

Happy Holidays: VTech data breach affects over 11 million parents and children worldwide

December 07, 2015 | Blog | By Julia Siripurapu, [Cynthia J. Larose](#)

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

The recent data breach of Hong Kong-based electronic toy manufacturer VTech Holdings Limited ("VTech" or the "Company") is making headlines around the world for good reason: **it exposed sensitive personal information of over 11 million parents and children users of VTech's Learning Lodge app store, Kid Connect network, and PlanetVTech in 16 countries!** VTech's Learning Lodge website allows customers to download apps, games, e-books and other educational content to their VTech products, the Kid Connect network allows parents using a smartphone app to chat with their children using a VTech tablet, and PlanetVTech is an online gaming site. As of December 3rd, VTech has **suspended** all its Learning Lodge sites, the KidConnect network and thirteen other websites pending investigation.

VTech announced the cyberattack on November 27th by [press release](#) and has since issued [follow-on press releases](#) on November 30th and December 3rd, noting that "the Learning Lodge, Kid Connect and PlanetVTech databases have been attacked by a skilled hacker" and that the Company is "deeply shocked by this orchestrated and sophisticated attack." According to the various press releases, upon learning of the cyber attack, VTech "conducted a comprehensive check of the affected site" and has "taken thorough actions against future attacks." The Company has reported that it is currently working with FireEye's Mandiant Incident Response services and with law enforcement worldwide to investigate the attack. According to VTech's [latest update on the incident](#):

- 4, 854, 209 parent Learning Lodge accounts containing the following information were affected: name, email address, secret question and answer for password retrieval, IP address, mailing address, download history and encrypted passwords;
- 6,368,509 children profile containing the following information were affected: name, gender, and birthdate were affected. 1.2 million of the affected profiles have enabled the Kid Connect App, meaning that the hackers could also have access to profile photos and undelivered Kid Connect chat messages;
- The compromised databases also include encrypted Learning Lodge content (bulletin board postings, ebooks, apps, games etc.), sales report logs and progress logs to track games, but, it did not include credit card, debit card or other financial account information or Social Security numbers, driver's license numbers, or ID card numbers; and
- The affected individuals are located in the following countries: USA, Canada, United Kingdom, Republic of Ireland, France, Germany, Spain, Belgium, the Netherlands, Denmark, Luxembourg, Latin America, Hong Kong, China, Australia and New Zealand. The largest number of affected individuals are reported in the U.S. (2,212,863 parent accounts and 2,894,091 children profiles), France (868,650 parent accounts and 1,173,497 children profiles), the UK (560,487 parent accounts and 727,155 children profiles), and Germany (390,985 parent accounts and 508,806 children profiles).

Given the magnitude and wide territorial reach of the VTech cyber attack, the incident is already on the radar of regulators in Hong Kong and at least [two attorneys general in the United States](#). On December 1, the Hong Kong Office of the Privacy Commissioner for Personal Data **announced** that it has initiated "a compliance check on the data leakage incident" of VTech Learning Lodge. In addition, on December 3rd, two separate class actions have already been filed against VTech Electronics North America, L.L.C. and VTech Holdings Limited in the Northern District of Illinois. Since the data breach compromised personal information of children located in the United States (first and last name, photographs, online contact information, etc.), it is likely that the Federal Trade Commission (FTC) will investigate VTech's compliance with the Children's Online Privacy Protection Act ("COPPA") and its implementing rule (as amended, the "[COPPA Rule](#)"). If a COPPA violation is found, the civil penalties can be steep and go up to \$16,000 per violation. In addition to civil penalties imposed by a court, the FTC can require an entity to implement a comprehensive privacy program and to obtain regular, independent privacy assessments for a period of time (you can link [here](#) for a copy of the Mintz Levin Guide to COPPA).

Read More: BBC: <http://www.bbc.com/news/technology-35027504>

New York Times: <http://www.nytimes.com/2015/12/01/business/security-breach-at-toy-maker-vtech-includes-data-on-children.html>

Authors



Julia Siripurapu



Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.