COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE CONSUMER FINANCIAL PROTECTION BUREAU

Request for Comment: "Debt Collection Survey from the Consumer Credit Panel"

September 29, 2014

By notice published on March 7, 2014, the Consumer Financial Protection Bureau ("CFPB") requests public comment on "Debt Collection Survey from the Consumer Credit Panel."[1] Pursuant to CFPB's notice, the Electronic Privacy Information Center ("EPIC") submits these comments to urge the CFPB to: (1) broadly interpret the term "debt collector" under the Fair Debt Collection Practices Act ("FDCPA"); (2) limit debt collector access to consumer debt records; (3) limit the consumer information included in debt validation notices; (4) require debt collectors to adhere to consistently applied, well-vetted record-keeping standards; (5) prohibit debt collectors from contacting debtors at their workplace without express debtor consent; (6) bar debt collectors from contacting third parties without express debtor consent; and (7) prohibit debt collectors from altering or blocking telephone identification information.[2]

EPIC is a public interest research center in Washington, DC. EPIC was 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

[1] "Debt Collection Survey from the Consumer Credit Panel," 79 Fed. Reg. 13,043 (Mar. 7, 2014).
[2] EPIC is grateful for the assistance of Natasha Duarte, Cody Duncan, Eric Glatt, Krister Johnson, Aimee Thomson, and Alex Vlisides in preparing these Comments.

interest in safeguarding personal privacy and preventing harmful data practices. For example, EPIC routinely submits comments to federal agencies, urging them to uphold the Privacy Act and protect individuals from telephone and Internet misuse. In 2004, EPIC submitted comments regarding the "CAN-SPAM" Act and the proposed National "Do Not Email" Registry, recommending that a Do Not Email Registry should use domain-level listings to protect the privacy of individual email addresses.[3] In 2009, EPIC submitted comments on "Rules and Regulations Implementing the Truth in Caller ID Act of 2009," recommending a prohibition against overriding calling parties' privacy choices and ensuring that Caller ID Spoofing rules do not impede on a person's legitimate need to keep his or her telephone number private.[4] EPIC is also a leading consumer advocate before the Federal Trade Commission ("FTC"). 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.[5]

The CFPB asked EPIC to submit comments on its Paperwork Reduction Act notice, which followed from its Advanced Notice of Proposed Rulemaking to amend

[33] EPIC, *Comments on CAN-SPAM Act Rulemaking (Do Not E-Mail Registry), FTC Project No. R411008* (Mar. 31, 2004), *available at* http://epic.org/privacy/junk_mail/spam/dne.html.
[4] EPIC, *Comments on "Rules and Regulations Implementing the Truth in Caller ID Act of 2009," WC Docket No. 11-39* (2011), *available at* http://epic.org/apa/comments/EPIC-Truth-in-Caller-Cmts.pdf.
[5] *See, e.g.*, Letter from EPIC Executive Director Marc Rotenberg to FTC Commissioner Christine Varney, EPIC (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., *FTC* File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief) , http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

Regulation F of the FDCPA. Regulation F stipulates the types of practices in which debt collectors may or may not engage, particularly those implicating technology and privacy. Many of the privacy harms associated with debt collectors also plague the data broker industry. Data brokers collect vast swathes of data on millions and sometimes hundreds of millions of consumers in order to resell the data or utilize it in targeted marketing campaigns."[6] EPIC has commented extensively on the need for comprehensive privacy protections in the data broker industry to protect consumers from data breaches and harmful uses of data, such as discriminatory predictive analytics.[7]

1. CFPB Should Broadly Interpret "Debt Collector" Under the Fair Debt Collection Practices Act to Safeguard Consumers Against Privacy Harms

A. The Current FDCPA Definition of "Debt Collector" Fails to Adequately Protect Consumers from Harmful Debt Collection Practices

CFPB should interpret the definition of "debt collector" under the FDCPA to incorporate not only third party collection agencies, but also creditors that collect debt on their own behalf and any other party that engages in the collection of debt, regardless of that party's institutional definition or status.[8] The definition of "debt collector" should be a functional definition that describes the practice of collecting debt, not an institutional definition that may be underinclusive and underprotective.

---

[6] EPIC, *Big Data and the Future of Privacy*, epic.org, http://epic.org/privacy/big-data/
[7] *See Comments of the Electronic Privacy Information Center to the Office of Science and Technology Policy* (April 4, 2014), available at http://epic.org/privacy/big-data/EPIC-OSTP-Big-Data.pdf
[8] Debt Collection (Regulation F), 78 Fed. Reg. 218 at 67853 (proposed Nov. 12, 2013) (to be codified as 12 C.F.R. pt. 1006).

In the notice of proposed rulemaking, CFPB stated that the FDCPA currently only applies to third-party debt collectors, even though "first efforts to collect [] debt are often made by the creditor itself, either through in-house collectors or others collecting in the name of the creditor."[9] Thus, the consumer privacy protections in the FDCPA do not apply when debt is collected by the creditor itself (*i.e.* the original company or party with whom the debt was incurred).

Congress excluded first-party creditors from FDCPA in 1977 "because it concluded that the risk of reputational harm would be sufficient to deter creditors from engaging in harmful debt collection practices."[10] However, Congress gave the CFPB the authority under the Dodd-Frank Act in 2010 "to prescribe rules applicable to creditors."[11] The CFPB notes, "first-party collection are in fact a significant concern in their own right" and sought input "on the basic premise that [CFPB] should generally seek to harmonize any rules it develops for third-party collectors and first-part collectors."[12]

The FDCPA defines a "debt collector" as

> any person who uses any instrumentality of interstate commerce or the mails in any business the principal purpose of which is the collection of debts, or who regularly collects or attempts to collect, directly or indirectly, debts owed or due or asserted to be owed or due another
>
> or any creditor who, in the process of collecting his own debts, uses any name other than his own which would indicate that a third person is collecting or attempting to collect such debts.[13]

[9] *Id.* at 67849.
[10] *Id.* at 67853.
[11] *Id.*
[12] *Id.*
[13] 15 U.S.C. 1692a.

While this definition includes a functional component (describing what a debt collector does), it is limited to institutions or parties that collect debts *owed to another* (or at least appear to be doing so). Thus, it excludes creditors themselves, even when those creditors are performing the function of collecting debts. However, as the CFPB pointed out, a large portion of debt collection transactions are performed by first-party creditors, and "the FTC receives tens of thousands of debt collection complaints each year concerning creditors."[14] Credit card issuers, for example are not "debt collectors" under the FDCPA, even though they regularly engage in the collection of debt.[15]

B. To Protect Consumer Privacy, the FDCPA Should Regulate Creditors and Third-party Debt Collectors

i. First-party Creditors and Third-party Debt Collectors Can Cause the Same Types of Harm to Consumers

Unfair debt collection practices and misuse of consumer information, whether by creditors or debt collectors, can subject consumers to privacy breaches and economic harm. In particular, both parties collect, store, and use consumers' sensitive personal information.[16] If not properly regulated, these data collection practices can lead to breaches through unauthorized disclosure, unauthorized sale, or insecure storage of consumer information. Improper disclosure of debt-related information harms consumer

[14] 78 Fed. Reg. 218, *supra* note 1 at 67853.
[15] *See* Donald Petersen, *Credit Card Banks Are Rarely "Debt Collectors,"* fdcpa.me (July 31, 2011), http://www.fdcpa.me/credit-card-banks-seldom-debt-collectors/,
[16] *See* 78 Fed. Reg. 218, *Supra* note 1 at 67850.

privacy and can cause marital and economic instability and even physical harm, *e.g.*, from stalkers.[17]

Debt collectors and creditors collect and store large amounts of information on consumers, including the debts they owe along with their identities, addresses, account numbers, and other personally identifiable information.[18] The aggregation and use of this information may be opaque to consumers.[19] Lack of notice to consumers of the disclosure of their debts puts the burden on consumers to discover whether their information has been misused. Creditors are in a better position than consumers to keep track of this information. Thus, debt collectors and creditors alike should be subject to the FDCPA's privacy safeguards and protections against deceptive debt collection practices.

Because debt collectors and creditors aggregate troves of sensitive financial information, they are at an increased risk for data breaches and improper disclosure of data. Credit card information, flowing from creditors, is particularly vulnerable to large-scale data breaches. During the 2013 holiday shopping season, for example, roughly 40 million Target customers' credit card numbers, expiration dates, CVV security codes, and PIN numbers were exposed when Target's point-of-sale terminals were hacked.[20]

---

[17] *Id.*
[18] 78 Fed. Reg. 218, *supra* note 1 at 67854-55.
[19] 78 Fed. Reg. 218, *supra* note 1 at 67856 ("The FDCPA does not currently require any notification to consumers at the time that a consumer's debt is sold or placed with a third party for collection. Instead, consumers often become aware that their debts have been sold or placed with a third party for collection because they receive a communication to collect the debt or a written validation notice from the debt buyer or third-party collector. Consumers may have difficulty recognizing a debt or knowing whom to pay because a debt may be sold and resold multiple times or placed for collection multiple times with different third-party collectors . . .").
[20] *Comments of the Electronic Privacy Information Center* at 3, http://epic.org/privacy/big-data/EPIC-OSTP-Big-Data.pdf ; Target: data breach FAQ, https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ; Target: data breach FAQ, https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ.

Improper disclosure of information by creditors themselves, such as to spouses or stalkers, can lead to domestic instability and physical harm. Creditors should therefore be subject to FDCPA control over how the information they hold is disseminated to third parties

ii. The FDCPA Should Employ a Functional Definition of "Debt Collector" that Incorporates Creditors

As described above, creditors pose many of the same privacy risks to consumers that third-party collectors pose. Therefore, the consumer protections included in the FDCPA should apply to all parties who engage in the practice of collecting debt, whether on behalf of themselves or others. Whether a party is collecting its own debt or the debt of another is irrelevant when it comes to practices that could threaten consumer privacy,. The threats of improper disclosure and deceptive practices apply to all parties collecting debt.

California's Rosenthal Fair Debt Collection Practices Act (Calif. Civil Code § 1788.2) provides a good model of a functional definition for debt collectors.[21] The Act defines "debt collector" as "any person who, in the ordinary course of business, regularly, on behalf of himself or herself or others, engages in debt collection."[22] An inclusive, functional definition would avoid arbitrarily exposing consumers to deceptive practices based on the institutional status of a collector.

2. The CFPB Can Protect Consumer Privacy by Limiting Access to Consumer Debt Records (Questions 11 and 12)

[21] Calif. Civil Code § 1788.2
[22] *Id.*

A. Debt Owners Reveal Sensitive Consumer Data to Debt Buyers (Question 11)

When a consumer's debt is bought or shared with other parties, the consumer's personally identifying information (PII) and other sensitive personal information accompanies the transfer. This sensitive consumer data located in debt documentation includes the "consumers' names, addresses, phone numbers, and social security numbers; original account numbers; original balances; charge-off balances; charge-off dates; interest rates; the identity of original creditors; date the account was opened; and last payment date."[23] This data is unreliable and is often unverified by the data buyer.[24] Not only does this sensitive information pass between the hands of buyers and sellers, debt sellers often share some or all of this information with *prospective* buyers as a part of the "bid file," a collection documents and information provided to help potential purchasers make bidding decisions.[25] Prospective buyers include both well-established industry purchasers and persons located via telephone calls, mailing lists, clearinghouses, web advertisements, and email alerts.[26] Even when some data in the bid files are redacted,

[23] FED. TRADE COMM., THE STRUCTURE AND PRACTICES OF THE DEBT BUYING INDUSTRY 20–21 (2013) [hereinafter FTC Debt Buying Report], *available at* http://www.ftc.gov/sites/default/files/documents/reports/structure-and-practices-debt-buying-industry/debtbuyingreport.pdf; *see id.* at T-9–T-10 ("Table 8: Data File Information Obtained at Time of Sale."); *id.* at 37 ("The Commission's analysis also reveals that the information that debt buyers conveyed to other debt buyers when debt was resold was very similar to the information that original creditors provided to debt buyers."). As detailed in the FTC report: "[O]ver 98% of debt accounts included the name, street address, and social security number of the debtor . . . 70% set forth the debtor's home telephone number, and 47% and 15% listed work and mobile telephone numbers, respectively." *Id.* at 34.
[24] *Id.* at 29–30.
[25] *Id.* at 20.
[26] *Id.*

there does not appear to be any consistency in or regulation of what data must be redacted when showing portfolios to prospective buyers.[27]

If debt is resold to secondary buyers (and beyond), "the original creditors typically [have] no obligation to provide documents directly to the secondary buyers; instead the secondary buyers [are] required to forward document requests through the original buyers."[28] As a result, the consumer's sensitive PII will traverse a network of secondary parties, all but one of whom do not have any financial or other relationship with the consumer. Furthermore, "[m]any debts are purchased and resold several times over the course of years before either the debtor pays the debt or the debt's owner determines that the debt can be neither collected nor sold."[29] Each selling junction creates another opportunity for inaccurate information to enter data files.

The widespread diffusion of PII between debt owners, debt buyers, debt sellers, and third-party collectors creates the real risk that PII will be intercepted and used for abusive purposes.[30] The Department of Justice reported last December that "[a]pproximately 16.6 million persons or 7% of all U.S. residents age 16 or older were victims of one or more incidents of identity theft on 2012."[31] Transferring sensitive documents between actual and prospective collectors without redacting or minimizing PII increases the likelihood that the PII will be used or accessed for an unlawful purpose.

---

[27] *Id.* at 21.
[28] *Id.* at iii–iv.
[29] *Id.* at 1.
[30] *See* OFFICE OF SCIENCE AND TECHNOLOGY POLICY, COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER REGARDING REQUEST FOR INFORMATION: BIG DATA AND THE FUTURE OF PRIVACY (2014), *available at* https://epic.org/privacy/big-data/EPIC-OSTP-Big-Data.pdf (outlining risks posed to Americas by the collection of personal information).
[31] ERIKA HARRELL & LYNN LANGTON, BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, VICTIMS OF IDENTITY THEFT, 2012, at 1 (2013), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf.

B. A Centralized Repository for Consumer Debt Information Poses Substantial Consumer Privacy Risks (Question 12)

The establishment of a centralized repository of consumer-related documentation and information poses the same privacy risks as identified in Question11, in addition to several others unique to centralized databases. Critically, such a database would void consumer choice by denying the consumer control over the addition or deletion of records. Although the sensitive personal data belongs to the consumer, the data is collected, packaged, and accessed by second and third parties who may or may not have a financial relationship with the consumer. If such a repository were owned and operated privately, operators would face incentives to expand their market share contrary to consumer privacy interests.

Databases pose unique threats to privacy due to the centralization of information and uniformity of data files. Debt sellers already share sensitive PII with *prospective* buyers, a serious privacy concern in and of itself.[32] To the extent that anyone can be a prospective buyer, creating a repository would give *anyone* access to a consumer's name, address, telephone numbers, social security number, and debt history.[33] Not only would this expose sensitive information to debt collectors and financial institutions not in a direct financial relationship with the consumer, but a privately owned repository could allow access to other groups of persons—such as employers and landlords—who should not be given access to the debt histories of their employees and tenants. Moreover, given the rate at which inaccurate and unverified information currently flows between debt

[32] FTC Debt Buying Report, *supra* note 23, at 20.
[33] *See supra* note 23.

owners and debt collectors,[34] misuse of mistaken repository data could have real pecuniary harms on innocent parties. Finally, a centralized database of PII—including Social Security numbers—would be a prime target for hackers, who would be able to perpetuate identity theft or use debt status to cause real-life harms.[35] For these reasons, EPIC opposes the establishment of a centralized repository of debt-related documentation and information.

If the CFPB nevertheless decides to construct a centralized repository, it must comply with the Fair Information Practices (FIPs),[36] which are built into the Privacy Act of 1974.[37] Such a CFPB-maintained repository must likewise be compliant with the Privacy Act, which includes specific privacy protections, like access and amendment rights.[38] In addition, CFBP must verify all actual or prospective debt collectors, authorize their access to the repository, and revoke the authorization of anyone who uses repository data for an unauthorized purpose.[39] The repository should prohibit anyone besides the

[34] FTC Debt Buying Report, *supra* note 23, at 29–30.
[35] Although consumers in default are generally less financially attractive for hackers, a centralized database of sensitive PII would outweigh the associated absence of good credit.
[36] *See* NAT. STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, NAT. INSTITUTE OF STANDARDS AND TECH. APPENDIX A – PAIR INFORMATION PRACTICE PRINCIPLES (FIPPS) 1 & n.1 [hereinafter FIPS], *available at* http://www.nist.gov/nstic/NSTIC-FIPPs.pdf ("Rooted in the United States Department of Health, Education and Welfare's seminal 1973 report, 'Records, Computers and the Rights of Citizens' (1973), these principles are at the core of the Privacy Act of 1974 and are mirrored in the laws of many U.S. states, as well as in those of many foreign nations and international organizations.").
[37] The Privacy Act of 1974, Pub. L. No 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a).
[38] *See* 5 U.S.C. § 552a(d) (2012).
[39] *See* FED. MOTOR CARRIER SAFETY ADMIN., DEP'T OF TRANSP., COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER REGARDING COMMERCIAL DRIVER'S LICENSE DRUG AND ALCOHOL CLEARINGHOUSE 9–10 (2014) [hereinafter EPIC Clearinghouse Comments], *available at* https://epic.org/privacy/workplace/EPIC-FMCSA-Clearinghouse.pdf (recommending that the Federal Motor Carrier Safety Administration mandate that the agency revoke access of anyone who abuses the centralized Commercial Driver's License Drug and Alcohol Clearinghouse database).

debt collector in a financial relationship with the consumer from accessing his or her debt records.

Of especial importance is the consumer's right to accuracy. Similar to privacy standards established by the Fair Credit Reporting Act for information provided by debt collectors to consumer reporting agencies, debt collectors authorized to add information to the repository must be bound by rules of accuracy and error-correction. Specifically, debt collectors must have a clear obligation to not provide any information about a consumer to the repository if the collector "knows or has reasonable cause to believe that the information is inaccurate."[40] In addition, if the debt collector makes an inadvertent error or learns that information it added to the repository is inaccurate (either through the ordinary course of business or from consumer notification), the collector must "make a correction immediately upon discovering the error, and notify all individuals having access to the erroneous information that the information is inaccurate."[41]

Were the CFPB to permit the establishment of a centralized repository of consumer information by a private company (not serving as a government contractor), the database must be subject to clear legal rules, setting out the obligations of the organizations in possession of the information and the individuals about whom the information pertains. Specifically, the CFPB must require the repository and all users (1) to establish and comply with privacy and data security practices and (2) to register with and undergo regular auditing by the CFPB. In addition, the CFPB should maintain

[40] 15 U.S.C. § 1681s-2(a)(1)(A) (2012).
[41] EPIC Clearinghouse Comments, *supra* note 39, at 9 (internal citation omitted); *see* 15 U.S.C. § 1681s-2(a)(2) (2012).

control over the registration of authorized users and revoke authorization if a collector accesses or uses repository data for an unauthorized purpose.

In addition to the practices outlined in the FIPs, the CFPB must further require compliance with the Consumer Privacy Bill of Rights (CPBR), the clearest articulation of the FIPs in the American legal context.[42] Under FIPs and CPBR, any private repository must, at minimum, adhere to the following practices:

- **Transparency**: The repository must "notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII)."[43] As a result, the repository must notify each consumer when his or her PII is added to the repository and detail how it will be used, disseminated, and maintained. Notifications to consumers must themselves ensure that consumer PII is property protected.
- **Control**: The repository must give consumers "a right to exercise control over what personal data companies collect from them and how they use it"[44] and must "provide mechanisms for appropriate access, correction, and redress regarding use of PII."[45]
- **Purpose Specification**: The repository must "specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used. . . . Organizations should use PII solely for the purpose(s) specified in the notice."[46] Any centralized repository must clearly establish (in coordination with CFPB) the authorized uses of consumer data. CFPB should bring enforcement procedures against anyone who makes unauthorized use of PII in the repository, and establish a route of civil remedy for consumers who discover that their data has been used for an unauthorized purpose.
- **Accuracy**: The repository must "ensure that PII is accurate, relevant, timely, and complete."[47] Given the FTC's findings about inaccurate and unverified data,

[42] *See* WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 1 (2012) [hereinafter CPBR], *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.
[43] FIPs, *supra* note 36; *see id.* at 47.
[44] CPBR, *supra* note 42, at 47.
[45] FIPs, *supra* note 36.
[46] *Id.*
[47] *Id.*; *see* CPBR, *supra* note 42, at 48.

CFPB should require all users of the repository to verify the accuracy of any data prior to its addition in the repository.

- **Focused Collection and Minimization**: The repository must "only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s)."[48] CFPB should ensure that any repository deletes all data records once the consumer pays the debt or the debt owner considers the debt unredeemable.
- **Security**: The repository must "protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure."[49]
- **Auditing**: The repository must submit to regular CFPB auditing to ensure accuracy in data, purpose compliance, and adequate training.[50]

Any centralized private repository—and its associated privacy and data security policies—must be registered with and approved by the CFBP. As with a repository maintained by CFPB, all actual or debt collectors should obtain CFBP authorization to gain access to the private repository, the repository should strictly deny access to anyone without authorization, and CFPB should revoke the authorization of anyone who uses repository data for an unauthorized purpose.[51] Likewise, any private repository should prohibit anyone besides the debt collector in a financial relationship with the consumer from accessing his or her debt records.

3. To Protect Consumer Privacy, the CFPB Should Limit Consumer Information Included in Debt Validation Notices (Question 18)

Three primary privacy concerns arise with validation notices: re-identification, identity theft, and the exposure of private facts. Re-identification occurs when

[48] FIPs, *supra* note 36; *see* CPBR, *supra* note 42, at 48.
[49] FIPs, *supra* note 36; *see* CPBR, *supra* note 42, at 48.
[50] *See* FIPs, *supra* note 36; CPBR, *supra* note 42, at 48.
[51] *See* EPIC Clearinghouse Comments, *supra* note 39, at 9–10 (recommending that the Fed. Motor Carrier Safety Admin. mandate that the agency revoke access of anyone who abuses the Clearinghouse).

anonymized or partially anonymized data is matched with an identifiable individual.[52] This may occur with unique personal identifiers, such as Social Security numbers, but also occurs with the combination of two or three quasi-identifiers, such as birthdates or zip codes.[53] Identity theft is the appropriation of another's identity for fraudulent purposes.[54] Exposure of the existence of debt can embarrass an individual, even when the information is not used for nefarious purposes.[55]

Re-identification can occur with seemingly innocuous quasi-identifiers. A zip code, birth date, and sex allows re-identification of 87% of the population.[56] Professor Latanya Sweeney, for example, has used this method to uniquely re-identify half of the participants in a large anonymous DNA study.[57] Furthermore, the combination of an individual's home zip code and work zip code can narrow an attempt at re-identification from the entire U.S. population down to 21 people, on average.[58] Health care data is especially vulnerable to re-identification, as an individual can be re-identified using the patient's combination of ailments.[59]

The same information that can be pieced together to re-identify an individual can also be used to steal someone's identity. For example, Social Security numbers can be

---

[52] *Re-identification*, EPIC.ORG, http://epic.org/privacy/reidentification/.
[53] *Id.*
[54] *Identity Theft*, EPIC.ORG, http://epic.org/privacy/idtheft/ (last visited Jul. 22, 2014).
[55] *Poll Respondents More Embarrassed to Admit Credit Card Balance and Credit Score than Age or Weight*, NFCC.ORG, http://www.nfcc.org/NewsRoom/newsreleases/FLOI_March14_Release_FINAL.cfm.
[56] Latanya Sweeney, *Simple Demographics Often Identify People Uniquely*, CARNEGIE MELLON UNIVERSITY LABORATORY FOR INTERNATIONAL DATA PRIVACY, 2000, at 16.
[57] Adam Tanner, Harvard Professor Re-Identifies Anonymous Volunteers In DNA Study, FORBES (Apr. 25, 2013).
[58] Philippe Golle and Kurt Partridge, *On the Anonymity of Home/Work Location Pairs*, PERVASIVE '09 PROCEEDINGS OF THE 7TH INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING, 2009, at 395.
[59] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1702 (2010).

guessed with a 44% success rate by knowing an individual's birthdate and zip code.[60] A Social Security number facilitates the creation of fraudulent credit cards, fake birth certificates, and illegitimate government benefits to third parties.[61] Every year, 16.6 million people, or 7% of the U.S. population, suffers from identity theft.[62] About 36% of identity theft victims suffer moderate to severe emotional distress as a result of the theft.[63] Two thirds of identity theft victims do not know how the thief obtained their personally identifying information.[64]

Even if third parties do not use personal information for nefarious ends, discovering the identity of a debtor can still embarrass that individual. People are more embarrassed to admit credit card debt or their credit score than to admit their weight or their age.[65] And credit card debt can run high – according to the Federal Reserve, average credit card debt in America is $7,100.[66] Validation notices should not include personal identifiers that others can readily link to the debtor (like birthdate, zip code, Social Security number, or medical conditions). Instead, validation notices should contain information specific to the debt, rather than the debtor (like type of debt, original creditor, date of last payment, or a copy of the last periodic statement). Minimizing

[60] Alessandro Acquisti and Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106(27) PROCEEDINGS OF THE NATIONAL ACADEMY OF SCIENCE 10977 (2009).
[61] Kristin Finklea, *Identity Theft: Trends and Issues*, CONGRESSIONAL RESEARCH SERVICE, 2014, at 19.
[62] Erika Harrell, *Victims of Identity Theft: 2012*, BUREAU OF JUSTICE STATISTICS, 2013, at 1.
[63] *Id.*
[64] *Id*.
[65] *Poll Respondents More Embarrassed to Admit Credit Card Balance and Credit Score than Age or Weight*, NFCC.ORG, http://www.nfcc.org/NewsRoom/newsreleases/FLOI_March14_Release_FINAL.cfm.
[66] Jesse Bricker, *Changes in U.S. Family Finances from 2007 to 2010: Evidence from the Survey of Consumer Finances*, 180 FEDERAL RESERVE BULLETIN 1, 67 (2010).

personally identifiable information in validation notices is necessary to prevent re-identification, identity theft, and the exposure of private facts.

4. Debt Collectors Should Be Required to Adhere to Consistent, Well-Vetted Record-Keeping Standards

The FDCPA makes no mention of records, recordkeeping, or any standard to which records must comply. The only mention the FDCPA makes to something record-like is to forms of communication between collectors and debtors, such as letters. It appears silent to the question of record quality.[67]

The lack of consistently applied, well-vetted record-keeping standards unnecessarily complicates the debt disputation process, both by leading to the sale of incomplete records that often fail to include whether or not the debt has been disputed, and by undermining the efficacy of the legal remedy intended by Congress for consumers to dispute claims. Buying and selling erroneous information about consumers' debt implicates their privacy interests by interfering with their "right to be left alone" from debt collectors and by increasing the unnecessary sharing of often incorrect information about them among outside parties.

Debt purchasers often receive incomplete information about consumers who have disputed claims, which can produce the undesirable outcome of burdening a debtor with repeatedly disputing a debt claimed by a debt buyer, intruding on one's right to be left in peace.[68] The Bureau's powers include the ability to require debt issuers, sellers, and

[67] 15 U.S.C.A. § 1692 (c) (2012).
[68] *The Structure and Practices of the Debt Buying Industry*, FEDERAL TRADE COMMISSION, ii–iii (Jan. 2013), *available at* http://www.ftc.gov/sites/default/files/documents/reports/structure-and-practices-debt-

purchasers, and the debt collectors with which they may contract, to maintain certain records such that the Bureau can effectively assess consumer risks,[69] and the ability to standardize the formats in which data about consumers is kept.[70] These powers could be used to protect consumers with debt disputes by improving the accuracy of information stored about them. EPIC urges the Bureau to specify in its rulemaking that clear, standardized information about debt disputes be maintained and included in all debt records sold to others.

Consumers should also have rights in their debt information to include access, transparency, respect for context, security, and accountability.[71] Consumers should be given "easily understandable" information about creditor and debt collector's security and privacy practices.[72] Such transparency should extend to providing consumers with easily understandable information about how to dispute records they believe to be in error. This is important, as the FTC has found that data on reported disputes "likely . . . understate the problem" because consumers may not receive or understand the validation notices—explaining the means by which a dispute should be asserted—collectors are

---

buying-industry/debtbuyingreport.pdf (finding that "debt sellers typically do not provide dispute history information to buyers at the time of sale").

[69] 12 U.S. Code § 5514 (b)(7)(B) ("The Bureau may require a person described in subsection (a)(1), to generate, provide, or retain records for the purposes of facilitating supervision of such persons and assessing and detecting risks to consumers.").

[70] 12 U.S. Code § 5533 (d) ("The Bureau, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under this section.").

[71] *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, THE WHITE House, 19–20 (Feb. 2012) (recommending "appropriate means and opportunity to correct inaccurate data").

[72] *Id.* at 14.

required to send when seeking to collect an outstanding debt.[73] Additionally, only appropriate information about debts in dispute should be recorded and kept. Incomplete records can lead to more harm to consumers in a position to dispute a claim than more complete records would. In the context of preserving consumers' ability to identify, contest, and litigate disputes about debt records, having access to detailed and accurate information can be critical. Thus, safeguards are recommended to ensure the "secure and responsible handling of personal data."[74] In elaborating on accountability, the White House noted that "[p]rivacy protection depends on companies being accountable to consumers as well as to agencies that enforce data privacy protections."[75] It also noted that "accountability must attach to data transferred from one company to another,"[76] which has important implications when considering rules affecting information about people that is bought and sold. The rules the Bureau promulgates should accordingly afford both consumers and the Bureau with meaningful recourse by which to enforce compliance.

5. Debt Collectors Should be Prohibited from Contacting Debtors at Their Workplace Without Express Debtor Consent (Questions 70 and 72)

The CFPB has recognized that debt collection calls to a workplace pose serious issues for employees.[77] Many agree that "[c]ollection calls to a consumer's workplace or

[73] *Supra* note 3, at 38.
[74] *Supra* note 71 at 19.
[75] *Id.* at 22.
[76] *Id*.
[77] FAIR DEBT COLLECTION PRACTICES ACT CFBP ANNUAL REPORT 2014, CONSUMER FINANCE PROTECTION BUREAU 22 (2014), *available at* http://files.consumerfinance.gov/f/201403_cfpb_fair-debt-collection-practices-act.pdf .

job are among the most intrusive violations of a consumer's right to privacy."[78] Consumers and collectors would benefit from a simple, bright line rule to deal with privacy and other concerns: No collection calls to a consumer's workplace without explicit consent.

The law currently allows a debtor to essentially opt-out of calls to their workplace by informing a collector that the employer prohibits such calls.[79] But while both CFPB[80] and consumer groups[81] have tried to educate debtors to inform debt collectors they cannot receive workplace calls, if the first contact occurs at a workplace, the debtor would have no prior notice or opportunity to opt out. One call is all it may take to cause the embarrassment and reputational damage Congress sought to avoid by regulating workplace collection calls.[82]

Indeed, creditors may depend on workplace collection calls not for actual communication, but to strike fear into debtors about their privacy or their job. Attorney H. Anthony Hervol, a debt collection specialist, says that collectors "know if they try to collect at your place of employment, that you're going to worry about your job and

---

[78] Donald Peterson, *Not While I'm Working!*, FAIR DEBT COLLECTION PRACTICES ACT BLOG (Nov. 13, 2010), http://www.fdcpa.me/not-while-im-working/.
[79] *See* 15 U.S.C.A. § 1692c(a)(3) (2012).
[80] *Can Debt Collectors Call My Employer and Tell Them They Are Calling About My Debts?*, CONSUMER FINANCE PROTECTION BUREAU (Apr. 8, 2014), http://www.consumerfinance.gov/askcfpb/337/can-debt-collectors-call-my-employer-and-tell-them-they-are-calling-about-my-debts.html.
[81] *Fact Sheet 27: Debt Collection Practices: When Hardball Tactics Go Too Far*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/debt-collection-practices-when-hardball-tactics-go-too-far (last visited July 18, 2014).
[82] H.R. REP. NO. 95-131, at 6 (1977) ("Contacting consumer's employer prior to final judgment can cause irreparable harm to the consumer's job or reputation").

somehow that's going to help them collect the debt."[83] Workplace calls can cost an employee their job,[84] and collectors take advantage of this fear.

Even if an employee is authorized to receive calls, receiving a great number of personal phone calls can create a red flag for the employer.[85] While a collector is prohibited from discussing an employee's debt with a boss, contacting the debtor at work can nonetheless reveal this private issue.[86] Even for employees authorized to receive calls, a "boss will likely take notice if [an employee starts] receiving a much higher-than-normal volume of personal calls at work and look into the matter."[87] At the least, an employer will generally ask the employee about the use,[88] meaning that to be truthful, an employee must explain their very private debt issues. Some collectors intentionally use workplace calls to produce this fear that co-workers will find out about an individual's debt, stating, "The great thing about calling someone at work is that it's hard for them to dodge the call without divulging to their co-workers or boss that they're in debt and someone is trying to collect from them." [89] This fear exists even for employees authorized to receive such calls.

---

[83] Patrick Danner, *Court Case Not the Way Whataburger Likes It*, HOUSTON CHRONICLE (Aug. 23, 2012), http://www.chron.com/default/article/Court-case-not-the-way-Whataburger-likes-it-3811325.php.
[84] Marjie Lundstrom & Sam Stanton, *Debtors Seeth, Sue Over Collector Tactics*, SACRAMENTO BEE (Apr. 22, 2012), http://www.sacbee.com/2012/04/22/4432940/debtors-seethe-sue-over-collector.html.
[85] *See* Patty Inglish, *Top 10 Reasons Employees Get Fired, Among Surveyed Companies in the 21st Century*, PATTY INGLISH, MS BLOG (June 24, 2014), http://pattyinglishms.hubpages.com/hub/Fired.
[86] *Can Debt Collectors Call Your Boss?,* COLLECTION AGENCY DEBT BLOG (June 5, 2014), http://collectionagencydebt.blogspot.com/2014/06/can-debt-collectors-call-your-boss.html.
[87] *Id.*
[88] *Excessive Telephone Usage*, WINMARK BUSINESS SOLUTIONS, http://www.wbsonline.com/resources/excessive-telephone-usage/ (last visited July 18, 2014).
[89] Paul Lawrence*, 6 Secrets to Getting Debtors to Pay Up*, EARLY TO RISE, http://www.earlytorise.com/6-secrets-to-getting-debtors-to-pay-up/# (last visited July 18, 2014)

Simply put, workplace collection calls to any worker, regardless of their workplace, threaten privacy. The calls can put an employee in a position of having to explain their issues to an employer, which defeats Congress's intent in prohibiting collectors from informing employers directly.[90]

Prohibiting calls to an employer, absent express debtor consent, would have huge benefits to consumers with minimal costs to collectors. Collectors must navigate a variable legal framework that allows for workplace calls, unless they know the debtor cannot receive such calls or have reason to know the employer does not allow it, unless the debtor consents.[91] This standard leads to the common situation in which collectors make illegal calls, whether knowingly or unknowingly, and expose themselves to lawsuits by debtors.[92] Corporations have even filed suit against debt collectors for persistent disruptive practices in contacting their employees.[93] An across-the-board ban on workplace collection calls without express debtor consent would create a bright line rule that all parties can depend on.

6. Debt Collectors Should be Barred from Contacting Third Parties Without Express Debtor Consent (Questions 78 and 81)

A. Collectors Should be Prohibited from Contacting a Debtor's Spouse When Collectors Become Aware That the Debtor is Estranged from Her Spouse (Question 78)

Collectors should not be permitted to contact a consumer's spouse where a collector becomes aware that the consumer is estranged from her spouse, or upon the

[90] H.R. REP. NO. 95-131, at 6 (1977) (explaining that such contact "constitutes an unwarranted invasion of the consumer's privacy and interference with the consumers employee-employer relationship").
[91] 15 U.S.C.A. § 1692c(a)(3) (2012).
[92] Lundstrom & Stanton, *supra* note 84.
[93] Danner, *supra* note 83.

consumer's request, because allowing that contact would provide an avenue for abuse, and serves no legitimate purpose.

Because debt is a sensitive issue, consumers risk hostility and even violence from family members.[94] Recent scholarship has analyzed the link between domestic violence and consumer credit.[95] In fact, financial abuse plays a role in in most cases of domestic violence.[96] "Even without the direct application of force, the underlying climate of intimidation in a violent relationship creates a context in which the victim has a decreased ability to prevent transactions to which she does not consent."[97] The troubles for a victim of abuse do not end at separation as, "[e]ven if a divorce court decides that an abusive spouse is responsible for paying a debt he has fraudulently or coercively incurred in the survivor's name, creditors still consider the survivor liable, so a division of debt favoring her will be only a paper victory."[98] While a victim of domestic violence might not legally or practically escape the debts incurred while she was in a violent relationship, debt collectors should be prohibited from exploiting that violence for the purposes of debt collection.

More than 90% of people own cellular phones,[99] and thus, the value of continuing to contact a particular residence is significantly diminished. When a consumer has

---

[94] Brenda Craig, *Tales from the Dark Side of Debt Collection,* Lawyers and Settlements (Nov. 30, 2013), http://www.lawyersandsettlements.com/articles/Bill-Collector-Harassment/interview-debt-collector-lawsuit-bill-2-19312.html.
[95] *See* Angela Littwin, *Coerced Debt: The Role of Consumer Credit in Domestic Violence*, 100 Cal. L. Rev. 951 (2012), *available at* http://scholarship.law.berkeley.edu/californialawreview/vol100/iss4/6/.
[96] *See id.* at 972.
[97] *Id.* at 978.
[98] *Id.* at 957.
[99] *Riley v. California*, 573 U.S. ____, slip op. at 19 (2014), *available at* http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

informed a collector that she has no continuing relationship with someone the collector has contacted, further contact serves no legitimate purpose, and only serves to harass third-parties and to exert pressure on the consumer through people with whom the consumer has purposefully chosen to have no contact.

B. The Theory of Implied Consent for Debt Collector Communications Violates the Fair Debt Collection Practices Act (Question 81)

It is inconsistent with the FDCPA for a debt collector to have any communication with a third-party based on a theory of implied consent. Furthermore, it is doubtful that the circumstances surrounding the example given, or debt collection practices more generally, could support a finding of implied consent as it is understood in the common law. Finally, because getting consent, even implied consent, requires communications between the consumer and the debt collector, the best policy is to require that debt collectors receive express consent before communicating with third parties regarding the consumer's affairs.

It is not uncommon for a parent to try to assist with his child's debts. Increasingly, rather than sending cash or a check as a gift to a child, parents are sending money directly to their children's creditors.[100] While this may be well-meant act by a parent, the FDCPA anticipates and prohibits communications between parents of non-

[100] Caren Chesler, *How Parents Solve Their Kid's Debt Crisis*, THE FISCAL TIMES (Dec. 21, 2011), http://www.thefiscaltimes.com/Articles/2011/12/21/How-Parents-Solve-Their-Kids-Big-Debt-Crisis#sthash.yyuqMglK.dpuf.

minor children and debt holders,[101] and more generally, strictly restricts communications between third parties and debt collectors.[102]

A debt collector is prohibited under FDCPA section 805(b) from communicating with a third-party in connection with the collection of a debt "without the prior consent of the consumer given directly to the debt collector."[103] Because the statute requires that prior consent be given *by the consumer* "directly to the debt collector," prior to the communication, it seems to anticipate express consent as the sole basis for communications between debt collectors and third parties. At the very least, consent must arise from conduct by the consumer directed at the debt collector, and thus it is impermissible for a debt collector to rely on the actions of a third party to who injects himself into the consumer's affairs.

As a secondary matter, it is doubtful that facts in the given example, or circumstances in contemporary debt collection generally, would support a finding of implied consent as understood by the common law. The Restatement (Second) of Torts states that "[i]mplied consent is consent which exists in fact, but is manifested by conduct rather than by words."[104] As defined by Black's Law Dictionary, this requires "[a]n inference arising from a course of conduct or relationship between the parties, in which there is mutual acquiescence or a lack of objection under circumstances signifying assent."[105] Thus, implied consent would require a consumer to engage in some conduct

[101] 15 U.S.C. § 1692c(d) (2012).
[102] *See* 15 U.S.C. § 1692c(b).
[103] 15 U.S.C. § 1692c(b) (2012).
[104] RESTAT. 2D OF TORTS, § 496C.
[105] BLACK'S LAW DICTIONARY 305 (6th ed. 1990).

manifesting consent to the debt collector. However, in the example described, a third-party has contacted the debt collector, and there is no interaction between the consumer and the debt collector from which to find any conduct at all, much less conduct manifesting consent. Because most communications between debt collectors and third-parties will take place via telephone or written communications, and not through a medium which allows the consumer himself to interact with the debt collector, this problem likely persists in all cases of third parties reaching out to debt collectors.

Finally, because even implied consent would require some contact between the consumer and the debt collector, the additional cost of seeking express consent is extremely low, and the benefits (specifically the mitigation of risks of identity theft and other crimes involving unauthorized access to personal information) are so great that a cost-benefit analysis weighs strongly in favor of requiring express consent before communicating with a third-party with regard to a consumer's affairs.

7. Debt Collectors Should be Prohibited from Altering Telephone Identification Information or Blocking Identification Information (Question 86)

Debt collectors should be prohibited from altering telephone identification information (spoofing) or blocking identification information (blocking) both because these activities implicate federal privacy laws and because they cause harm to consumers. First, a debt collector spoofing caller ID is illegal. Under the FDCPA, collectors are barred from "[t]he use of any false representation or deceptive means to collect or attempt to collect any debt or to obtain information concerning a consumer."[106] This includes intentional deception over a caller ID. In *Knoll v. IntelliRisk Mgmt. Corp.,* a federal

[106] 15 U.S.C. § 1692e(10) (2012).

district court ruled that a debt collector who spoofed caller ID information to read "Jennifer Smith," despite having no employee by that name, had violated the FDCPA.[107] The court found that the altered information "masked that a debt collector was calling," in violation of § 1692e as a false or deceptive misrepresentation.[108]

Second, the Telephone Consumer Protection Act makes it illegal for any person "to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value."[109] In some circumstances, collection calls may be meant to "wrongfully obtain" payment, such as when a debt collector implies or threatens legal action on a debt time-barred by a statute of limitations.[110]

Caller ID spoofing and blocking create clear harms to consumers. Debt collectors use caller ID spoofing to intimidate consumers. "Some debt collectors are using false caller ID info to show that the collection agency is a 'Sheriff,' 'Police Department', 'State Attorney' or other law enforcement agency."[111] Other collectors have spoofed caller ID to appear as emergency responders and asked the consumer to verify their

---

[107] *Knoll v. IntelliRisk Mgmt. Corp*., 2006 WL 2974190 at *4 (D. Minn. Oct. 16, 2006).
[108] *Id.*
[109] 47 U.S.C. § 227(e)(1) (2012). *See generally,* Testimony and Statement for the Record of Marc Rotenberg President and Executive Director, EPIC, "Hearing on H.R. 5126, the Truth in Caller ID Act of 2006," Before the Subcommittee on Telecommunications and the Internet Committee on Energy and Commerce U.S. House of Representatives (May 18, 2006), *available at* http://epic.org/privacy/iei/hr5126test.pdf; EPIC Comments to the FCC, In the Matter of "Rules and Regulations Implementing the Truth in Caller ID Act of 2009," WC Docket No. 11-39 (Apr. 27, 2011), *available at* http://epic.org/apa/comments/EPIC-Truth-in-Caller-Cmts.pdf.
[110] *See Harvey v. Great Seneca Fin. Corp.,* 453 F.3d 324, 332 (6th Cir. 2006) ("[A] debt collector violates the FDCPA when it threatens or pursues litigation "to collect on a potentially time-barred debt that is otherwise valid.").
[111] Donald Petersen, *Just Spoofing*, FAIR DEBT COLLECTION PRACTICES ACT BLOG (Dec. 7, 2010), http://www.fdcpa.me/just-spoofing/.

identity because a family member was in the hospital, only then to reveal themselves as a debt collector.[112] Spoofing enables this type of deceit and harassment, and causes the very harms Congress sought to prevent in the FDCPA.

Although Courts have been more reluctant to find Caller ID blocking in violation of the FDCPA,[113] this practice also harms to consumers. Blocking or spoofing can be used by collectors trying to get around the anti-harassment provisions of the FDCPA by limiting a consumer's ability to generate phone records proving that a collector made impermissible calls. Preserving evidence of illegal collection calls is imperative for aggrieved consumers, and one important way to do this is Caller ID evidence.[114] One of the central purposes of the FDCPA was to limitations on debt collection practices and allow consumers with legal remedies if their rights were violated.[115] Caller ID blocking can allow collectors to intentionally deprive consumers of key evidence of illegal collection practices.

Debt collectors spoofing caller ID information is and should be illegal under current federal law. Blocking should be banned as well. It causes similar harm to consumers and enables deceptive practices. Any intentional interference with a collector

---

[112] *Id.*

[113] *Glover v. Client Servs*., Inc., 2007 WL 2902209 at *4 (W.D. Mich. Oct. 2, 2007). *Contra* Jiminez v. Accounts Receivable Mgmt., Inc., 2010 WL 5829206 at *6 (C.D. Cal. Nov. 15, 2010) ("Again, it is not impossible to imagine some scenario in which a debt collector's hanging up without leaving any identifying information might entail a violation of the statute (for example, if the debt collector used some form of caller identification blocking device).").

[114] *See* Cerrato v. Solomon & Solomon, 909 F. Supp. 2d 139, 149 (D. Conn. 2012) ("[T]he court has determined that eight unanswered telephone calls can constitute "communications" under the FDCPA—at least calls in which the debt collector's name and telephone number appear on the consumer's caller ID display.").

[115] 15 U.S.C. § 1692.

identifying themselves as a collector flies in the face of the core principles of the FDCPA: notice and disclosure to consumers.

Conclusion

EPIC appreciates this opportunity to comment and looks forward to continued public engagement on the issue of debt collection and privacy.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Administrative Law Counsel

Julia Horwitz
EPIC Consumer Protection Counsel

Electronic Privacy Information Center
1718 Connecticut Avenue, NW, Suite 200
Washington, DC 20009
(202) 483-1140