Marketing, LLC; Threadpoint, LLC; PC Global Investments, LLC; Slash 20, LLC; Brent Cranmer, individually and as an o□cer and manager of All Square Marketing, LLC; PC Global Investments, LLC, and Slash 20, LLC; Christopher McVeigh, individually and also d/b/a CMB Marketing, Inc., and as a manager of All Square Marketing, LLC; and Michael Mazzella, individually and also d/b/a Mazzco Marketing, Inc. and as an o□cer and manager of All Square Marketing, LLC, Defendants. According to the complaint, the corporate defendants hired a□liate marketers to send millions of spam text messages to consumers around the country. When consumers clicked on the links in the spam text messages, they were taken to landing pages operated by one group of defendants that asked them to "register" for the free prizes they had been o□ered. The registration process was allegedly a method to collect information about the consumers that was then sold to third parties. Once consumers provided this information, they were taken to sites owned by another group of defendants. On these sites, consumers were told that to win the prize they had been o□ered, they were required to complete a number of "o□ers," many of which involved either paid subscriptions to services, or applying for credit.

- In PCCare247, Inc. and Virtual PC Solutions

descriptions that they were “secure.” In fact, the cameras had faulty software that left them open to online viewing, resulting in hundreds of consumers’ private camera feeds were made public on the Internet.

- The FTC filed a complaint against medical testing laboratory LabMD, Inc. alleging that the company

require the consumer to pay a deposit or pre-pay the first month's bill. Consumers with more favorable credit histories are not required to pay a deposit or the first month's bill. The complaint alleges that Time Warner Cable failed to provide the required risk-based pricing notices to consumers from January of 2011 until March 2013.

- FTC staff members posed as individuals or representatives of companies seeking information about consumers to make decisions related to their creditworthiness, eligibility for insurance or suitability for employment. Following the test-shopping operation, the FTC issued warning letters to ten data brokers that appeared to be selling information for FCRA purposes without following the FCRA requirements.

U.S.-E.U. Safe Harbor

The U.S.-E.U. Safe Harbor Framework provides a way for businesses to transfer personal data from the EU to the U.S. in a manner consistent with EU law. The U.S. Department of Commerce administers the voluntary framework, and the FTC provides an enforcement backstop. To participate, a company must self-certify annually to the Department of Commerce that it complies with the seven privacy principles required to meet the EU's adequacy standard: notice, choice, onward transfer, security, data integrity, access, and enforcement. The FTC is strongly committed to vigilant Safe Harbor enforcement. Since 2009, the FTC has used Section 5 to bring **23 Safe Harbor cases**. During the past year, the FTC brought the following cases:

- Twelve U.S. businesses agreed to settle FTC charges that they falsely claimed they were abiding by the Safe Harbor. The companies settling with the FTC represented a cross-section of industries, including retail, professional sports, laboratory science, data broker, debt collection, and information security. They are: Apperian, Inc.; Atlanta Falcons Football Club, LLC; Baker Tilly Virchow Krause, LLP; BitTorrent, Inc.; Charles River Laboratories International, Inc.; DataMotion, Inc.; DDC Laboratories, Inc.; Level 3 Communications, LLC; PDB Sports, Ltd., d/b/a Denver Broncos Football Club; Reynolds Consumer Products Inc.; Receivable Management Services Corporation; and Tennessee Football, Inc. The FTC also separately entered into a settlement with Fantage.com, the maker of a popular multiplayer online role-playing game directed at children ages 6-16. The FTC complaints charge each company with representing, through statements in their privacy policies or display of a Safe Harbor certification mark, that they held current Safe Harbor certifications, even though the companies had allowed their certifications to lapse. Under the proposed settlement agreement, each company is prohibited from misrepresenting the extent to which it participates in any privacy or data security program sponsored by the government or any other self-regulatory or standard-setting organization.

Children's Privacy

The **Children's Online Privacy Protection Act of 1998 ("COPPA")** generally requires websites and apps to get parental consent before collecting personal information from children under 13. Since 2000, the FTC has brought **over 20 COPPA cases** and collected **millions of dollars in civil penalties**. The FTC recently updated it

- Following a public comment period, the FTC approved the kidSAFE Seal Program as a safe harbor program under COPPA. The COPPA safe harbor provision provides flexibility and promotes e□ciency in complying with the Act by encouraging industry members or groups to develop their own COPPA oversight programs.
- Following a public comment period and review of iVeriFly's proposed COPPA verifiable parental consent method application, the FTC determined it was unnecessary to approve the company's specific method. Under the COPPA Rule, online sites and services directed at children must obtain permission

WORKSHOPS

Beginning in 1996, the FTC has hosted **over 35** workshops, town halls, and roundtables bringing together stakeholders to discuss emerging issues in consumer privacy and security. During this past year, the FTC has hosted the following privacy events:

- In 2014, the FTC hosted a three-part Spring Privacy Series to examine the privacy implications of three new areas of technology that have garnered considerable attention for both their potential benefits and the possible privacy concerns they raise for consumers.
  - The first event focused on the privacy and security implications of mobile device tracking, which involves tracking consumers in retail and other businesses using signals from their mobile devices.
  - The second seminar examined alternative scoring products, which are used for a variety of purposes, ranging from identity verification and fraud prevention to marketing and advertising. Because consumers are largely unaware of these scores, and have little to no access to the underlying data that comprises the scores, the event discussed the privacy concerns and questions raised by such predictive scores.
  - The final seminar examined consumers' use of connected health and fitness devices that regularly collect information about them and transmit this information to other entities
- The staff of the FTC held a workshop in November 2013 entitled *Internet of Things – Privacy and Security in a Connected World* to explore consumer privacy and security issues posed by the growing connectivity of consumer devices, such as cars, appliances, and medical devices.
- At the *Mobile Security: Potential Threats and Solutions* forum in June 2013, FTC staff convened stakeholders to explore the security of existing and developing mobile technologies and the roles various members of the mobile ecosystem can play in protecting consumers from these types of security threats.

CONSUMER EDUCATION AND BUSINESS GUIDANCE

The FTC views its role in educating businesses and consumers about privacy and security issues as critical to its mission. The Commission has distributed **millions of copies of educational materials** for consumers and businesses to address ongoing threats to security and privacy. The FTC has developed extensive materials providing guidance on a range of topics, such as identity theft, internet safety for children, mobile privacy, credit reporting, behavioral advertising, peer-to-peer file sharing, Do Not Call, and computer security. Recent examples of such education and guidance include:

- The FTC recently released an updated version of Net Cetera: Chatting with Kids About Being Online, our guide to help parents and other adults talk to kids about being safe, secure, and responsible online. This new version deals with such topics as mobile apps, public Wi-Fi security, text message spam, and updated guidance on COPPA.
- For consumers who may have been a□ected by the recently announced breaches at major retailers, the FTC posted information online about steps they should take to protect themselves. Many of these retailers recommended that consumers contact the FTC for additional information.
- The FTC has developed both a Business Center Blog and a Consumer Blog that explain, in plain language, recent enforcement actions, reports, and guidance. Some recent examples of blogs about privacy and data security include the announcement of GMR Transcription Services, the FTC's 50th data security settlement; steps that human resources professionals can take to protect sensitive consumer information; and tips for consumers to protect themselves if their data is exposed in a data breach.
- The Commission sponsors OnGuard Online, a website designed to educate consumers about basic computer security. OnGuard Online and its Spanish-language counterpart, Alerta en Línea, average more than 2.2 million unique visits per year.
- The FTC hosted 16 events across the country, along with a series of national webinars and Twitter chats as part of Tax Identity Theft Awareness Week. The events were designed to raise awareness about tax identity theft and provide consumers with tips on how to protect themselves, and what to do if they become victims.
- The FTC widely disseminates a business guide on data security, along with an online tutorial based on the guide. These resources are designed to provide diverse businesses – and especially small businesses – with practical, concrete advice as they develop data security programs and plans for their companies.
- Because mobile applications ("apps") and devices often rely on consumer data, the FTC has developed specific security guidance for mobile app developers as they create, release, and monitor their apps.

INTERNATIONAL ENGAGEMENT

A key part of the FTC's privacy work is engaging with international partners. The agency works closely with foreign privacy authorities, international organizations, and global privacy networks to develop robust mutual enforcement cooperation on privacy and data security investigations and cases. The FTC also plays a lead role in advocating for strong, globally interoperable privacy protections for consumers around the world.

with other U.S. agencies and stakeholders, participated actively in revising the guidelines, which contain key concepts advocated by the agency, including the need for greater e□orts to address the global dimension of privacy through improved interoperability and a rea□rmation of a commitment OECD members made in 2007 to enhance cross-border cooperation among privacy enforcement authorities.

- E□ective enforcement of the U.S.-EU Safe Harbor Framework, which enables data transfers from the European Union to the United States, is an agency priority. This year, in addition to bringing 13 new Safe Harbor actions, discussed above, the FTC provided significant input to the European Commission's review of the framework, highlighting the importance of future cooperation in Safe Harbor enforcement.

  The FTC, together with the Department of Commerce and other U.S. agencies, also is engaged bilaterally in negotiations over improvements to the Safe Harbor. In March 2014, the United States and the European Union pledged to strengthen the Safe Harbor Framework in a comprehensive manner to "ensure data protection and enable trade through increased transparency, e□ective enforcement and legal certainty when data is transferred for commercial purposes."