COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE FEDERAL TRADE COMMISSION

"Public Workshop and Request for Public Comments and Participation"

May 27, 2011

By notice published on March 15, 2011, the Federal Trade Commission ("FTC") has requested public comments on the Fair Debt Collection Practices Act.[1] The Commission previously published a proposal to amend the underlying Act as well as regulatory implementation in the wake of technological advances that Congress did not contemplate when the FDCPA was first passed in 1978.[2] Pursuant to the FTC notice in the Federal Register, the Electronic Privacy Information Center ("EPIC") submits these comments and recommendations to address the substantial privacy risks posed by debt collectors' use of new technologies to gather, store, and manage consumers' personal information.

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 constitutional values. EPIC has a particular interest in protecting consumer privacy, and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers. EPIC was instrumental in the FTC's recent consent order compelling Google to develop a comprehensive

---

[1] Public Workshop and Request for Public Comments and Participation, 76 Fed. Reg. 14010 (Mar. 15, 2011) (Soliciting public comment in response to twenty-one separate questions regarding advances in technology, consumer protection, and the debt-collection industry).
[2] Workshop Report, *Collecting Consumer Debts: The Challenges of Change*, Fed. Trade Comm'n (2009) ["Workshop Report"].

privacy plan and submit to biennial, independent privacy audits.[3] EPIC now recommends a similar approach to ensuring meaningful protection of consumer privacy in the debt collection industry.

I. Background: Skip-Tracing in the Debt Collection Industry

Debt collection firms buy the right to collect payments for debts owed to banks, utility companies, wholesale retailers, automotive financing entities, hospitals, municipal water departments, and telecommunications companies who initiate credit arrangements with consumers.[4] These firms contract with companies like LexisNexis, who collect and maintain both public and private records of personal identifying information in voluminous electronic databases.[5] The databases are populated with personal information of consumers, including names, addresses, and telephones, dates of birth, prior addresses, bank and credit card account numbers, account information, and Social Security numbers ("SSNs"), which these companies furnish to subscribers for a fee.[6] The Senior Vice President and General Counsel of a large debt-buying company has stated that "[i]t would be rare for a large debt buyer to have much, if any, interest in a portfolio of debt that did not have a high proportion of Social Security numbers."[7] Information sources include credit header data from consumer reporting agencies, insurance claims data, police records, and government records such as real estate records, motor vehicle

[3] *In re Google Buzz*, Federal Trade Comm'n File No, 1023136 (EPIC Complaint) *available at* http://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf.
[4] Workshop Report at 12; Transcript of Workshop at 38, *Collecting Consumer Debts: The Challenges of Change*, Fed. Trade Comm'n (Oct. 10, 2007) ["Oct. 10, 2007 Workshop Transcript"].
[5] Transcript of Workshop at 11, *Collecting Consumer Debts: The Challenges of Change*, Federal Trade Comm'n (Oct. 11, 2007) ["Oct 11, 2007 Workshop Transcript"].
[6] *Id.* at 43, 44, 57.
[7] *Id.* at 43.

records, bankruptcy and lien records, and marriage licenses.[8] The firms request "waterfall" or "batch requests," whereby long lists of debt consumers' names are checked against electronic databases to retrieve their personal information, as well as personal information about their known associates.[9] The collectors then "skip-trace" the consumers whose debt payments they have purchased, using database information either to contact the individuals or to confirm their location by contacting family members and known associates. After substantial efforts to retrieve payment, some collectors bundle the debts they cannot collect and resell them again.[10]

II. Congress Gave The FTC Multiple Sources of Legal Authority to Prevent Consumer Abuse

A. *Fair Debt Collection Practices Act*

The FTC has multiple sets of regulatory tools to protect debt consumer privacy. By statute, Congress instructed the FTC to "eliminate abusive debt collection practices," tailoring the FDCPA to avoid harassment as debt collectors track consumers.[11] Congress specifically found "abundant evidence of the use of abusive, deceptive, and unfair debt collection practices by many debt collectors" that "contribute to the number of personal bankruptcies, to marital instability, to the loss of jobs, and to invasions of individual privacy."[12] Rather than confirming location, debt collectors were violating individuals' privacy rights and shaming them into paying off debts. To curb this conduct, the FDCPA strictly regulates communications between debt collectors and third parties such as the consumers' known associates.

---

[8] *Id.* at 21, 44; *In the Matter of Choicepoint, Inc.*, Federal Trade Comm'n File No, 0523069, (Complaint at 3) *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf.
[9] Oct. 11, 2007 Workshop Transcript at 14, 15, 21, 24, 28.
[10] Eileen Ambrose, *Zombie Debt: Debt Can Come Back To Haunt You Years Later*, BALT. SUN, May 6, 2007, *available at* http://articles.baltimoresun.com/2007-05-06/business/0705060084_1_zombie-debt-debt-buyers-consumer-debt/.
[11] 15 U.S.C. § 1692(e) (2011).
[12] 15 U.S.C. § 1692(a).

Through the FDCPA, Congress scripted the only acceptable form of communicating with "any person other than the consumer for the purpose of acquiring location information about the consumer."[13] The debt collector may identify himself or herself by name, state that he is confirming or correcting location information, and "only if expressly requested, identify his employer."[14] If debt collectors prefer to confirm location by mail, the FDCPA prohibits "any language or symbol on any envelope or in the contents of any communication effected . . . that indicates that the debt collector is in the debt collection business or that the communication relates to the collection of a debt."[15] Debt collectors are prohibited from communicating with third parties (with stated exceptions for the original creditor, attorneys, or consumer reporting agencies) about the collection of an individuals' debt in any other manner.[16]

B. Federal Trade Commission Act

Congress also empowers the FTC to adopt industry-wide trade regulation rules through Section 5(a) of the Federal Trade Commission Act,[17] which prohibits unfair or deceptive acts or practices in or affecting commerce. EPIC has been instrumental in spurring the FTC to protect consumer privacy and to enforce Section 5 against the misuse of personal information.[18] The Federal Trade Commission ("FTC") generally identifies three factors that support a finding of unfairness: whether the practice injures consumers, whether it violates established public policy,

[13] 15 U.S.C. § 1692b.
[14] 15 U.S.C. § 1692b(1).
[15] 15 U.S.C. § 1692b(5).
[16] 15 U.S.C. § 1692c(b).
[17] 15 U.S.C. § 45(a) (2011).
[18] Letter from Electronic Privacy Information Center to Christine Varney, Commissioner, Fed. Trade Comm'n (Dec. 14, 1995), *available at* http://epic.org/privacy/internet/ftc/ftc_letter.html; *In the Matter of Google, Inc. and DoubleClick, Inc*., Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (Sept. 20, 2007), *available at* http://epic.org/privacy/ftc/google/epic_complaint.pdf; Privacy? Proposed Google/DoubleClick Deal, http://epic.org/privacy/ftc/google/.

and whether it is unethical or unscrupulous.[19] A practice is "unfair" if: a) it causes substantial injury to consumers; b) the harm is not outweighed by any countervailing benefits; and c) the harm is not reasonably avoidable.[20] Deception occurs under Section 5 if there is a material representation, omission, or practice that is likely to mislead reasonable consumers.[21] The FTC Policy Statement on Deception states that the Commission analyzes deceptive business practices under the following rubric:

> a) There must be a representation, omission or practice that is likely to mislead the consumer.[22]
>
> b) The practice is examined from the perspective of a reasonable person in the circumstances.[23]
>
> c) The representation, omission or practice must be a material one, i.e. it is likely to affect the consumer's conduct or decision regarding the product or service.[24]

C. Gramm-Leach-Bliley Act

The third statute empowering the FTC to regulate debt collectors is the Gramm-Leach-Bliley Act. The Act states "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[25] It has become particularly incumbent upon the FTC to enforce this provision on behalf of consumers as a Federal Circuit Court of Appeals has held that consumers cannot sue financial institutions

---

[19] Fed. Trade Comm'n Policy Statement on Unfairness (Dec. 17, 1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.
[20] *Orkin Exterminating Company, Inc. v. FTC*, 849 F.2d 1354, 1364 (11th Cir. 1988).
[21] Fed. Trade Comm'n, Policy Statement on Deception, Oct. 14, 1983, *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm.
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] 15 U.S.C. § 6801 (2011).

directly for violations of this policy.[26] The FTC has published guidance for complying with the Gramm-Leach-Bliley Safeguards Rule that includes rudimentary measures for protecting data, including actively logging all access to consumer data on internal company networks, and erasing consumer data in accord with the Disposal Rule.[27] The agency has yet to clarify that these measures are binding and mandatory.

III. The Debt-Collection Industry Has a History of Systematically Violating the FDCPA, Section 5, and the Gramm-Leach-Bliley Safeguards Rule

In 2007, the Chair of the FTC, Deborah P. Majoras, identified industry self-regulation as one of three major prongs that bolster the agency's overarching strategy to address consumers' privacy and security concerns.[28] In sharp contrast, self regulation fails time and again to hold the weight the agency has placed upon it to fill gaps in enforcement. Debt collectors have a checkered past complying with FTC regulations. In 2004, EPIC filed a complaint with the FTC regarding the deceptive practices of data broker ChoicePoint, reporting that the company's business practices put consumers' privacy at risk.[29] ChoicePoint's security deficiencies compromised the sensitive personal data of more than 163,000 consumers.[30] In 2006, the FTC brought an enforcement action against ChoicePoint for failing to employ "reasonable and appropriate measures to secure the personal information it collect for sale to its subscribers."[31] The agency found this failure to constitute an unfair act or practice in violation of Section 5 of

---

[26] *Dunmire v. Morgan Stanley DW, Inc*., 475 F.3d 956, 960 (8th Cir.2007).
[27] FED. TRADE COMM'N, FINANCIAL INSTITUTIONS AND CUSTOMER INFORMATION: COMPLYING WITH THE SAFEGUARDS RULE (2006).
[28] Oct. 10, 2007 Workshop Transcript at 14.
[29] In the Matter of Choicepoint, Request for Investigation and for Other Relief, before the Fed. Trade Comm'n (Dec. 16, 2004), *available at* http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.
[30] See generally EPIC, EPIC Choicepoint Page, http://epic.org/privacy/choicepoint/.
[31] *In the Matter of Choicepoint, Inc.*, Federal Trade Comm'n File No. 0523069, (Complaint at 9) *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf.

the FTC Act. The ChoicePoint settlement required the company to pay $10 million in civil penalties and $5 million in consumer redress.[32] The settlement also bound ChoicePoint to a comprehensive information security program of "administrative, technical, and physical safeguards" that better protected consumer data.[33] The company was required to submit to security audits by a "qualified, objective, independent third-party professional who uses procedures and standards generally accepted in the profession" through year 2026.[34]

In 2008, the FTC settled a similar action against databrokers Reed Elsevier and Seisint for using substandard security measures that allowed unauthorized access to its databases.[35] Among the nine separate security failures the FTC catalogues in its enforcement action, the agency alleged that the company failed even to adopt "simple, low-cost, and readily available [security] defenses."[36] The databases contained particularly sensitive consumer information, including drivers' license numbers and Social Security numbers.[37] Criminals exploited the security failure and obtained sensitive information about at least 316,000 consumers: almost twice the number of individuals affected by ChoicePoint's security breach.[38] Criminals then used

---

[32] U.S. Federal Trade Commission, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress, January 26, 2006, *available at*: http://www.ftc.gov/opa/2006/01/choicepoint.shtm.
[33] *In the Matter of Choicepoint, Inc.*, Federal Trade Comm'n File No, 0523069, (Stipulated Final Judgment at 5) *available at* http://www.ftc.gov/os/caselist/choicepoint/091019choicepointstiporder.pdf.
[34] *Id.* at 4.
[35] *In the Matter of Reed Elsevier Inc. and Seisint, Inc.*, Federal Trade Comm'n File No. 0523094 (Mar. 27, 2008) (Agreement Containing Consent Order) *available at* http://www.ftc.gov/os/caselist/0523094/080327agreement.pdf.
[36] *In the Matter of Reed Elsevier Inc. and Seisint, Inc.*, Federal Trade Comm'n File No. 0523094 (Mar. 27, 2008) (Complaint at 4) *available at* http://www.ftc.gov/os/caselist/0523094/080327agreement.pdf.
[37] *Id.*
[38] *Id*.

the information to activate credit cards, open new accounts, and make fraudulent purchases.[39] The FTC found that as a result of the data breach, "several hundred thousand consumers face the possibility of future fraud."[40] EPIC filed objections to the settlements for failing to levy civil penalties similar to those in the 2006 ChoicePoint settlement.[41] EPIC urged the agency that "[t]he inclusion of civil penalties in the Consent Orders would send the clear message that serious financial consequences will result if companies fail to protect consumer data in the future."[42] It is clear that the debt collection industry has yet to process such a message.

In 2009, consumers launched three separate FDCPA lawsuits against debt collection firms for violating their online privacy. A resident of Cook County, Illinois sued JP Morgan Chase after a self described "senior investigator" posted the following message on his daughter's MySpace page: "We have been retained by JPMorgan Chase Bank, to locate and repossess their missing collateral (sic) a 2007 Mercedes GL450. Please contact our office immediately . . . Failure to contact me will result in further action against your father James Ricobene."[43] A resident of Phoenix, Arizona sued Auto Financing Network Inc. for creating a website using her name. The title of www.jenniferdicks.com stated "Jennifer Dicks isn't paying for her Cavalier!"[44] A third plaintiff, from Edwardsburg, Michigan sued two collection firms, Assets Recovered, L.L.C and Advanced Equity, Inc., for publishing information about her automotive

[39] *Id.* at 4-5.
[40] *Id* at 5.
[41] *In the Matter of Reed Elsevier, Inc. and Seisint, Inc.*, FTC Docket No. 052-3094 (FTC 2008) (Comments of the Electronic Privacy Information Center), available at http://epic.org/privacy/idtheft/042808_ftc.pdf.
[42] *Id.* at 3.
[43] *Ricobene v. JP Morgan Chase, et al.,* No. 09-CIV-02904 (N.D. Ill. Nov. 13, 2009).
[44] *Dicks v. Auto Financing Network, et al*. No. CV2009-021940 (Apr. 24, 2009) *Car Stalk*, HARPER'S MAGAZINE, July 2009, at 22.

debt on her MySpace page.[45] The plaintiff reported that the public disclosure of her private financial affairs caused "damage to her business and community reputation, extreme mental distress, aggravation, humiliation, and embarrassment."[46]

In 2010, the Department of Justice brought multiple suits against the directors of a 2,600-employee debt collection firm who transferred debtor profiles to bad actors running a full-scale fraudulent debt collection scheme.[47] Bad actors approached the directors with specific requests for profiles from individuals who recently paid off their debts.[48] Over a three year period, the directors regularly transported consumer information off company premises by copying it into spreadsheets, downloading the spreadsheets onto an Apple iPod, and then later uploading them onto an offsite computer.[49] Meanwhile, their colleagues routinely called these innocent consumers pretending to be the Sheriff's Department executing bench warrants related to fraudulent debts.[50] The scheme generated $6.8 million dollars over a three year period and defrauded over a thousand consumers.[51]

Under the Gramm-Leach-Bliley Safeguard Rule, the firm, Capital Management Services, should already have deleted records for individuals that satisfied their debts.[52] The firm should

---

[45] *Newland v. Assets Recovered,* No. 2009-099373-NZ (Mar. 19, 2010).
[46] Anita Ramasastry, *Don't Let A Debt Collector "Friend" You on Facebook: The Legal Issues Posed by Internet Debt Collection*, FindLaw, Oct. 19, 2010, http://writ.lp.findlaw.com/ramasastry/20101019.html.
[47] *US v. Pytlewski*, No. 1:10-cr-00290-WMS-1 (W.D.N.Y. Feb. 28, 2011); Press Release Department of Justice, Man Pleads Guilty to Sale of Debtor Information In Connection With Debt Collection Scheme (Oct. 25, 2010), *available at* http://www.justice.gov/usao/nyw/press/press_releases/PytlewskiPlea.pdf.
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] FED. TRADE COMM'N, FINANCIAL INSTITUTIONS AND CUSTOMER INFORMATION: COMPLYING WITH THE SAFEGUARDS RULE AT 3.

also have been logging access to these records.[53] The FTC has published guidance for complying with the Safeguards Rule that includes these rudimentary security measures for protecting data.[54] The FTC frequently expresses its preference for flexible standards that balance the need to mitigate identifiable risks with each company's ability to control costs.[55] One of the costs firms fail to control, but should take into account, is the burden on consumers who are exposed to identity theft because of inadequate security safeguards.[56] Furthermore, it is now clear that data leaks from internal sources at the highest level of authorized access are a concrete, identifiable risk that the FTC should require every firm to directly address.[57] Still, the FTC has yet to bring any significant sanction against Capital Management Service for its role in facilitating a fraudulent scheme with lax security measures.

In 2011, the FTC reported a veritable deluge of complaints about debt collectors' systematic violations of the FDCPA. Complaints over the previous year, 2010, covered every major provision of the law, reporting that debt collectors:

- disclosed purported debts to a third party (13,568)[58]
- harassed consumers at their place of work (17,008)[59]
- falsely threatened arrest or seizure of property (20,256)[60]

---

[53] *Id*. at 4.
[54] *Id*.
[55] *See, e.g., id.* at 2.
[56] FED. TRADE COMM'N, IDENTITY THEFT SURVEY REPORT 38-48 (2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf.
[57] *See US v. Pytlewski*, No. 1:10-cr-00290-WMS-1 (W.D.N.Y. Feb. 28, 2011); Press Release Department of Justice, Man Pleads Guilty to Sale of Debtor Information In Connection With Debt Collection Scheme (Oct. 25, 2010), *available at* http://www.justice.gov/usao/nyw/press/press_releases/PytlewskiPlea.pdf.
[58] FED. TRADE COMM'N, FEDERAL TRADE COMMISSION ANNUAL REPORT 2011: FAIR DEBT COLLECTION PRACTICES ACT (2011), at 9.
[59] *Id.*
[60] *Id.* at 8.

- repeatedly called consumers (54,147)[61]
- used or threatened violence if consumers failed to pay (4,182)[62]

All of these statistics represent significant increases, sometimes doubling the previous years' figures, from the same category of complaints throughout 2009.[63]

IV. The FTC Must Develop Proactive Regulations and Take Meaningful Enforcement Actions With Effective Sanctions to Deter Non-Compliant Behavior Going Forward

The FTC should clarify that existing industry practices that expose consumers to unlawful harassment and unacceptable risks of identity theft violate the statutes Congress tasked the agency to enforce. The agency is uniquely suited to correct the debt collection industry's unlawful consumer abuse. EPIC recommends that the FTC clarify that its Guidance Document for complying with the Gramm-Leach-Bliley Safeguards Rule is mandatory. EPIC also recommends the agency to clearly state that the FDCPA, as it is currently constituted, prohibits contacts between debt collectors and consumers via social networking sites, text messaging, or email. Finally, EPIC recommends finding that the industry's current use of Social Security numbers constitutes an unfair trade practice under Section 5a of the FTC Act. EPIC urges the agency to pursue meaningful enforcement actions that hold debt collectors accountable for unlawful activity.

A. Clarify that Agency Guidance Implementing the Gramm-Leach-Bliley Safeguards Rule is Mandatory

The FTC's authority under the Gramm-Leach-Bliley Safeguards Rule is an essential tool for protecting debt consumers. Alongside the agency's efforts to police debt collectors in the field through the FDCPA, the agency should expand its focus on protecting debt consumers from

[61] *Id.* at 6.
[62] *Id.*
[63] *Id.* at 6-9.

faulty information practices in back offices. Debt collection firms fail routinely to safeguard their records, as was the case in the aforementioned DOJ criminal case out of Buffalo, New York and the settlement orders the agency reached in 2006 and 2008.[64] Almost a decade ago, the agency first published its recommendations for common sense security measures that would have prevented all three of these major breaches.[65]

To date, the agency has maintained that the legal standard mandating "reasonable" security measures will be enforced according to each "financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue."[66] There are, however, rudimentary measures that every financial institution should take regardless of individual circumstances. Data breaches, accidental and purposeful, expose Social Security numbers, credit card information, names, addresses, telephone numbers, and other types of private, personally identifiable information (PII) to bad actors and public onlookers. This exposes consumers to a range of harms, most significantly identity theft. The agency should clarify that the standard security practices laid out in its 2002 guidelines implementing the Gramm-Leach-Bliley Safeguards Rule are legally binding and therefore mandatory.[67]

---

[64] *See US v. Pytlewski*, No. 1:10-cr-00290-WMS-1 (W.D.N.Y. Feb. 28, 2011); Press Release Department of Justice, Man Pleads Guilty to Sale of Debtor Information In Connection With Debt Collection Scheme (Oct. 25, 2010), *available at* http://www.justice.gov/usao/nyw/press/press_releases/PytlewskiPlea.pdf; *In the matter of Choicepoint, Inc.*, Federal Trade Comm'n File No, 0523069, (Stipulated Final Judgment at 5) *available at* http://www.ftc.gov/os/caselist/choicepoint/091019choicepointstiporder.pdf. *In the matter of Reed Elsevier Inc. and Seisint, Inc.*, Federal Trade Comm'n File No. 0523094 (Mar. 27, 2008) (Agreement Containing Consent Order) *available at* http://www.ftc.gov/os/caselist/0523094/080327agreement.pdf.

[65] *See* FED. TRADE COMM'N, FINANCIAL INSTITUTIONS AND CUSTOMER INFORMATION: COMPLYING WITH THE SAFEGUARDS RULE (2002).

[66] FED. TRADE COMM'N, FINANCIAL INSTITUTIONS AND CUSTOMER INFORMATION: COMPLYING WITH THE SAFEGUARDS RULE (2006) at 2, available at http://www.ftc.gov/opa/2002/10/safeguard.shtm.

[67] *Id.* at 3.

In light of the industry's recent history of exposing consumers to greater and greater forms of unacceptable risk, the following security measures from the agency's 2002 guidelines titled "Financial Institutions and Customer Information: Complying with the Safeguards Rule" should be mandatory across the industry:

- Checking references or doing background checks before hiring employees who will have access to customer information
- Limiting access to customer information to employees who have a business reason to see it
- Locking rooms and file cabinets where records are kept
- Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data
- Reporting suspicious attempts to obtain customer information to designated personnel
- Avoiding the storage of sensitive customer data on a computer with an Internet connection
- Ensuring that customer information is only stored on a computer with a "strong" password, kept in a physically-secure area
- Maintaining a careful inventory of the company's computers and any other equipment on which customer information may be stored
- Encrypting any sensitive data transmitted over the Internet, for instance by email
- Disposing of customer information in a secure way and in compliance with the FTC's Disposal Rule
- Designating or hiring a records retention manager to supervise the disposal of records containing customer information
- Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information
- Keeping logs of activity on internal networks with access to sensitive data and monitoring them for signs of unauthorized access to customer information[68]

B. Clarify that Contacts via Social Networking Sites, Text Messaging, or Email are all Prohibited Under the FDCPA

Debt collection firms have signaled a growing interest in social networking sites, text messaging, and email as potential venues for more immediate contact with individuals they hope

[68] *Id.* at 2-4.

to locate. Some have pursued legal means of changing the law by discussing this interest openly before the FTC.[69] Others have prompted lawsuits from consumers they've tried to reach through wall postings on social networking sites.[70] Opening additional channels of communication to an industry with a demonstrated record of consumer abuse and illegality is an invitation to further violations of the FDCPA.[71]

Section 805(b) of the Act already prohibits debt collectors from "communicat[ing], in connection with the collection of any debt, with any person other than a consumer, his attorney, a consumer reporting agency if otherwise permitted by law, the creditor, the attorney of the creditor, or the attorney of the debt collector."[72] Email, SMS messages, and social networking sites all facilitate such prohibited communication. A number of these services record and store communications by default, which renders such communications accessible to third parties who share devices or accounts with the consumer.[73] Debt collectors admit that they cannot verify a

---

[69] Oct. 10, 2007 Workshop Transcript at 108 ("I think that SMS messaging, particularly with the younger creditors, as they come up, it's going to be, you know, the preferred way to contact them, and I think as issuers and also as debt buyers, you know, we have to make sure that, you know, we come together and decide, you know, what's the best way to communicate in that manner"), 212 ("The internet, email, and cellular technology has allowed us as employers and employees, parents and children, sellers and consumers, friends and acquaintances, to conduct our interaction in a way that is efficient, useful, and timely. The FDCPA should allow creditors, consumers, and collection agencies to make full use of these technologies to the benefit of all involved."), 214 ("I think that as long as the consumer is willing to allow us to communicate with them via email . . . then we should be permitted to communicate with them in that fashion").
[70] *Ricobene v. JP Morgan Chase, et al.,* No. 09-CIV-02904 (N.D. Ill. Nov. 13, 2009); *Newland v. Assets Recovered,* No. 2009-099373-NZ (Mar. 19, 2010).
[71] *See US v. Pytlewski*, No. 1:10-cr-00290-WMS-1 (W.D.N.Y. Feb. 28, 2011); *In the matter of Choicepoint, Inc.*, Federal Trade Comm'n File No, 0523069, (Stipulated Final Judgment at 5) *available at* http://www.ftc.gov/os/caselist/choicepoint/091019choicepointstiporder.pdf. *In the matter of Reed Elsevier Inc. and Seisint, Inc.*, Federal Trade Comm'n File No. 0523094 (Mar. 27, 2008) (Agreement Containing Consent Order) *available at* http://www.ftc.gov/os/caselist/0523094/080327agreement.pdf.
[72] 15 U.S.C. § 1692c(b).
[73] Elliot Schrage, *Improving Transparency Around Privacy*, The Facebook Blog (Oct. 29, 2009, 12:24 PM) http://blog.facebook.com/blog.php?post=167389372130&fb_comment_id=fbc_

consumer's identity on text-based services before discussing an alleged debt.[74] Moreover, there is no reason to believe they would make affirmative efforts to self-regulate, given the industry's lackluster efforts to date.

Section 804 of the FDCPA prohibits debt collectors from communicating with third parties about a specific consumer's location from "us[ing] any language or symbol . . . that indicates that the debt collector is in the debt collection business or that the communication relates to the collection of a debt." To connect to consumers on Facebook, the most popular social networking site with more than 50 million active users, debt consumers must create descriptive profiles or use their employees' profiles.[75] Facebook's official policy bars the creation of fake profiles, and requires that individuals only have one profile.[76] For debt collection companies that create their own profiles, the only way to comply with this policy is to use logos, symbols, or other information that, by default, reveals the collector's profession. Commandeering employees' personal Facebook accounts for consumer contacts would also present legal issues, unless the company compelled its employees not to list or discuss any employment information on their profiles. Unlawful industry practices persuaded Facebook to email a major news publication citing internally enforced policies against "any kind of

---

167389372130_14231226_428327597130#u295942_1 ("Even after removal, copies of User Content may remain viewable in cached and archived pages"); Kevin Purdy, *How Offline Gmail Decides Which Messages to* Download, LifeHacker (Jan. 28, 2009, 4:00 AM) http://lifehacker.com/5140828/how-offline-gmail-decides-which-messages-to-download, Michelle Kimball, *Eager To Check Those Texts?*, Divorce 360 https://www.divorce360.com/divorce-articles/cheating/catching/eager-to-check-those-texts.aspx?artid=1071.

[74] Oct. 10, 2007 Workshop Transcript at 104 (General Counsel for an international debt purchasing firm: "For example, a lot of consumers would like to be contacted via email . . . . yet the FDCPA doesn't necessarily allow for that, because you may not know who's on the other end, and you don't know if that consumer has consented to that.").

[75] Facebook, *Statistics*, *available at* http://www.facebook.com/press/info.php?statistics.

[76] Facebook, *Statement of Rights and Responsibilities* (Oct. 4, 2010), *available at* http://www.facebook.com/terms.php.

threatening, intimidating, or hateful contact from one user to another," urging any users subject to FDCPA violations to contact the FTC and state Attorneys General.[77] The only practicable approach is for the agency to completely prohibit online communications with consumers.

C. Clarify that the use of SSNs as primary identifiers is an unfair trade practice

The Social Security Administration has stated that "[r]epetitive use and disclosure of SSNs in organizational record keeping systems . . . multiplies the susceptibility of persons to potential identity theft."[78] In contrast, the Vice President and Chief Council of one of the major "Risk Information and Analytics" skip-tracing practices states that his company is bound to increase "wrong party contacts" if regulators incorporate the SSA's statements as binding policy.[79] The implication is that the debt collection industry will not expend additional resources on maintaining accurate records, even in cases where the only safe, legal alternative to contacting wrong parties is to invest in better information management. Furthermore, industry is fully aware that it artificially inflates its own demand for skip-tracing because of upfront deficiencies in data retention. The President and CEO of a collection agency informed the FTC in 2007 that:

> There is a tremendous amount of incorrect information . . . that actually causes accounts to become skip accounts, if you will, inadvertent skips. The people didn't give them the wrong zip code, but somebody keyed the wrong zip code early on, and that the reason for that.[80]

The FTC should take the industry at its word and account for the fact that self-regulation, or even self-control, are both non-starters. The proper response, however, is to enforce regulations

---

[77] Alexis Madrigal, *Facebook Warns Debt Collectors About Using Its Service*, The Atlantic (Nov. 19, 2010), *available at* http://www.theatlantic.com/technology/archive/2010/11/facebook-warns-debt-collectors-about-using-its-service/66831/#.
[78] Soc. Sec. Admin., *Avoid Identity Theft: Protect Social Security Numbers*, *available at* http://www.ssa.gov/phila/ProtectingSSNs.htm.
[79] Oct. 11, 2007 Workshop Transcript at 16.
[80] *Id*. at 29.

comprehensively instead of discussing piecemeal reforms that the industry openly plans to subvert through non-cooperation.

The FTC should find that using Social Security numbers as primary identifiers in an industry that routinely loses and often fails to safeguard consumer information constitutes an "unfair trade practice." Both the agency and the courts have stated that the three criteria for "unfair trade practices" are (1) whether the practice injures consumers (2) whether it violates established public policy, and (3) whether it is unethical or unscrupulous.[81] Establishing that a practice injures consumers requires three findings: first that the injury is substantial, second, that it is not outweighed by any countervailing benefits to consumers or competition that the practice produces, and third, that consumers can not reasonably avoid the injury.

The heightened risk of identity theft that the SSA identified is a substantial harm to consumers.[82] The FTC has catalogued the costs of identity theft, from substantial quantities of lost money and time, to credit card problems, loan and insurance rejections, civil suits and criminal investigations, and even harassment by debt collectors pursuing payments on fraudulent lines of credit.[83] Industry representatives claim that using Social Security numbers reduces the number of wrong party calls, but investing in information management up front to avoid "inadvertent skips" would achieve the same end without subjecting consumers to the risk of identity theft.[84] Third, what the FTC stated in its complaint against ChoicePoint applies across the industry: "ChoicePoint collects the information without making any contact with the

---

[81] Fed. Trade Comm'n Policy Statement on Unfairness (Dec. 17, 1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm; *Orkin Exterminating Company, Inc. v. FTC*, 849 F.2d 1354, 1364 (11th Cir. 1988).
[82] Soc. Sec. Admin., *Avoid Identity Theft: Protect Social Security Numbers*, *available at* http://www.ssa.gov/phila/ProtectingSSNs.htm.
[83] FED. TRADE COMM'N, IDENTITY THEFT SURVEY REPORT 38-48 (2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf.
[84] See Oct. 11, 2007 Workshop Transcript at 29.

consumers whose information it sells, and consumers cannot remove their information from ChoicePoint's databases."[85] Consumers cannot reasonably reduce their risk of identity theft if they cannot control the industry's combined retention of sensitive data and failure to safeguard it.

As the Social Security Administration has established, the use of Social Security numbers violates public policy. The FTC has stated that public policies should be "clear and well-established" and "declared or embodied in formal sources."[86] The SSA has clearly and formally declared that "[o]rganizations should avoid using Social Security numbers (SSNs) as identifiers for any type of transaction."[87] For collection companies, the SSN is "best identifier known to man."[88] The agency has instructed organizations "never" to send SSNs via an electronic format.[89] Creditors "forward" their information to debt purchasers, who then "forward" them to other debt purchasers.[90] Electronic transmission of SSNs is the business model for skip-tracing, as third party debt collectors often ask for "the kitchen sink" and seller technology allows them to provide all consumer information they possess "at the time of sale."[91] The SSA warns that "[t]he routine and often indiscriminate use of SSNs as identifiers creates opportunities for individuals to inappropriately obtain personal information."[92] Electronic database companies pride themselves on the speed with which they can call up SSNs and a variety of other PII upon

---

[85] *In the matter of Choicepoint, Inc.*, Federal Trade Comm'n File No, 0523069, (Complaint at 3) *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf.
[86] Fed. Trade Comm'n Policy Statement on Unfairness (Dec. 17, 1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.
[87] Soc. Sec. Admin., *Avoid Identity Theft: Protect Social Security Numbers*, *available at* http://www.ssa.gov/phila/ProtectingSSNs.htm.
[88] Oct. 11, 2007 Workshop Transcript at 55.
[89] Soc. Sec. Admin., *Avoid Identity Theft: Protect Social Security Numbers*, *available at* http://www.ssa.gov/phila/ProtectingSSNs.htm.
[90] Oct. 11, 2007 Workshop Transcript at 65-67.
[91] *Id.* at 296.
[92] Soc. Sec. Admin., *Avoid Identity Theft: Protect Social Security Numbers*, *available at* http://www.ssa.gov/phila/ProtectingSSNs.htm.

individual requests.[93] Some even use SSNs as ongoing search identifiers in order to monitor bankruptcy filings electronically on behalf of debt collectors.[94] After comparing the routine uses of SSNs in the debt collection industry to the SSA's policy statement, it is impossible not to conclude that there is an ongoing violation of public policy.

The FTC has stated that the "unethical or unscrupulous" test is "largely duplicative," adding that "conduct that is truly unethical or unscrupulous will almost always injure consumers or violate public policy as well." Using SSNs poses a clear risk of substantial injury to consumers. There have been multiple security failures resulting in numerous cases of identity theft. Finally, the agency that supervises the SSN program has formally expressed a public policy against industry practice. There is sufficient basis, therefore, to justify a finding of "unethical or unscrupulous behavior." Given that all three of the FTC's criteria for an "unfair business practice" are present in this case, the agency should move forward to prevent the industry's continued use of SSNs.

D. Enforcement

The FTC's current approach to enforcement is insufficient, relying on consent decrees instead of civil penalties and suggested guidelines instead of mandatory, rigorous regulations. Adapting to changing times requires strengthening enforcement efforts as much as it does adjusting the substance of relevant regulations. It is clear that criminal networks target electronic skip-tracing databases, and their tactics have evolved from exploiting technical security flaws to paying off executives for sneaking PII out the back door. The agency should initiate investigations, make accurate findings of law and fact, bring enforcement proceedings with

[93] Oct. 11, 2007 Workshop Transcript at 15.
[94] *Id.* at 23 ("Basically they'll submit names or Socials to us. We'll alert them when there's a filing.").

serious sanctions, and generate prospective settlement orders with civil sanctions and supervised security mandates.

V. Conclusion

For the foregoing reasons, the EPIC recommends that the agency fully assess the privacy and security implications of current industry practices, clarify the import of the FDCPA's existing rules, and bring robust enforcement actions. EPIC anticipates the agency's specific and substantive responses to each of these proposals in its final report.

Marc Rotenberg
EPIC President

John Verdi
EPIC Senior Counsel

Conor Kennedy
EPIC Appellate Advocacy Fellow