# Federal Trade Commission
# 2013 Privacy and Data Security Update*

The Federal Trade Commission (FTC or Commission) is an independent U.S. law enforcement agency charged with protecting consumers and enhancing competition across broad sectors of the economy. The FTC's primary legal authority comes from the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace. The FTC also has authority to enforce a variety of sector specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act. This broad authority allows the Commission to address a wide array of practices affecting consumers, including those that emerge with the development of new technologies and business models.

## How Does the FTC Protect Consumer Privacy and Ensure Data Security?

The FTC's principal tool is to bring enforcement actions to stop law violations and require companies to take affirmative steps to remediate the unlawful behavior. This includes, when appropriate, implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and provision of robust notice and choice mechanisms to consumers. If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes, including Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and Do Not Call. To date, the Commission has brought hundreds of privacy and data security cases protecting billions of consumers.

The FTC's other tools include:

- conducting studies and issuing reports
- hosting public workshops
- developing educational materials for consumers and businesses
- testifying before the U.S. Congress and commenting on legislative and regulatory proposals that affect consumer privacy, and
- working with international partners on global privacy and accountability issues

In all of its privacy work, the FTC's goals have remained constant: to protect consumers' personal information and ensure that consumers have the confidence to take advantage of the many benefits offered in the marketplace.

* This document covers the time period from approximately January 2013-March 2014. It will be updated on an annual basis.

# ENFORCEMENT

The FTC has unparalleled experience in consumer privacy enforcement. Its enforcement actions have addressed practices offline, online, and in the mobile environment. It has brought enforcement actions against well-known companies, such as Google, Facebook, Twitter, Microsoft, and Myspace, as well as lesser-known companies. The FTC's consumer privacy enforcement orders do not just protect American consumers; rather, they protect consumers worldwide from unfair or deceptive practices by businesses within the FTC's jurisdiction.

## Privacy

The FTC has brought enforcement actions addressing a wide range of privacy issues, including spam, social networking, behavioral advertising, pretexting, spyware, peer-to-peer file sharing, and mobile. These matters include **over 130 spam and spyware cases** and **more than 40 general privacy lawsuits**. During the past year, the FTC announced the following privacy cases:

- The FTC announced a settlement with Goldenshore Technologies, the maker of a popular flashlight app that promised it would collect information from users' mobile devices for certain internal housekeeping purposes, but failed to disclose that the app transmitted the device's location, precise device ID, and other device data to third parties, including mobile advertising networks.
- Aaron's, Inc., a national rent-to-own retailer, agreed to settle charges that it knowingly played a direct role in its franchisees' installation and use of software on rental computers that secretly monitored consumers, such as by taking webcam pictures of them in their homes. The complaint alleged that Aaron's knew about the privacy-invasive features of the software, but nonetheless allowed its franchisees to access and use the software.
- The Commission settled an enforcement action with Path, a social networking app that accessed users' contacts without permission, in violation of the FTC Act. The settlement requires Path to establish a comprehensive privacy program and to obtain independent privacy assessments every other year for the next 20 years.
- Epic Marketplace, an online advertising company, agreed to settle FTC charges that it used "history sniffing" to secretly and illegally gather data from millions of consumers about their interest in sensitive medical and financial issues ranging from fertility and incontinence to debt relief and personal bankruptcy. The order bars the company from using history sniffing technology or from making misrepresentations to consumers.
- An affiliate marketer, Jason Q. Cruz d/b/a Appidemic Inc., was a subject in a series of FTC complaints targeting the senders of deceptive spam text messages. Cruz agreed to settle charges that he was responsible for sending millions of unwanted text messages to consumers that deceptively promised "free" gift cards and electronics. In its complaint, the FTC alleged that he sent text messages to consumers around the country offering free merchandise, such as $1,000 gift cards to major retailers or free iPads, to those who clicked on links in the messages.
- Twelve defendants that allegedly operated websites enticing consumers with bogus offers and hired affiliates to send spam text messages to promote them agreed to pay $2.5 million in settlements with the FTC. The defendants are: SubscriberBASE Holdings, Inc.; SubscriberBASE, Inc., Jeffrey French, individually and as an officer of SubscriberBASE Holdings, Inc. and SubscriberBASE, Inc.; All Square

Marketing, LLC; Threadpoint, LLC; PC Global Investments, LLC; Slash 20, LLC; Brent Cranmer, individually and as an officer 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 officer and manager of All Square Marketing, LLC, Defendants. According to the complaint, the corporate defendants hired affiliate 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 offered. 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 offered, they were required to complete a number of "offers," many of which involved either paid subscriptions to services, or applying for credit.

- In PCCare247, Inc. and Virtual PC Solutions, the defendants posed as major computer security and manufacturing companies to deceive consumers into believing that their computers were riddled with viruses, spyware and other malware. The complaints alleged that the defendants were not actually affiliated with major computer security or manufacturing companies and they had not detected viruses, spyware or other security or performance issues on the consumers' computers. The defendants charged consumers hundreds of dollars to remotely access and "fix" the consumers' computers.

## Data Security

Since 2002, the FTC has brought **50 cases** against companies that have engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk. During the past year, the FTC brought the following cases:

In its 50th data security settlement, the FTC settled allegations that GMR Transcription Services – an audio file transcription service – violated the FTC Act. According to the complaint, GMR relied on service providers and independent typists to transcribe files for their clients, which include healthcare providers. As a result of GMR's failure to implement reasonable security measures and oversee its service providers, at least 15,000 files containing sensitive personal information – including consumers' names, birth dates, and medical histories – were available to anyone on the Internet.

- According to the FTC, GeneLink, Inc. and its former subsidiary, foru™ International Corp., the makers of genetically customized nutritional supplements, deceptively and unfairly claimed that they had reasonable security measures to safeguard and maintain personal information – including genetic information, Social Security numbers, bank account information, and credit card numbers.

- In Accretive Health, Inc. – a company that provides medical billing and revenue management services to hospitals – the FTC alleged the company failed to provide reasonable security to protect consumers' personal information, including sensitive personal health information, which led to an incident involving an employee's stolen laptop containing 20 million pieces of information on 23,000 patients.

- In its first "Internet of Things" case, the FTC's complaint alleged that TRENDnet marketed its IP cameras for purposes ranging from home security to baby monitoring and claimed in numerous product

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 failed to reasonably protect the security of consumers' personal data, including medical information. The complaint alleges that in two separate incidents, LabMD collectively exposed the personal information of approximately 10,000 consumers. This matter is currently in litigation.
- Mobile device manufacturer HTC settled FTC charges that the company failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers and introducing security flaws that placed sensitive information about millions of consumers at risk. HTC must establish a comprehensive security program, undergo independent security assessments for 20 years, and develop and release software patches to fix security vulnerabilities found in millions of HTC devices.
- The Commission brought a case against Cbr Systems, Inc., a leading cord blood bank, for failing to protect nearly 300,000 customers' personal information, including Social Security numbers, credit and debit card account numbers, and sensitive medical information.

## Credit Reporting & Financial Privacy

The **Fair Credit Reporting Act (FCRA)** sets out rules for companies that use data to determine creditworthiness, insurance eligibility, suitability for employment, and to screen tenants. The FTC has brought **100 FCRA cases** against companies for credit-reporting problems and has collected **over $30 million in civil penalties**. The **Gramm-Leach-Bliley ("GLB") Act** requires financial institutions to send consumers annual privacy notices and allow them to opt out of sharing their information with unaffiliated third parties. It also requires financial institutions to implement reasonable security policies and procedures. Since 2005, the FTC has brought **almost 30 cases for violation of the GLB Act**. During the past year, the FTC brought the following cases:

- TeleCheck Services, Inc., one of the nation's largest check authorization service companies, agreed to pay $3.5 million to settle that they violated the FCRA by failing to follow proper dispute procedures, including refusing to investigate disputes.
- Certegy provided merchants with recommendations as to whether to approve consumers checks, based on their past payment history. The FTC obtained a $3.5 million fine for FCRA violations, alleging that Certegy did not have reasonable procedures to resolve consumer disputes over errors in its database.
- The Commission took action against mobile app developer Filiquarian that compiled and sold criminal record reports without complying with the FCRA. The order bars Filiquarian from furnishing reports to anyone they do not believe has a permissible purpose to use the report, failing to take reasonable steps to ensure the maximum possible accuracy of information conveyed in its reports, and failing to provide users of its reports with information about their FCRA obligations.
- Time Warner Cable, Inc. agreed to pay $1.9 million in civil penalties to settle charges that the company violated the Risk-Based Pricing Rule, which requires creditors to give notice to consumers who are provided less favorable credit terms based on information in their credit reports. According to the complaint, the company gets prospective customers' credit reports to evaluate whether they qualify for video, data, or phone services. If the credit report contains negative information, Time Warner Cable may

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 regulatory rule that implements COPPA to address new developments – such as social networking, smartphone Internet access, and the ability to use geolocation information – that affect children's privacy. (The new rule went into effect July 1, 2013). During the past year, the Commission brought the following case:

- In addition to privacy allegations, the FTC's settlement with Path addressed charges that the social network app also collected information from children under 13 without obtaining parental consent, in violation of COPPA. Path paid $800,000 to settle the COPPA charges.

- 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 efficiency 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 from a child's parents before collecting personal information from that child. The rule includes a provision allowing interested parties to submit new verifiable parental consent methods to the Commission for approval. The FTC determined that iVeriFly's proposed method – which relies on the use of Social Security numbers and knowledge-based authentication questions – is a variation on existing methods already recognized in the Rule, or recently approved by the Commission.

## Do Not Call

In 2003, the FTC amended the **Telemarketing Sales Rule** (TSR) to create a national Do Not Call (DNC) Registry, which now includes more than 221 million unique telephone numbers. Do Not Call provisions prohibit sellers and telemarketers from engaging in certain abusive practices that infringe on a consumer's right to be left alone, including calling an individual whose number is listed with the Do Not Call Registry or who has asked not to receive telemarketing calls from a particular company. Since 2004, the FTC has brought **over 100 cases enforcing Do Not Call Provisions against telemarketers**. Through these enforcement actions, the Commission has sought civil penalties, monetary restitution for victims of telemarketing scams, and disgorgement of ill-gotten gains from the 341 companies and 272 individuals involved. Although a number of cases remain in litigation, the 89 cases that have concluded thus far have resulted in orders totaling **more than $129 million in civil penalties and $824 million in redress or disgorgement**. During the past year, the Commission brought the following cases:

- In Worldwide Info Services, Inc., the FTC and the Office of the Florida Attorney General obtained a court order to stop an operation that used pre-recorded telephone calls, commonly known as robocalls, to pitch purportedly "free" medical alert devices to senior citizens by false representing that the devices had been purchased for them by a relative or friend. The defendants also allegedly led consumers to believe that the devices were endorsed by various health organizations and that they would not be charged anything before the devices were activated.

- Versatile Marketing Solutions settled FTC allegations that the home security company illegally called millions of consumers on the DNC Registry to pitch home security systems. VMS bought phone numbers from lead generators, who had obtained the information obtained by illegal means through rampant use of robocalls. VMS subsequently called these consumers without first checking to see if they had registered their telephone numbers on the DNC Registry, and ignored warning signs that the lead generators were engaged in illegal telemarketing practices.

- The FTC obtained a temporary restraining order to shut down a medical discount scheme by AFD Advisors that scammed seniors across the U.S. by offering phony discounts on prescription drugs and pretending to be affiliated with Medicare, Social Security, or medical insurance providers. According to the FTC, the defendants violated Section 5 of the FTC Act by deceptively presenting themselves as government or insurance representatives, as well as by telling consumers that the discount plans they

were selling could provide substantial discounts on prescription drugs. AFD also violated the TSR for their deceptive acts and for calling consumers whose numbers were on the DNC Registry.

- In Money Now Funding, the FTC obtained a court order halting a business opportunity scheme that allegedly conned more than $6 million from American and Canadian consumers. The FTC alleged that Money Now Funding falsely promised consumers that they could make money by referring merchants in their area to the defendants' non-existent money-lending service. The company violated the TSR by calling phone numbers listed on the DNC Registry, calling consumers who had told them not to call, repeatedly calling consumers to annoy them, using obscenities and threats, and failing to pay the Registry access fee.

- Mortgage Investors Corporation of Ohio, one of the nation's leading refinancers of veterans' home loans, paid a $7.5 million civil penalty, the largest fine the FTC has ever collected for allegedly violating DNC provisions of the TSR. According to the complaint, Mortgage Investors called consumers on the DNC Registry, failed to remove consumers from its company call list upon demand, and misstated the terms of available loan products during telemarketing calls.

- In Resort Solution Trust and Vacation Communications Group, the defendants allegedly called timeshare owners and claimed they had buyers willing to pay a specified price for their properties, or that the timeshares would be sold in a specified period of time. At most, after charging consumers' accounts, the defendants provided agreements to "advertise" consumers' timeshare units. In both cases, the defendants allegedly violated the TSR by calling consumer whose numbers were on the DNC Registry.

- In Skyy Consulting, doing business as CallFire, the company agreed to stop transmitting illegal robocalls to consumers to settle charges that it violated the TSR. CallFire assisted its clients in placing telemarketing robocalls to consumers without their written consent, even though such calls have been illegal since 2009. CallFire also paid a $75,000 civil penalty as part of the settlement.

- Instant Response Systems allegedly used deception, threats, and intimidation to induce elderly consumers to pay for medical alert systems they neither ordered nor wanted. The FTC alleged that telemarketers for Instant Response Systems called elderly consumers – many of whom are in poor health and rely on others for help with managing their finances – to pressure them into buying a medical alert service. The FTC alleged that Instant Response Systems illegally made numerous unsolicited calls to consumers whose phone numbers are listed on the DNC Registry.

# RULES

As directed by Congress, the FTC has authority to develop rules that regulate specific areas of consumer privacy and security. Since 2000, the FTC has promulgated rules in a number of these areas:

- The Health Breach Notification Rule requires certain Web-based businesses to notify consumers when the security of their electronic health information is breached.
- The Red Flags Rule requires financial institutions and certain creditors to have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.
- The COPPA Rule requires websites and apps to get parental consent before collecting personal information from kids under 13. The Rule was recently revised to strengthen kids' privacy protections and gives parents greater control over the personal information that websites and online services may collect from children under 13.
- The GLB Privacy Rule sets forth when financial institutions must provide a consumer with a notice explaining the institution's privacy policies and practices and provide a consumer with an opportunity to opt out of, disclosures of certain information to nonaffiliated third parties.
- The GLB Safeguards Rule requires financial institutions over which the FTC has jurisdiction to develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards.
- The Telemarking Sales Rule requires telemarketers to make specific disclosures of material information; prohibits misrepresentations; limits the hours that telemarketers may call consumers; and sets payment restrictions for the sale of certain goods and services. **Do Not Call provisions** of the Rule prohibit sellers and telemarketers from engaging in certain abusive practices that infringe on a consumer's right to be left alone, including calling an individual whose number is listed with the Do Not Call Registry or who has asked not to receive telemarking calls from a particular company. The Rule also **prohibits robocalls** – prerecorded commercial telemarketing calls to consumers –unless the telemarketer has obtained permission in writing from consumers who want to receive such calls.
- The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Rule is designed to protect consumers from deceptive commercial email and requires companies to have opt out mechanisms in place.
- The Disposal Rule under the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), which amended the FCRA, requires that companies dispose of credit reports and information derived from them in a safe and secure manner.
- The Pre-screen Opt-out Rule under FACTA requires companies that send "prescreened" solicitations of credit or insurance to consumers to provide simple and easy-to-understand notices that explain consumers' right to opt out of receiving future offers.

# 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.
- To discuss the unique challenges facing victims of different types of senior identity theft – tax and government benefits, medical, and long-term care – the FTC hosted *Senior Identity Theft: A Problem in this Day and Age* in May 2013 to explore the best consumer education and outreach techniques for reaching seniors.

## REPORTS AND SURVEYS

The FTC is a leader in developing policy recommendations related to consumer privacy and data security. The FTC has authored **over 50 reports**, based on independent research as well as workshop submissions and discussions, in a number of areas involving privacy and security. Recent examples of such reports and surveys include:

- In March 2012, the FTC issued a landmark Privacy Report, which articulated best practices for companies collecting and using data that can be reasonably linked to a consumer, computer, or device. The FTC's Privacy Report contained three overarching recommendations: privacy by design, enhanced consumer choice, and greater transparency.
- Expanding on the principles outlined in the Privacy Report, FTC staff issued *Mobile Privacy Disclosures: Building Trust Through Transparency* in February 2013, which makes recommendations for all players in the mobile marketplace – platforms, app developers, ad networks and analytics companies, and trade associations – to ensure that consumers get timely, easy-to-understand disclosures about what data companies collect and how that data is used.
- In *Paper, Plastic…or Mobile?: An FTC Workshop on Mobile Payments* (March 2013), the FTC examined the mobile payments ecosystem and highlighted the need for companies to incorporate privacy and security principles into mobile payment products.
- FTC staff issued two surveys about disclosures in mobile apps for children: *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (February 2012) and *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (December 2012). The reports discussed what data is collected from children and how it is shared, and urged industry to take steps so that parents have easier access to information about the data apps are collecting and sharing.

# 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 affected 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.

## Enforcement Cooperation

The FTC cooperates on enforcement matters with its foreign counterparts through informal consultations, memoranda of understanding, complaint sharing, and statutory mechanisms developed pursuant to the U.S. SAFE WEB Act, which authorizes the FTC to share information with foreign law enforcement authorities and provide them with investigative assistance by using the agency's statutory powers to obtain evidence in appropriate cases. During the past year, the FTC took several steps to enhance privacy enforcement cooperation:

- In a Memorandum of Understanding with the United Kingdom's Information Commissioner's Office, the FTC and the U.K. authority agreed voluntarily to engage in mutual assistance and the exchange of information in connection with the enforcement of applicable privacy laws.
- In a Memorandum of Understanding with the Ireland's Office of the Data Protection Commissioner, the FTC and the Irish authority also agreed voluntarily to engage in mutual assistance and the exchange of information to promote increased cooperation and communication between the two agencies in their efforts to protect consumer privacy.
- As part of a joint action by members of the Global Privacy Enforcement Network (GPEN), the FTC sent warning letters to ten data broker companies, described above. This was part of GPEN's first worldwide privacy sweep, which focused on the transparency of online privacy notices. GPEN is an international network of more than 40 privacy enforcement authorities, including the FTC.

## Policy

The FTC advocates for sound policies that ensure strong privacy protections for consumer data that is transferred outside the U.S. and across other national borders. It also works to promote global interoperability among privacy regimes and better accountability from businesses involved in data transfers. During the past year, the FTC played a lead role in these international efforts:

- Through a Mapping Project involving privacy regulators and experts from the Asia Pacific Economic Cooperation (APEC), including the FTC, and the European Union (EU), the FTC continued to contribute to international initiatives on consumer privacy protections for cross-border data flows. The project released a tool, called a "referential," which is designed to serve as a practical reference tool for companies that seek "double certification" under APEC and EU systems for cross-border data transfers. The FTC also continued its work on the implementation of APEC's Cross-Border Privacy Rules (CBPR) System, which was put into place in 2011. The FTC serves as an administrator of APEC's Cross-border Privacy Enforcement Arrangement, which now has 23 participating member authorities.
- The Organization for Economic Cooperation and Development issued revised Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (July 2013), updating the original guidelines from 1980 that became the first set of accepted international privacy principles. The FTC, together

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 efforts to address the global dimension of privacy through improved interoperability and a reaffirmation of a commitment OECD members made in 2007 to enhance cross-border cooperation among privacy enforcement authorities.

- Effective 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, effective enforcement and legal certainty when data is transferred for commercial purposes."