No. 14-3514

IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

FEDERAL TRADE COMMISSION,

Plaintiff-Appellee,

v.

WYNDHAM HOTELS & RESORTS, LLC, *et al.*,

Defendants-Appellants.

On Interlocutory Appeal from an Order of the United States District Court
For the District of New Jersey, No. 2:13-cv-01887-ES-JAD

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND THIRTY-THREE TECHNICAL EXPERTS AND LEGAL SCHOLARS IN SUPPORT OF RESPONDENT

Marc Rotenberg
Counsel of Record
Alan Butler
Julia Horwitz
John Tran
Electronic Privacy Information Center
1718 Connecticut Ave. NW,
Suite 200
Washington, DC 20009
(202) 483-1140

November 12, 2014

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1 and 29(c), *Amicus Curiae* Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE AMICI

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values.[1] EPIC has written extensively on the privacy implications of the collection and storage of sensitive consumer information.

EPIC routinely participates as *amicus curiae* before federal and state courts in cases concerning consumer privacy rights. *See*, *e.g.*, *First Am. Financial Corp. v. Edwards*, 132 S. Ct. 2536 (2012) (defending consumer standing claims); *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011) (defending state prescription privacy law against commercial speech challenge); *Fraley v. Facebook*, No. 13-16918 (9th Cir. Feb. 20, 2014) (defending consumer interests in a class action privacy settlement)*; Joffe v. Google*, 746 F.3d 920 (9th Cir. 2013) (defending Internet users against unlawful interception of private wi-fi communications); Harris v. Blockbuster, Inc., No. 09-10420 (5th Cir. Nov. 9, 2009) (preserving privacy safeguards for video rental records).

[1] The parties consent to the filing of this brief. In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief. This brief was not authored, in whole or in part, by counsel for a party.

EPIC also advocates on behalf of Internet users before the Federal Trade Commission, and frequently files complaints based on the unfair and deceptive practices of companies that put at risk the sensitive user data they gather. As a result of EPIC's complaints, the Commission has brought several important enforcement actions. *See*, *e.g.,* Google, Inc., 152 F.T.C. 435 (2011) (finding that Google violated Section 5 by failing to obtain consent for the use of personal email contacts for a social networking service); Facebook, Inc., FTC No. C-4365, 2012 WL 3518628 (July 27, 2012) (finding that Facebook violated Section 5 by disclosing personal information to third parties contrary to user privacy settings).

EPIC's efforts on behalf of consumers before the Commission are extensive. EPIC has filed suit against the Commission to ensure enforcement of consent orders. *EPIC v. FTC*, 844 F. Supp. 2d 98 (D.D.C. 2012). EPIC has argued that the FTC should require compliance with the Consumer Privacy Bill of Rights in settlements concerning consumer privacy. *See*, *e.g.*, Comments of EPIC, In the Matter of Apperian, Inc., et al., FTC Docket No. 142-3017 (Feb. 20, 2014). EPIC has stated that the Commission should establish a formal and transparent process to assess significant changes in business practices by a company subject to an FTC consent order. *See*, *e.g.*, Comments of EPIC, In the Matter of MySpace, FTC Docket No. 102-3058 (Jun. 8, 2012).

While EPIC believes the FTC can do more to safeguard consumer privacy, there is no dispute that the Commission plays a critical role in safeguarding the privacy and security interests of American consumers. Efforts to carve out a "data security exemption" for the agency's Section 5 authority would be devastating to American consumers.

The EPIC amicus brief is joined by 33 technical experts and legal scholars:

EPIC Technical Experts and Legal Scholars

Alessandro Acquisti, Professor, Heinz College, Carnegie Mellon University

Ann Bartow, Professor of Law, Pace Law School

Colin J. Bennett, Professor, University of Victoria

Francesca Bignami, Professor of Law, George Washington University School of Law

Christine L. Borgman, Professor & Presidential Chair in Information Studies, University of California Los Angeles

Danielle Keats Citron, Lois K. Macht Research Professor of Law, University of Maryland School of Law

Simon Davies, Project Director, London School of Economics

David Farber, Distinguished Career Professor of Computer Science and Public Policy, School of Computer Science, Carnegie Mellon University

Addison Fischer, Former Owner, RSA Data Security; Co-Founder, Verisign

David H. Flaherty, Professor Emeritus of History and Law, University of Western Ontario; Information Privacy Commissioner for British Columbia, 1993-99

Philip Friedman, Friedman Law Offices, PLLC

Pamela Jones Harbour, Senior Vice President & Legal Officer, Global Member Compliance & Privacy, Herbalife

Deborah Hurley, Chair, EPIC Board of Directors

Jerry Kang, Professor of Law, UCLA School of Law

Sheila Kaplan, Founder, Education New York

Ian Kerr, Canada Research Chair in Ethics, Law & Technology, University of Ottawa Faculty of Law

Chris Larsen, CEO, Ripple Labs Inc.

Harry Lewis, Gordon McKay Professor of Computer Science, School of Engineering and Applied Science, Harvard University

Anna Lysyanskaya, Professor of Computer Science, Brown University

Mary Minow, Follett Chair, Graduate School of Library and Information Science, Dominican University

Dr. Pablo Molina, Adjunct Professor, Georgetown University

Peter G. Neumann, Principal Scientist, SRI International Computer Science Lab

Helen Nissenbaum, Professor of Media, Culture and Communication & Computer Science, New York University; Director, Information Law Institute

Ray Ozzie, Founder & CEO, Talko; Former Chief Software Architect, Microsoft

Frank Pasquale, Professor of Law, University of Maryland Francis King Carey School of Law

Dr. Deborah C. Peel, M.D., Founder and Chair, Patient Privacy Rights

Stephanie Perrin, Director, Integrity Policy and Risk Management, Integrity Branch, Service Canada

Chip Pitts, Lecturer, Stanford Law School and Oxford University

Ronald L. Rivest, Professor of Electrical Engineering and Computer Science, Massachusetts Institute of Technology

Pamela Samuelson, Richard M. Sherman Distinguished Professor of Law; Professor of School Information; Co-Director, Berkeley Center for Law & Technology

Bruce Schneier, Security Technologist; Author, Schneier on Security (2008)

Robert Ellis Smith, Publisher, Privacy Journal

Barbara Simons, IBM Research (retired)

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

Consumers in the United States face unprecedented levels of identity theft and financial fraud. This is a direct result of the failure of companies to establish adequate security standards. Data breaches cause billions of dollars in damage each year and incalculable costs in aggravation and concern. As the primary guardian of consumers in the United States, the Federal Trade Commission plays a critical role in safeguarding consumer privacy and promoting stronger security standards.

Removing the FTC's authority to regulate data security would be to bring dynamite to the dam. Data breach incidents are increasing as companies gather detailed personal data they are unable to protect. The risk of even greater danger is very real. The FTC's authority to regulate business practices impacting consumer privacy is well established, the problem is obvious, and the agency has a clear record of success.

Leading technical experts and legal scholars have long argued for stronger data security standards in the United States. Where their advice is followed, companies offer services with the trust and assurance that personal information will be safeguarded. When companies fail to adequately secure the personal data they collect, they fall within the ambit of the FTC's Section 5 authority.

ARGUMENT

The Federal Trade Commission has had a broad mandate since 1914 to safeguard American consumers. *See Am. Fin. Serv. Ass'n v. FTC*, 767 F.2d 957, 966 (D.C. Cir. 1985). The FTC has the authority under Section 5 to regulate "unfair or deceptive acts or practices in or affecting commerce." That language is purposefully broad to ensure that the agency can regulate a wide range of harmful business practices. *FTC v. Sperry & Hutchinson, Co.*, 405 U.S. 233, 239-40 (1972).

Over the last two decades, consumer privacy has become a critical part of the Federal Trade Commission's work.[2] The FTC's Section 5 authority has provided the basis to curb bad business practices and safeguard American consumers. Congress has often supplemented the Section 5 authority with complementary statutory provisions, such as the Fair Credit Reporting Act of 1970 and the Children's Online Privacy Protection Act. But these targeted laws do not diminish the FTC's general authority to regulate privacy practices under Section 5. In recent years, the FTC's enforcement actions have been the main source of privacy protection for American consumers.

[2] *See* Letter from Marc Rotenberg, Director, EPIC, to Commissioner Christine Varney, FTC (Dec. 15, 1995) (calling on the agency to "begin a serious and substantive inquiry into the development of appropriate privacy safeguards for consumers in the information age"), *available at* https://epic.org/privacy/internet/ftc/ftc_letter.html.

Identity theft is the number one concern of American consumers. *See* Press Release, Fed. Trade Comm'n, *FTC Announces Top National Consumer Complaints for 2013* (Feb. 27, 2014).[3] In 2013 alone, the FTC received 290,506 identity theft complaints. *Id.* The Federal Bureau of Investigation has called identity theft is a "key priority" for Americans. FBI, *Identity Theft Overview*.[4] Without the authority to bring enforcement actions against companies that fail to safeguard sensitive consumer data, the FTC would be unable to address the primary concern of American consumers.

I. Consumer Privacy Organizations Rely on the FTC to Enforce Data Protection Standards in the United States

There is currently no comprehensive consumer privacy law in the United States. Instead, Congress has enacted a series of sector-specific rules and relied upon the FTC's broad authority to regulate privacy practices in commerce.[5] While other countries have government agencies dedicated to privacy enforcement, the

[3] http://www.ftc.gov/news-events/press-releases/2014/02/ftc-announces-top-national-consumer-complaints-2013.

[4] http://www.fbi.gov/about-us/investigate/cyber/identity_theft/identity-theft-overview (last visited Nov. 12, 2014).

[5] *See*, *e.g.*, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, §§ 261-64; Fair Credit Reporting Act of 1970 (FCRA), Pub. L. No. 91-508, §§ 1681-1681u; Children's Online Privacy Protection Act of 1998 (COPPA), Pub. L. No. 105-277, 15 U.S.C. §§ 6501-06; Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. § 1232g; Graham-Leach-Bliley Act, 15 U.S.C. § 6801.

United States relies on ad-hoc adjudication by several federal agencies. The FTC is the primary agency charged with protecting consumer privacy in the United States.

The problem of consumer identity theft and fraud is accelerating. According to the most recent National Crime Victimization Survey, seven percent of all Americans over the age of sixteen suffer from identity theft each year. Erika Harrell & Lynn Langton, U.S. Dep't of Justice, No. NCJ 243779, *Victims of Identity Theft, 2012* (Dec. 2013).[6] Nearly one third of the victims whose personal information was used for fraudulent purposes spend more than a month resolving their fraud issues. *Id*. Eighteen percent of adults have had their personal information stolen. Mary Madden, Pew Research Center, *More Online Americans Say They've Experienced a Personal Data Breach* (Apr. 14, 2014).[7]

The sharp increase in the use of software that can prevent companies from gathering personal data also reflects the growing concern of Internet users that companies are unable to protect their personal information. *See* EPIC, *Online Guide to Practical Privacy Tools*.[8] Without the FTC's enforcement, consumers would have little ability to protect the sensitive data they entrust to others.

With the emergence of Internet-based commerce, companies collect far more information about consumers than they did two decades ago. The FTC has

[6] *Available at* http://www.bjs.gov/index.cfm?ty=pbdetail&iid=4821.
[7] http://www.pewresearch.org/fact-tank/2014/04/14/more-online-americans-say-theyve-experienced-a-personal-data-breach.
[8] https://epic.org/privacy/tools.html.

used its Section 5 "deception" authority to hold companies accountable for their privacy policies, to require companies to provide notice before they disclose personal information to third parties, and to establish reasonable data security safeguards. The FTC has also used its Section 5 "unfairness" authority to prohibit companies from retroactively changing the terms of their privacy promises, to prevent improper use of collected data, and to ensure that sensitive data is adequately safeguarded.

For example, following a complaint filed by EPIC,[9] the FTC entered into a consent decree with Snapchat, a mobile photo-sharing app that claimed to allow users to take photos that would "vanish." Snapchat, Inc., FTC File No. 132-3078, 2014 WL 1993567 (May 8, 2014). The FTC found that Snapchat did not actually delete the images from users' phones, but merely hid them; the files could be easily recovered from the phone's memory. *Id*. As a result of the FTC's action, Snapchat will be subject to 20 years of privacy audits and will be prohibited from making false claims about its privacy policies. *Id*.[10]

The FTC has also found it deceptive for companies to transfer personal user information to third parties without first obtaining meaningful consent. In the Commission's 2012 settlement with Facebook, which followed from a Complaint

[9] Complaint of EPIC et al. before the FTC, In the Matter of Snapchat, Inc. (May 16, 2013), *available at* https://epic.org/privacy/ftc/EPIC-Snapchat-Complaint.pdf.
[10] The final consent order is still pending.

filed by EPIC and a coalition of privacy and civil liberties organizations,[11] the FTC found that Facebook "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public." Press Release, Fed. Trade Comm'n, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises* (Nov. 29, 2011). Facebook agreed to a consent decree whereby it is:

- barred from making misrepresentations about the privacy or security of consumers' personal information;
- required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences;
- required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account;
- required to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services, and to protect the privacy and confidentiality of consumers' information; and
- required, within 180 days, and every two years after that for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers' information is protected.

Id.

These FTC enforcement actions, brought under Section 5, are critically important for consumers. After a company obtains a consumer's personal information, the consumer no longer has the ability to limit the disclosure to third

[11] Complaint of EPIC et al. before the FTC, In the Matter of Facebook, Inc. (Dec. 17, 2009), *available at* https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

parties or to ensure adequate security standards. In the 2012 Facebook case, the FTC found that:

> by designating certain user profile information publicly available that previously had been subject to privacy settings, Facebook materially changed its promises that users could keep such information private. Facebook retroactively applied these changes to personal information that it had previously collected from users, without their informed consent. . . .This practice constitutes an unfair act or practice.

Facebook, Inc., FTC No. C-4365, 2012 WL 3518628, at *6 (July 27, 2012).

Consumers face unique risks when they use online services. Companies now collect vast amounts of personal information, from pages viewed and searches made, to credit card numbers, bank account information, and even social security numbers and location information. Consumers may expect that the data is gathered for a narrow purpose associated with a particular service, but once the data is in the possession of the company the consumer loses any meaningful ability to limit its use.

One particularly vivid example is Google's collapse of privacy policies in 2012, which allowed the company to merge user data across dozens of distinct services, well beyond what users initially agreed to. Google simply changed the terms of service for several hundred million users of more than sixty Google services, including Gmail, Google+, YouTube, and the Android mobile operating

system. *Updating our Privacy Policies and Terms of Service*, The Google Blog (Jan. 24, 2012).[12]

II. Data Breaches Impose Enormous Costs on Consumers and Businesses

Data security enforcement by the FTC is increasingly important because corporate data breaches cause substantial harm to consumers and businesses. Data breaches expose billions of sensitive records are exposed every year, putting consumers at risk of identity theft and credit card fraud. Fraud also produces long-term damage to consumer credit and requires expensive monitoring services.[13] This makes data security one of the most important regulatory priorities for the FTC today.

A. Data Breaches Cause Hundreds of Millions of Dollars in Damage Every Year

Last year the cost of credit card fraud in the United States grew to $7.1 billion, at least $500 million of which was attributable to "[r]ecord-breaking data breaches at major retailers." John Heggestuen, *The US Sees More Money Lost to Credit Card Fraud Than the Rest of the World Combined*, Business Insider (Mar.

[12] http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html.
[13] *See generally* Fed. Trade Comm'n, *Identity Theft*, http://www.consumer.ftc.gov/features/feature-0014-identity-theft (last visited Nov. 12, 2014).

5, 2014).[14] Surveys indicate that more than forty percent of Americans have "experienced some form of payment card fraud in the last five years." *Skimming Off the Top*, The Economist, Feb. 5, 2014.[15] Data breaches were "one of the main sources of fraud last year," and a recent report found that "one in three people who received notifications of a data breach" have discovered that they were subject to fraud. Blake Ellis, *Identity Fraud Hits New Victim Every Two Seconds*, CNN Money (Feb. 6, 2014).[16] The costs of these breaches have increased exponentially over the last few decades.

In 1974 the Chamber of Commerce estimated that computer crime cost the country over $100 million. U.S. Chamber of Commerce, *A Handbook On White Collar Crime* 4-6 (1974). Today that number could be over $100 billion, almost half a percentage of the total United States GDP. *See* Ctr. for Strategic and Int'l Studies, *Net Losses: Estimating the Global Cost of Cybercrime - Economic Impact of Cybercrime II* 21 (2014).[17] One annual report, incorporating statistics from a broad spectrum of companies and law enforcement agencies, estimated that the number of data breaches per year increased from roughly 100 to over 1,000

[14] http://www.businessinsider.com/the-us-accounts-for-over-half-of-global-payment-card-fraud-sai-2014-3.
[15] *Available at* http://www.economist.com/news/finance-and-economics/21596547-why-america-has-such-high-rate-payment-card-fraud-skimming-top.
[16] http://money.cnn.com/2014/02/06/pf/identity-fraud/.
[17] *Available at* http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

between 2004 and 2013. Verizon Enterprise Solutions, *2014 Data Breach Investigations Report* 8 (2014) [hereinafter *Verizon Report*].[18]

Financial losses due to personal identity theft totaled $24.7 billion in 2012, over $10 billion more than the losses attributed to all other property crimes. *Victims of Identity Theft, 2012* at 4. And these figures do not reflect the fraud and identity theft resulting from major data breaches over the last year. In May of 2014 it was estimated that the personal information of 110 million Americans–roughly half of the nation's adults–had been exposed in the prior year. Jose Pagliery, *Half of American Adults Hacked This Year*, CNN Money (May 28, 2014).[19]

B. Recent Breaches Have Impacted Tens of Millions of Consumers

Data breaches are increasing in both frequency and impact. Computer criminals infiltrate corporate networks to obtain credit card details and bank account information in much larger data sets than in the past. A single breach can expose the identities of tens of millions of individuals. Many of these breaches were the result lax data security practices and led to fraudulent charges on consumer credit cards.

In 2013, there were eight "mega breaches," a breach "that resulted in the *personal details of at least 10 million identities being exposed in an individual*

[18] *Available at* http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf.
[19] http://money.cnn.com/2014/05/28/technology/security/hack-data-breach.

incident." Symantec, *Internet Security Threat Report* 12 (2014) (emphasis added).[20] These mega breaches exposed hundreds of millions of records, including names, birth dates, social security numbers, addresses, medical records, phone numbers, financial information, e-mail addresses, user names and passwords, and insurance information. *Id*. Companies may be the targets of the attack but "[u]ltimately, consumers are the real victims of data breaches, as they face many serious risks as a result of this cybercrime." *Id*. at 42.

Breaches over the past year have imposed severe financial harm on consumers. *See*, *e.g.*, John Vomhof Jr., *Target's Data Breach Fraud Cost Could Top $1 Billion*, Charlotte Bus. J. (Feb. 23, 2014) (estimating fraudulent charges of between $1.4 billion and $2.2 billion resulting from the Target data breach);[21] Elizabeth Weise, *Massive Data Breaches: Where They Lead is Surprising*, USA Today (Oct. 3, 2014) (citing examples of several small financial institutions that have already seen more than $100,000 in fraudulent transactions resulting from the Home Depot breach); Robin Sidel, *Fraudulent Transactions Surface in Wake of Home Depot Breach*, Wall St. J. (Sep. 23, 2014) (same).[22] Experts have also

[20] *Available at* http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.
[21] http://www.bizjournals.com/charlotte/news/2014/02/03/targets-data-breach-fraud-cost-could-top-1-billion.html.
[22] http://online.wsj.com/articles/fraudulent-transactions-surface-in-wake-of-home-depot-breach-1411506081.

warned that the recent JP Morgan breach could lead to years of fraud at the consumers' expense. Jim Finkle & Karen Freifeld, *States Probe JPMorgan Chase as Hack Seen Fueling Fraud*, Reuters (Oct. 3, 2014).[23]

The most extreme breaches over the last year include credit card breaches at major retailers and exposure of user information at large Internet service providers. Up to 110 million people, about a third of the U.S. population, had sensitive information stolen from Target between November 27 and December 15, 2013. Grant Gross, *Update: Breach Exposes Data on 110 Million Customers, Target Now Says*, Computer World (Jan. 10, 2014);[24] *see also* Paul Ziobro & Danny Yadron, *Target Now Says 70 Million People Hit in Data Breach*, Wall St. J. (Jan. 10, 2014).[25] The data breach exposed customer names, credit and debit card numbers, card expiration dates, and CVVs (card verification values). *Id*. A result of a recent breach at Neiman Marcus may have compromised one million customer credit cards between mid-July to late October of 2013. Andrew Harris, *Neiman Marcus Sued Over Customer Credit Card Data Breach*, Bloomberg (Mar. 13,

[23] http://www.reuters.com/article/2014/10/03/us-jpmorgan-cybersecurity-idUSKCN0HS1ST20141003.

[24] http://www.computerworld.com/article/2487587/cybercrime-hacking/update--breach-exposes-data-on-110-million-customers--target-now-says.html.

[25] http://online.wsj.com/articles/SB10001424052702303754404579312232546392464.

2014).[26] More than three million Michael's customers had their credit card information exposed during an eight-month period during 2013. Amrita Jayakumar, *Michaels Says 3 Million Customers Hit by Data Breach*, Wash. Post (Apr. 19, 2014).[27] And more than sixty million Home Depot customers' card numbers were exposed over five months due to a data security failure. Robin Sidel, *Home Depot's 56 Million Card Breach Bigger Than Target's*, Wall St. J. (Sep. 18, 2014).[28]

In simple terms, data security is one of the top concerns of American consumers. The problem is bad and it is getting worse.

III. The FTC's Enforcement Actions Are Necessary to Ensure That Companies Adopt Sufficient Data Privacy and Security Safeguards

The FTC has long recognized that lax data security practices can lead to significant consumer harm. To curb such practices, the FTC has brought enforcement actions against companies who fail to adequately protect sensitive data. The FTC has already settled more than 50 data security cases arising out of its investigations. As a result, the FTC has developed expertise in detecting the greatest data security risks to American consumers. The FTC's enforcement

[26] http://www.bloomberg.com/news/2014-03-12/neiman-marcus-sued-over-customer-credit-card-data-breach.html.
[27] http://www.washingtonpost.com/business/economy/michaels-says-nearly-3-million-customers-hit-by-data-breach/2014/04/18/3074e432-c6fc-11e3-8b9a-8e0977a24aeb_story.html.
[28] http://online.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.

actions have focused on three different data security problems: the failure to secure internal networks, the failure to encrypt sensitive data, and the failure to screen and monitor third party access.

The FTC has brought many actions against companies for failure to encrypt sensitive customer data. These companies left their networks vulnerable to attacks and stored sensitive information about consumers in plaintext. The criminals who accessed the unsecured networks could also access the sensitive information stored in the databases. Some companies left their networks vulnerable to SQL injections and stored sensitive consumer information in clear readable text. *See*, *e.g.*, Life is Good, Inc., FTC No. C-4218, 2008 WL 1839971 (Apr. 16, 2008), Genica Corp., FTC No. C-4252, 2009 WL 783713 (Mar. 16, 2009), Stipulated Final Judgment, *United States v. ValueClick, Inc.*, No. 08-1711 (C.D. Cal. Mar. 17, 2008). Other companies failed to physically secure their systems, and allowed hard drives containing sensitive customer information to be stolen. *See, e.g.,* Accretive Health, Inc., FTC No. C-4432, 2014 WL 726603 (Feb. 5, 2014). One company failed to use a secure File Transfer Protocol, making sensitive health data easily accessible by any search engine. *See* GMR Transcription Servs., Inc., FTC No. C-4482, 2014 WL 4252393 (Aug. 14, 2014).

The Commission has also brought actions against companies that claimed to protect sensitive consumer data, but failed to use basic encryption tools. *See, e.g.,*

Upromise, Inc., FTC No. C-4351, 2012 WL 1225058 (Mar. 27, 2014); Ceridian Corp., 151 F.T.C. 514 (2011); Stipulated Final Judgment, *FTC v. Lifelock, Inc.*, No. 10-1793 (D. Ariz. Feb. 23, 2010).[29] In one notable case, a company not only stored sensitive consumer data in plaintext, but also transmitted the data over an unsecured network. *See* Compete, Inc., 155 F.T.C. 264 (2013).

The FTC has also brought "deception" actions against companies that failed to properly limit and monitor third party access to their customer data. Some companies failed to authenticate user credentials, so that sensitive consumer data was transmitted to unintended recipients. *See, e.g.,* Snapchat, Inc., FTC File No. 132-3078, 2014 WL 1993567 (May 8, 2014) (final consent order currently pending); Stipulated Final Judgment, *United States v. Rental Research Servs., Inc.*, No. 09-524 (D. Minn. Mar. 6, 2009). Other companies transmitted consumer data to an intended recipient without obtaining consumers' consent. *See, e.g.,* Goal Financial, LLC, FTC No. C-4216, 2008 WL 1779208 (Apr. 9, 2008). And still other companies failed to adequately audit and secure their sensitive databases after they learned they had been hacked. *See* Reed Elsevier, Inc., FTC No. C-4226, 2008 WL 3150420 (July 29, 2008).

[29] *Available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockstip.pdf.

Finally, the Commission has investigated several companies that granted permissions to software developers and data resellers without verifying the third parties' data security practices. For instance, in Premier Capital Lending, Inc., FTC No. C-4241, 2008 WL 5266769 (Dec. 10, 2008), a financial data broker allowed home real estate sellers to access the company's database without ensuring that the seller had secured its own networks. When a seller's network was subsequently attacked, the criminal gained access to the data broker's database. And in HTC America, Inc., FTC No. C-4406, 2013 WL 3477025 (June 23, 2013), the manufacturer of Android-based mobile phones delivered cellular devices containing programming flaws that allowed third-party applications to bypass Android's permission-based security model.

In response to the FTC's enforcement efforts, companies have entered into consent decrees and agreed to a range of remedial measures to prevent future data breaches.

For example, companies have agreed to establish and maintain comprehensive data security programs and submit to security audits by independent auditors. *See*, *e.g.*, Foru Int'l Corp., FTC No. C-4457, 2014 WL 2142612 (May 8, 2014); James B. Nutter & Co., FTC No. C-4258, 2009 WL 1818012 (June 12, 2009). Others have agreed to designate an employee responsible for data security programs and to conduct regular risk assessments. *See*, *e.g.*,

Fajilan and Associates, Inc., 152 F.T.C. 389 (2011); ACRAnet, Inc., 152 F.T.C. 367 (2011); Settlementone Credit Corp., FTC No. C-4330, 2011 WL 3726287 (Aug. 17, 2011); Lookout Serv., Inc., 151 F.T.C. 532 (2011).

Some companies have agreed to block the installation of unauthorized software on company networks that contain sensitive consumer health and financial information. *See*, *e.g.*, EPN, Inc., FTC No. C-4370, 2012 WL 5375158 (Oct. 3, 2012); Franklin's Budget Car Sales, Inc., FTC No. C-4371, 2012 WL 5375157 (Oct. 3, 2012). Some have also agreed to provide copies of all consumer complaints, law enforcement subpoenas, and widely-disseminated policy statements for FTC inspection. *See*, *e.g.*, Twitter, Inc., FTC No. C-4316, 2011 WL 914034 (Mar. 2, 2011). And most importantly, companies have agreed to make changes to secure company networks, monitor network traffic, and block the flow of personal information out of company networks. *See*, *e.g.*, Dave & Buster's, Inc., 149 F.T.C. 1449 (2010); Fandango, LLC, FTC No. C-4481, 2014 WL 4252396 (Aug. 13, 2014); Credit Karma, Inc., FTC No. C-4480, 2014 WL 4252397 (Aug. 13, 2014).

The FTC's enforcement actions have led to significant changes in the business practices of companies that failed to protect sensitive data. And these actions have also provided guidance to other companies in how to ensure that consumer information is protected.

IV. Widely Accepted Data Security Standards Already Guide The Secure Handling of Consumer Data; Companies Who Fail to Follow These Guidelines Put Consumers At Risk

Industry standards for data protection provide clear guidance for companies that handle sensitive consumer data. These standards, combined with more than 50 FTC consent agreements, provide companies with ample warning about potential data security failures. Companies cannot justifiably claim ignorance of data security risks given the number of enforcement actions and the scope of industry guidance.

A. Current Cybersecurity Frameworks Provide Clear Guidance for Saefguarding Sensitive Customer Data

Over many years, industry groups have developed security standards to combat data breaches. They have now consolidated these standards into a comprehensive data security framework.

Companies that process major credit cards, including the respondent in this matter, must meet the Payment Card Industry Data Security Standard ("PCI DSS"). PCI Sec. Stds. Council, *Requirements and Data Security Procedures* 5 (2013).[30] The PCI DSS is a self-regulatory standard created by major credit card companies and designed "to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally." *Id*. "The PCI standards are probably the biggest non-government security standard." Bruce

[30] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

Schneier, *PCI Lawsuit*, Schneier.com (Jan. 16, 2012).[31] Industry standards like the PCI DSS "are building a foundation for a stronger duty of care for firms to adequately protect consumer information." Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 Berkeley Tech. L.J. 1061, 1083 (2009).

More generally, the National Institute of Standards and Technology ("NIST") has set out a Framework for Improving Infrastructure Cybersecurity ("Framework") to provide guidance for companies to manage cyber risks. Nat'l Inst. of Stds. & Tech., U.S. Dep't of Commerce, Framework for Improving Critical Infrastructure Cybersecurity (2014) [hereinafter NIST Framework].[32] NIST is the "leading source of independent technology expertise in the U.S. government." Edward Felten, *NIST Recommends Not Certifying Paperless Voting Machines*, Freedom to Tinker (Dec. 1, 2006).[33] The Framework is a product of the President's initiative to improve cybersecurity in the U.S., and includes a collection of cybersecurity best practices established by widely-adopted data security standards, which have been organized into a roadmap for companies seeking to secure their

[31] https://www.schneier.com/blog/archives/2012/01/pci_lawsuit.html.
[32] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
[33] https://freedom-to-tinker.com/blog/felten/nist-recommends-not-certifying-paperless-voting-machines/.

networks. *See* Exec. Order No. 13636, 78 Fed. Reg. 11737 (2013); NIST Framework at 7.

The Critical Security Controls standard ("CSCs") originated from protocols developed by the National Security Agency and were subsequently refined by an international consortium of government agencies, private industry groups, and non-profit organizations. *See* SANS Institute, *Critical Security Controls: A Brief History* (2014);[34] Council on CyberSecurity, *The Critical Security Controls for Effective Cyber Defense* (2014) [hereinafter CSCs].[35] The CSCs are currently maintained by the Council on CyberSecurity, a non-profit formed to "accelerate the widespread availability and adoption of effective cybersecurity measures, practice and policy." Council on CyberSecurity, *About Us* (2014).[36] The NIST Framework also references Special Publication 800-53 ("NIST SP 800-53"), NIST's catalog of cybersecurity controls and procedures approved for federal government computer systems. Joint Task Force, Transformation Initiative, Nat'l Inst. For Stds. & Tech., U.S. Dep't of Commerce, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Pub. No. 800-53, at ii (April 2013) [hereinafter NIST SP 800-53].[37]

---

[34] http://www.sans.org/critical-security-controls/history.
[35] http://www.counciloncybersecurity.org/bcms-media/Files/Download?id=a52977d7-a0e7-462e-a4c0-a3bd01512144.
[36] http://www.counciloncybersecurity.org/about-us/.
[37] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

These well-established cybersecurity best practices have converged on three key steps to ensuring data security: identify, protect, and respond.

The first step in securing any network is to identify and inventory all hardware devices on the network. CSCs at 9; NIST SP 800-53 at F-73. Companies should "[a]ctively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access." CSCs at 9. Under the CSCs, companies must regularly monitor their device inventory by sending ping packets to identify devices connected to the network or verifying MAC addresses collected by network switches and routers. CSCs at 10-11. Similarly, NIST SP 800-53 requires federal agencies to develop an inventory of networked devices that monitors machine names and network addresses. NIST SP 800-53 at F-73.

Next, companies must implement measures to ensure that sensitive data is protected from exposure. Such measures include: maintaining firewalls, encrypting sensitive data, and prohibiting default or simple system passwords. *See* NIST Framework at 23-26. Firewalls regulate computer traffic into and within an organization's network and are "a key protection mechanism for any computer network." PCI DSS at 19. *See* CSCs at 55; NIST SP 800-53 at F-188. Cyber attacks exploit vulnerable firewalls to gain access to networks, manipulate traffic,

and steal data. CSCs at 55. Companies should ensure that firewalls are regularly monitored and kept up to date with the latest stable security patches. CSCs at 56; PCI DSS at 50; NIST SP 800-53 at F-215.

Encryption is "the process of converting plaintext into ciphertext using a cryptographic algorithm and key." Elaine Barker et al., Nat'l Inst. of Stds. & Tech., U.S. Dep't of Commerce, Special Pub. 800-57, *Recommendation for Key Management Part 1: General (Rev. 3*), at 22 (July 2012) [herenafter NIST SP 800-57].[38] Proper encryption policies mitigates the harm of a data breach by rendering data useless without the key. CSCs at 90. Best encryption practices include the use of industry-tested and accepted cryptographic algorithms identified by NIST and compliance with the Federal Information Processing Standard. PCI Sec. Stds. Council, *Glossary of Terms, Abbreviations, and Acronyms* 18 (2014) (definition of "strong cryptography");[39] CSCs at 90; see NIST SP 800-57 at 17. Such algorithms include AES (128 bits and higher), TDES (minimum triple-length keys), RSA (2048 bits and higher), ECC (160 bits and higher), and ElGamal (2048 bits and higher). PCI DSS Glossary, *supra*, at 18.[40] Companies should also deploy tools to automatically monitor networks to detect unauthorized exfiltration of sensitive

[38] http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf.
[39] https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3.pdf.
[40] The RSA (Rivest, Shamir, Adleman) algorithm was co-invented by Ronald Rivest. EMC^2, *RSA Laboratories, RSA Algorithm* (2014), http://www.emc.com/emc-plus/rsa-labs/historical/rsa-algorithm.htm.

information. CSCs at 91. Furthermore, companies should regularly scan servers to identify and encrypt or destroy sensitive information stored in plaintext. CSCs at 91.

Another fundamental but frequently overlooked, data security best practice is the use of adequately complex passwords. CSCs at 86; PCI DSS at 28; NIST SP 800-53 at F-91. Attackers frequently gain access to networks through default accounts and passwords that have not been changed. PCI DSS at 28; Trustwave, *Global Security Report* (2014).[41] Weak passwords contributed to thirty-one percent of data breaches in 2012. *Id*. (finding the most commonly used password in the U.S. in 2012 was "123456."). Default passwords and accounts should be removed or disabled before any device or system is connected to a company's network. PCI DSS at 28; CSCs at 86. Under the CSCs, passwords should contain letters, numbers, and special characters; change every 90 days; and not be identical to the previous 15 passwords. CSCs at 86.

Finally, companies must create a response plan in anticipation of a network breach or security failure,. The plan must define the roles, strategies, and procedures to be implemented in the event of a cyberattack. CSCs at 96-97; PCI DSS at 97; NIST SP 800-53 at F-108-09. An adequate incident response plan

41 https://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf.

establishes how quickly network administrators must report anomalous activity to incident response teams and the steps that those teams must take upon receiving a report. CSCs at 96-97; PCI DSS at 105-06; NIST SP 800-53 at F-107. Incident response plans must be updated regularly to enable a company to effectively respond to repeat or emerging threats. NIST SP 800-53 at F-107; PCI DSS at 106; CSCs at 97.

When companies fail to follow these important steps to secure sensitive consumer data, they create huge risks for their customers and for other businesses who could be harmed by fraud or identity theft.

B. The President Has Emphasized the Importance of Data Security

1) Under the President's Consumer Privacy Bill of Rights Consumers Have the Right to Secure Handling of Personal Data

President Obama has also recognized the need to set out broad principles to safeguard consumer information. The President has created a framework for safeguarding consumer privacy, the Consumer Privacy Bill of Rights ("CPBR"), based on the widely known Fair Information Practices ("FIPs"). White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy* (2012) [hereinafter CPBR].[42] As the President explained:

> As the Internet evolves, consumer trust is essential for the continued growth of the digital economy. That's why an online privacy Bill of

[42] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

> Rights is so important. For businesses to succeed online, consumers must feel secure. By following this blueprint, companies, consumer advocates and policymakers can help protect consumers and ensure the Internet remains a platform for innovation and economic growth.

Press Release, The White House, *We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online* (Feb. 23, 2012).[43]

The FIPs, on which the CPBR is based, were first articulated in a 1973 report for the Secretary on Health, Education, and Welfare ("HEW"). Willis H. Ware, Chairman, Secretary's Advisory Comm. on Automated Personal Data Sys., U.S. Dep't of Health, Education, and Welfare, DHEW Pub. No. (OS)73-94, *Records, Computers and the Rights of Citizens* (1973). The Ware Report recommended that any institution that keeps records on individuals must safeguard the rights of each individual's right to his or her information. The Ware Report also recommended five FIPs. The Final FIP read, "Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data."

EPIC has frequently recommended that the Commission make compliance with the CPBR one of the elements of settlement with companies subject to

[43] *Available at* http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

consent orders. In comments to the Commission on proposed settlements with companies that made misrepresentations regarding compliance with the Safe Harbor Arrangement, EPIC proposed that "[b]y requiring compliance with the CPBR, the Commission will ensure that the personal data of consumers is protected throughout the data lifecycle. More importantly, the Commission will put in place the baseline privacy standards that are widely recognized around the world and necessary to protect the interests of consumers." Comments of EPIC, *Apperian, Inc. et al.*, FTC File Nos. 142-3017-3020; 142-3022-3024; 142-3028; 142-3025; 142-3030-3032 (Feb. 25, 2014).

EPIC has made the same recommendation in settlement proceedings where the FTC has asked for public comment. *See*, *e.g.*, Comments of EPIC, MySpace, LLC., FTC File No. 102-3058 (Jun. 8, 2012) ("These principles would impose certain requirements on the collection and use of personal information in the social networking context.");[44] Comments of EPIC, Facebook, Inc., FTC File No. 092-3184 (Dec. 17, 2011) (urging the Commission to require Facebook to adopt many of the FIPs in the 2012 consent agreement).[45]

[44] *Available at* https://epic.org/privacy/socialnet/EPIC-Myspace-comments-FINAL.pdf.
[45] *Available at* https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf.

2) The President Has Ordered the Federal Government to Adopt the More Secure Chip-and-PIN Card Payment System

The President's recent order that the federal government adopt more secure payment systems that use chip-and-PIN technology illustrates the gravity of the risk of consumer data breaches. Exec. Order No 13681, 79 Fed. Reg. 63489 (2014).[46] Unlike traditional credit cards that store unencrypted data in an easily cloned magnetic strip, chip-and-PIN cards embed data in a secure chip and require users to enter a PIN to complete the transaction. Leo King, *Is The US Finally Accelerating A Move To Chip And Pin?*, Forbes (Oct. 21, 2014).[47] The adoption of chip-and-PIN technology, explained the President, is an important step in preventing credit card fraud and identity theft, which affected millions of Americans last year. Presidential Statement on Executive Order 13681, 2014 Daily Comp. Pres. Doc. 778 (Oct. 17, 2014).

Companies, too, are recognizing the threat to consumer data from insecure payment systems. Retailers such as Home Depot, Target, Walgreens, and Walmart have pledged to adopt the chip-and-PIN standard by early 2015. Press Release, The White House, *Fact Sheet: Safeguarding Consumers' Financial Security* (Oct. 17,

[46] http://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions.
[47] http://www.forbes.com/sites/leoking/2014/10/21/is-the-us-finally-accelerating-a-move-to-chip-and-pin/

2014).[48] Card issuers like American Express are also adopting the more secure payment standard. American Express, *Chip and PIN* (2013).[49] The adoption of chip-and-PIN by government and private industry reflects a growing awareness of the need to implement improved standards to protect consumer data.

C. Recent Incidents Show That a Failure to Follow Data Security Standards Can Lead to Harmful Data Breaches

Two recent data breaches at Home Depot and Target demonstrate that wide-scale harm to consumers that can result from companies' failure to follow data security standards.

For example, the September 2014 Home Depot data breach resulted in the exposure of 50 million credit cards to fraudulent charges. Press Release, The Home Depot (Sept. 18, 2014).[50] Those issues could likely have been avoided if the company had followed many of the basic security best practices: updating its software; encrypting payment data, including credit card numbers, during transfers; maintaining adequate firewalls; and performing regular vulnerability scans of its systems. Ben Elgin, et al., *Former Home Depot Managers Depict 'C-Level'*

[48] http://www.whitehouse.gov/the-press-office/2014/10/17/fact-sheet-safeguarding-consumers-financial-security.
[49] https://www.americanexpress.com/icc/eurodollar/chip-and-pin.html.
[50] http://media.corporate-ir.net/media_files/IROL/63/63646/HD_Data_Update_II_9-18-14.pdf.

Security Before the Hack, Bloomberg Businessweek (Sep. 12, 2014);[51] Ben Elgin, et al., *Home Depot Hacked After Months of Security Warnings*, Bloomberg Businessweek (Sep. 18, 2014) [hereinafter *Hacked After Warnings*];[52] Julie Creswell & Nicole Perlroth, *Ex-Employees Say Home Depot Left Data Vulnerable*, N.Y. Times (Sep. 19, 2014);[53] *see also* Brian Krebs, *Banks: Credit Card Breach at Home Depot*, Krebs on Security (Sept. 2, 2014).[54]

Similarly, the recent Target breach compromised millions of consumers' personal data and credit card information because the company failed to promptly respond to a data security breach. Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, Bloomberg Businessweek (Mar. 13, 2014).[55] Criminals began stealing credit card information from Target's network on November 27, 2013. *Id*. Three days after hackers began stealing credit card information from Target's network in 2013, Target security specialists in India detected the breach. *Id*. Target personnel identified another breach the following week, but again Target's security team failed to respond. *Id*.

[51] http://www.businessweek.com/articles/2014-09-12/home-depot-didnt-encrypt-credit-card-data-former-workers-say
[52] http://www.businessweek.com/articles/2014-09-18/home-depot-hacked-wide-open#p1
[53] http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html
[54] http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/.
[55] http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

In fact, Target did not investigate the breach until federal law enforcement notified Target of suspicious card payments at its stores, two weeks later. *Id.* Because Target failed to follow well-established incident response procedures upon first discovering the cyber attack, criminals were able to steal 40 million credit card numbers and personal data of 70 million consumers. *Id*.

* * *

The cost to American consumers of inadequate data security is enormous. Billions of dollars are lost to identity theft, security breaches, and financial fraud. Once credit card information and bank details are improperly disclosed, the risks to consumers are ongoing.

The Federal Trade Commission has used its Section 5 authority as Congress intended: to address unfair and deceptive trade practices that put the safety and wellbeing of American consumers at risk.

CONCLUSION

Amici respectfully request this Court affirm the lower court's order denying Appellant's motion to dismiss.

Respectfully submitted,

/s/ Marc Rotenberg

Marc Rotenberg
Counsel of Record
Alan Butler
Julia Horwitz
John Tran
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140

CERTIFICATE OF COMPLIANCE WITH FEDERAL RULES

This brief complies with the type-volume limitation of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(a)(7)(B) because it contains 6,985 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief also complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word for Mac 2011 in 14 point Times New Roman.

Dated: November 12, 2014

/s/ Marc Rotenberg
Marc Rotenberg

CERTIFICATE OF COMPLIANCE WITH LOCAL RULES

I certify that I have complied with LAR 31.1(c) because this file was scanned by the most current version of Virus Total, https://www.virustotal.com, and no virus was detected. Also because the text of this electronically filed brief is identical to the text of the 10 paper copies mailed to the court.

Dated: November 12, 2014

/s/ Marc Rotenberg
Marc Rotenberg

CERTIFICATE OF SERVICE

I hereby certify that on November 12, 2014, I electronically filed the foregoing Brief of *Amici Curiae* Electronic Privacy Information Center and Thirty-Three Technical Experts and Legal Scholars in Support of Appellee with the Clerk of the United States Court of Appeals for the Third Circuit using the CM/ECF system. All parties are to this case will be served via the CM/ECF system.

Dated: November 12, 2014

/s/ Marc Rotenberg
Marc Rotenberg