raises questions about Spiral Toys' compliance with the Children's Online Privacy Protection Act (COPPA), a law that, among other things, requires covered companies to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[5]

As Ranking Member of the U.S. Senate Committee on Commerce, Science, and Transportation, I request that you respond to the following inquiries:

1. Provide a summary of the data breach, including, but not limited to:

    a. When the breach occurred;
    b. When and how Spiral Toys first learned of the breach;
    c. What consumer information was compromised in the breach;
    d. What consumer information was potentially accessible to the hackers (i.e., the universe of data stored in the database accessed by the hackers);
    e. How many Spiral Toys consumers were affected, including the number of affected children;
    f. Whether and how Spiral Toys has notified affected consumers (if so, please provide a copy of the notice);
    g. Whether Spiral Toys currently offers, or plans to offer, a free identity theft protection service for impacted consumers;
    h. What security measures Spiral Toys had in place at the time of breach to protect against the risk of unauthorized access to its data;
    i. Whether, prior to the breach, Spiral Toys had a chief information officer (CIO), a chief technology officer (CTO), or an employee with responsibilities similar to those of a CIO or CTO;
    j. Whether, prior to the breach, Spiral Toys provided notice to consumers of its data collection, use, and sharing practices, such as a privacy policy and terms of use (if so, please describe how you provided notice and copies of each notice); and
    k. Whether, prior to the breach, Spiral Toys had policies in place that offered consumers the ability to control data collection, such as the ability to access, correct, and/or delete collected information.

[5] 16 C.F.R §312.8.

2. Does COPPA apply to Spiral Toys' products and/or services? If so, list the products and services to which COPPA applies.

3. For each Spiral Toys product or service that is intended for use by children, identify and provide a description of the consumer information your company collects.

4. Provide a description of how this information is collected and how it is used. If this information is combined with data collected from other sources, describe the additional data and identify the sources.

5. Does Spiral Toys share or sell any of the collected information with or to third parties? If so, please identify and provide a description of these third parties, the information that is shared, how that information is used, and how you notify parents that collected information may be shared or sold with or to third parties.

6. Provide a detailed description of all security procedures that Spiral Toys currently has in place to protect collected consumer information, including a detailed description of how the information is stored and for how long Spiral Toys retains the information.

7. Describe the measures Spiral Toys currently has in place to protect against the risk of unauthorized access to its data. In addition, does your company have in place consumer notification procedures to be used in the event of a breach?

8. During the previous two years, has Spiral Toys suffered any other data breaches impacting consumer data? If so, please provide a detailed description, including what information was compromised, the number of impacted consumers, whether consumer notification of the breach was provided and, if so, a copy of the notification, and whether any free identity theft protection was offered to consumers.

9. Does Spiral Toys provide notice to consumers of its data collection, use, and sharing practices (e.g., privacy policy and terms of use)? If so, please describe how you provide notice and copies of each notice.

10. Can consumers access, correct, and delete the information your company collects about them? If not, why not? If so, please provide a description of the process through which a consumer can access, correct, and delete the information and how your company makes consumers aware of these choices.

Please provide this information as soon as possible but by no later than March 23, 2017. Thank you in advance for your assistance with this matter.

Sincerely,

Bill Nelson

BILL NELSON
Ranking Member

cc: The Honorable John Thune, Chairman

The Honorable Senator Bill Nelson

Ranking Member, United States Senate

Committee on Commerce, Science and Transportation

Dear Senator Nelson,

We really appreciate your efforts and we want to thank you for the opportunity to shed some light on the unfortunate event that happened so that other toy makers can learn from this situation and avoid it in the future. Spiral Toys was the victim of a person illegally entering our database, downloading our data, and then using special scripts to find weak passwords people have entered.

Just for some background on CloudPets, the CloudPets product is a plush stuffed animal toy, that includes a proprietary mobile application which allows, for example, parents to send messages to their children through the product and their smartphone. The messaging component of the toy, and ability to send messages, is controlled exclusively by the parents. We, SpiralToys, are the inventor of the product and technology provider of the toy. We manage the iOS and Android apps and servers for the CloudPets product, but we do not sell the product or own the brand.

The toy is not directly connected to the internet. The receiving mobile app collects messages from the server and then the messages are sent to the toy via the connected phone. This needs to be done by logging into the app by an adult user and manually pushing the messages to the toy. It is not possible for the toys to get messages directly from the Internet without going through the app screening process because the toy uses Bluetooth technology not WiFi.

You can find bellow the answers to each question from your letter.

1a. When the breach occurred.

The breach occurred somewhere between December 27th and January 9th, when our development contractor was conducting a data migration from Parse, a technology which announced their final shutdown at the end of January 2017. We performed data migration tests to a temporarily MongoDB database, which had an unknown security misconfiguration, that could lead to information leakage.

The incident happened on a development server, not on our production server. Being a server used only for data migration tests and not as an operating server, at that time we were not aware of any data breach from an unauthorized person. The vulnerability was fixed as we progressed through the migration process.

In that period, the same MongoDB security misconfiguration also affected more than 28000 servers from companies (other than Spiral/CloudPets) worldwide.

1b. When and how Spiral Toys first learned of the breach.

We first became aware of the breach on February 21st-22nd, when we were contacted by a journalist, Lorenzo Franceschi-Bicchierai, from Vice Media, contacted me on my business email address. Immediately after this we started our internal security investigation to determine when, how and what data was leaked.

Spiral Toys is only the technology provider. The support channels for CloudPets are not run by Spiral Toys, but by the toy's manufacturer. Unfortunately, because of this, we did not receive the warnings from the security experts in time and did not become aware of the breach until Mr. Franceschi-Bicchierai contacted me directly.

1c. What consumer information was compromised in the data breach.

CloudPets user accounts are identified by email address and are available **only** to adult customers (with age-gating). Each user account can have multiple adult/child profiles for sending and receiving voice recordings.

User profiles and friends can record and send voice messages between each other. Messages received by children are played on the toy only after the adult's whose phone is paired with the toy approves the message. Replies are played on the adult's mobile application.

As part of the data breach the following customer information could have been accessed:

- User login information (emails and *bcrypt* hashed passwords).
- Adult and child profile display names (the CloudPets applications don't require users to provide full or real names)
- Child profile day and month of birth (the year of birth is never stored in the database)
- File identifiers for profile pictures and voice messages (all leaked file identifiers were invalidated as part of the migration process and are currently unusable)

We do not request any other personal information from our users. We did not collect or store any geo-location, identity or financial information on our server. (e.g full name, address, full date of birth, social security number, credit card information, etc.)

1d. What consumer information was potentially accessible to hackers. The universe of data stored in the database accessed by hackers.

CloudPets uses the industry standard *bcrypt* algorithm to hash user account passwords making it very difficult for attackers determine a user's password. However, for accounts that used very weak passwords, such as "1234", a hacker might be able to

guess these passwords to gain access to user accounts and also possibly access that user's profile pictures and voice recordings.

1e. How many Spiral Toys consumers were affected, including the number of children.

We do not know whether any consumer, was, in fact, affected and, if so, how many. While the hacker may have had access to email addresses and hashed passwords, the only way any additional information could have been obtained was if the hacker was able to successfully guess a user's password. We do not believe that the hacker would have been able to successfully guess the majority of passwords.

As for users, there were roughly 586,284 user emails and hashed passwords on our server. Reports in the press indicate that more than 800,000 users were part of the leak, the difference between the two numbers is because the table contained anonymous sessions that had no account information attached. The press reports didn't take this information into consideration.

The total number of sub-accounts under the parent user accounts was 718,018. These are not all valid accounts since many users set up multiple accounts on one toy. From our attempts to estimate the number of child accounts, we estimated that there were about 400,000 accounts. These accounts are opened and managed by parents.

1f. Whether Spiral Toys has notified affected customers.

Yes, Spiral toys has sent emails to every customer, not only the affected ones. The email explains the potential breached data and required all users to reset their password. We have also posted a notice on the CloudPets website. Both notifications followed the guidelines supplied by the California Department of Justice.

Before sending the notification emails, as an extra security measure we invalidated all users' passwords, thereby preventing access to the accounts until users created new passwords.

1g. Whether Spiral Toys currently offers, or plans to offer, a free identity theft protection service for impacted consumers.

We do not believe we need to offer identity theft protection since we only collect email addresses as user identifiable information. We do not collect location data, financial data, or any other user identifiable information.

1h. What security measures Spiral Toys had in place at the time of the breach to protect against the risk of unauthorized access to its data.

We do not manage on our own the infrastructure needed to run our services and we rely on 3rd party service providers like Parse or Amazon.

At the time of the data breach the production server used for the mobile applications was hosted and secured by the 3rd party service provider Parse.com. The data was only accessible through the Parse.com Dashboard only by authorized persons.

The test server database was configured with SSL-only access. User accounts with secure passwords and limited access were also created. Unfortunately, due to the security misconfiguration in the MongoDB server, attackers could access the data by circumventing the security measures that were in place.

For user accounts, we use the industry-standard *bcrypt* algorithm to hash the passwords.

As an extra privacy and security feature, all voice messages can be previewed in the APP before they are sent to the toy so a parent can screen all messages before sending them to the toy. We also use a proprietary data encryption method when audio messages are sent from the phone to the connected toy.

1i. Whether, prior to the breach, Spiral Toys has a chief information officer (CIO), a chief technology officer (CTO), or an employee with responsibilities similar to those of a CIO or CTO.

Yes, SpiralToys had employed, and continues to employ, such persons. For example, Spiral employed a CTO. However, in November 2016, Spiral's CTO obtained employment with another company. After November, other employees with responsibilities similar to those of a CIO and/or CTO remained employed by Spiral, including me (I have a degree in electrical engineering with over 20 years experience in the entertainment software industry with Sony Computer Entertainment and Disney).

1j. Whether, prior to the breach, Spiral Toys provided notice to consumers of its data collection, use, and sharing practices, such as a privacy policy and terms of use. (if so, please describe how you provided notice and copies of each notice)

Yes, the terms of use and privacy policy were available when someone made an account through the APP. Users had to explicitly agree and accept our terms and privacy policy in order to create an account.

We also made the privacy policy and terms of service available on our website and they can also be accessed from the app's settings menu for later reference.

1k. Whether, prior to the breach, Spiral Toys had policies in place that offered consumers the ability to control data collection, such as the ability to access, correct, and/or delete collected information.

Yes, we offered our users the ability to control their data collection. Directly through the mobile applications, the users could: edit their account information, edit or delete child profiles, remove friendship records, delete voice recordings.

If a customer contacts us we can also delete their entire user account from our server. Since the data breach we have honored user requests to delete their accounts and associated data from our database that were sent to us via email.

2. Does COPPA apply to Spiral Toys products and/or services? If so, list the products or services to which COPPA applies.

Most of COPPA's rules apply to web applications where kids share information online with other customers. Our application does not enable the features covered under COPPA, but COPPA is a great guideline on how children should be administrated by an operator. Following COPPA's rules, here is how we protect children.

- We do age gate our account set up process. The APP has an age gate and parents need to verify their email.
- We do not collect user identifiable information from children that are covered under COPPA. We only collect a nickname and birth month and day from a child. We do not collect the year. This information is also not required to be entered.
- A parent is the only person that can add friends. Parents can also delete any friend.
- We also enable the parent to screen on all messages before they are sent to the toy. The toy is not connected to the internet. The toy is connected to the APP and the parent needs to push the message to the toy once they review. The toy and the parents APP need to be within 30 feet of each other for the transfer to work.
- Parents have the ability to delete any content at any time and any child account in entirety. When deleted from the APP it is deleted off any server.

3. For each Spiral Toys product or service that is intended for use by children, identify and provide description of the consumer information you company collects.

The only information we collect and use was listed above. That information is only used by the company and only to enable customers to use the service.

4. Provide a description of how this information is collected and how it is used. If this information is combined with data collected from other sources, describe the additional data and identify the sources.

We do not collect any additional data. The APP does not have any user analytics inside of it. We only use the data to enable customers to login and access their services.

5. Does Spiral Toys share or sell any collected information with or to third parties? If so, please identify and provide a description of these third parties, the information that is shared, how that information is used, and how you notify parents that collected information may be shared or sold with or to third parties.

Spiral does not share or sell any information that it collects with 3rd parties. Spiral Toys will only share the email information with the toy manufactures marketing firm Echo Factory. Echo Factory has used the email list in the past to send product update emails to the CloudPets parent customers.

6. Provide a detailed description of all security procedures that Spiral Toys currently has in place to protect collected consumer information, including a detailed description of how the information is stored and for how long Spiral Toys retains this information.

We currently store our information in a secure server for the last 2 years. This has always been the case but during a migration our developer had emails and encrypted passwords in a compromised server. We also use several 3rd party services so secure the data and services.

As stated also in a previous answer, as a privacy feature, the receiving mobile app collects messages from the server and then the messages are sent to the toy via the connected phone. This needs to be done by logging into the app by an adult user and manually pushing the messages to the toy. It is not possible for the toys to get messages directly from the Internet without going through the app screening process.

All communication between the apps and server is made through SSL.

Server administration access is restricted and is made only by authorized personnel and only using a secure channel (SSL/VPN/SSH).

We also have in place a secure daily data backup solution to maintain the data consistency in case of data loss.

Now we also have in place a notification procedure in case of information breach and security issues.

Currently we have no time limit on how long we hold the data. We are evaluating changing our voice message data to 30 days. Parents liked having the service of going back and listening to the older messages but due to the risk and liability for Spiral Toys we may discontinue that service.

7. Describe the measures Spiral Toys currently has in place to protect against the risk of unauthorized access to its data. In addition, does your company have in place consumer notification procedures to be used in the event of a breach.

We have several protections in place to stop unauthorized use.

We have the ability to inform customers through the use of email. We have several email programs that are able to send updates to customers. Since the recent events we have more strict rules for notifying users about security breaches and we have increased the capacity of sending email notifications.

In case of detecting a breach, we can now shut down external access to all services almost instantly in order to analyze the data, patch the issue and send notifications to affected users.

Other security measures we have in place at the moment:

- Remote server access through an encrypted SSH tunnel using PGP
- User restrictions, access controls and authentication procedures based on email address and password, previously validated with a confirmation email
- Monitoring networks and logs for unauthorized activity
- Regular updates and patches to software, libraries and services, both for the server and for the mobile apps

We take into consideration a risk assessment, vulnerability assessment & code review for entire infrastructure's assets, services and products with help from third-party specialists. At the end of the analysis, we will patch discoveries & increase the security measures according to third-party's recommendation.

Furthermore, we plan to develop a disaster recovery plan, a data leakage prevention procedure, a vulnerability assessment procedure and improve our migration procedures, software development life cycle procedures and notification procedure we already have in place.

8. During the previous two years, has Spiral Toys suffered any other data breaches impacting consumer data? If so, please provide a detailed description, including what information was compromised, the number of impacted consumers, whether consumers notification of the breach was provided and, if so, a copy of the notification, and whether any free identify theft protection was offered to consumers.

Spiral Toys has never had a breach before. We have been running the CloudPets service on a 3rd party service called Parse for over two years.

9. Does Spiral Toys provide notice to consumers of its data collection, use, and sharing practices, (e.g privacy policy and terms if use)? If so, please describe how you provide notice and copies if each notice.

We do have our privacy policy and terms of use listed in several places:

- In the mobile app – when the user needs to accept the terms before creating an account
- In the mobile app – in the settings menu
- on our website
- on the mobile app pages in Apple AppStore and Google Play

10. Can consumers access, correct, and delete the information your company collects about them? If not, why not? If so, please provide a description of the process through which a consumer can access, correct, and delete the information and how your company makes consumers aware of these choices.

Yes, customers can edit the information directly from the mobile app, in their account: edit account information, delete individual messages from the server, or delete a child's account in entirety from using the APP. Once they do this the information is changed or deleted from our server.

Since the data breach we have honored user requests to manually delete their accounts and associated data from our database that were sent to us via email.

We appreciate the opportunity to shed some light on the CloudPets data breach. Spiral Toys will continue to make its best efforts to protect their customers. We will continue to improve our security on CloudPets and future products. We have hired a 3rd party consultant to evaluate our data services and help us put in place new and enhanced security measures and safety procedures. If you have any additional questions or concerns please don't hesitate to inquire.

Best Regards,

Mark Meyers

CEO, Spiral Toys