epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

CONSUMER FINANCIAL PROTECTION BUREAU

Proposed Amendment of Regulation F, 12 C.F.R. pt. 1006

[Docket No. CFPB-2019-0022]

September 18, 2019

By notice published on May 21, 2019, the Consumer Financial Protection Bureau ("CFPB") requested comments on the proposed amendment of Regulation F, 12 C.F.R. pt. 1006, which implements the Fair Debt Collection Practices Act ("FDCPA") and currently contains the procedures for State application for exemption from the provisions of the FDCPA.[1] CFPB proposes to amend Regulation F to prescribe Federal rules governing the activities of debt collectors. The Bureau requested comments on its proposals to address communications in connection with debt collection, clarify requirements for certain consumer-facing debt collection disclosures, and interpret and apply prohibitions on harassment or abuse, false or misleading representations, and unfair practices in debt collection.

Pursuant to the agency's request, the Electronic Privacy Information Center ("EPIC") submits these comments to highlight the substantial harms to consumers caused by debt collectors and underscore privacy concerns that should be considered in the agency rulemaking. In these

[1] Debt Collection Practices (Regulation F), 84 Fed. Reg. 23274 (May 21, 2019) (to be codified at 12 C.F.R. pt. 1006) [hereinafter Proposed Amendment of Regulation F], https://www.federalregister.gov/documents/2019/08/02/2019-16476/debt-collection-practices-regulation-f-extension-of-comment-period.

comments EPIC recommends that the CFPB: (1) clarify the definition of debt collector, (2) impose limitations on quantities of texts and emails, (3) not provide a safe harbor for debt collectors through limited-content messages, (4) impose liability for third-party disclosures by email or text, (5) require debt collector to offer a streamlined process for opt-out on any given medium, (6) limit the consumer information that can be included in debt validation notices, and (7) require debt collectors to comply with E-Sign Act consent requirements.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy issues.[2] EPIC has a particular interest in safeguarding consumer privacy and preventing harmful data practices. EPIC routinely comments on regulations which impact consumer privacy and protect individuals from telephone and Internet misuse. These include comments on the CAN-SPAM Act and proposed National "Do Not Email" Registry, advanced methods to eliminate unlawful robocalls, and "Rules and Regulations Implementing the Truth in Caller ID Act of 2009."[3] EPIC has previously submitted comments to CFPB on the "Debt Collection Survey from the Consumer Credit Panel" and the CFPB Consumer Complaint Narrative, CFPB-2014-0016.[4]

---

[2] EPIC, *About EPIC* (2019), https://epic.org/epic/about.html.

[3] *See, e.g.*, EPIC, *Comments on CAN-SPAM Rule, CFR Part 316, Project No. R711010* (Aug. 31, 2017), *available at* https://epic.org/apa/comments/EPIC-FTC-CAN-SPAM-Comments.pdf; 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; EPIC, *Comments on Refreshed Record on Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59* (Sept. 24, 2018), *available at* https://epic.org/apa/comments/EPIC-FCC-Robocalls-Refresh-Sept2018.pdf; EPIC, *Comments on Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59 FCC 17-24* (July 31, 2017), *available at* https://epic.org/apa/comments/EPIC-FCC-Robocall-ReplyComments.pdf; EPIC, *Comments on "Rules and Regulations Implementing the Truth in Caller ID Act of 2009," WC Docket No. 11-39* (2011), *available at* https://epic.org/apa/comments/EPIC_FCC_Truth_in_Caller_ID_1.pdf.

[4] EPIC, Comments on "Debt Collection Survey from the Consumer Credit Panel" (Sept. 29, 2014), *available at* https://epic.org/apa/comments/EPIC-Comments-FDCPA.pdf; EPIC, *CFPB Consumer Complaint Narrative Comments, Docket No. CFPB-2014-0016* (Sept. 19, 2014), *available at* https://epic.org/apa/comments/CFPB-Complaint-Cmts-9-19-14.pdf.

I. Debt Collection Practices Continue to Cause Substantial Consumer Harm.

A. Unfair Debt Collection Practices Intrude on Consumer Privacy.

Constant communications by debt collectors are a substantial invasion of consumer privacy. Unsolicited calls, texts, and e-mails facilitate fraud, drain battery life, eat into data plans and phone battery space, and interrupt consumers' daily routines. Consumers constantly carry their phones, looking at them an average of 52 times per day.[5] This results in unwanted calls, texts, and e-mails disturbing meetings and meals, interrupting consumer sleep, and disrupting important moments in consumers' lives. At a minimum, this is incredibly embarrassing for consumers.[6] Debt is also a major relationship challenge for many marriages, and unfair debt collection practices often contribute to marital stress.[7] Debt collection practices can also contribute to a loss of employment.[8] In addition to disrupting relationships and careers, the constant financial stress of debt collection can lead to physical pain over time.[9]

These communications often result in economic harm to consumers, ranging from additional cellular service charges to lost income due to loss of employment. These harms particularly affect low-income consumers, who often rely on pay-as-you-go, limited-minute prepaid wireless plans that

---

[5] Deloitte, *Global Mobile Consumer Survey, US Edition* (2018), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-global-mobile-consumer-survey-extended-deck-2018.pdf.

[6] Consumer Credit Counseling Service, *Poll Respondents More Embarrassed to Admit Credit Card Balance and Credit Score than Age or Weight* (2014), https://cccsoftheozarks.org/poll-respondents-embarrassed-admit-credit-card-balance-credit-score-age-weight/.

[7] Fidelity Investments, *2018 Fidelity Investments Couples & Money Study* (2018), https://www.fidelity.com/bin-public/060_www_fidelity_com/documents/pr/couples-fact-sheet.pdf.

[8] Martha C. White, *Yikes-When Debt Costs You a Job*, TIME (Sept. 17, 2012), http://business.time.com/2012/09/17/yikes-when-debt-costs-you-a-job/.

[9] Eileen Y. Chou, Bidhan L. Parmar, Adam D. Galinsky, *Economic Insecurity Increases Physical Pain*, Psychological Science (Feb. 18, 2016).

can be quickly exhausted by communications from debt collectors.[10] Calls from debt collectors are also more likely to jeopardize the employment of low-income consumers who serve as at-will employees.

The need to combat these invasions of privacy is at the core of the Federal Debt Collection Practices Act ("FDCPA"). When enacting the FDCPA, Congress noted that: "There is abundant evidence of the use of abusive, deceptive, and unfair debt collection practices by many debt collectors. Abusive debt collection practices contribute to the number of personal bankruptcies, to marital instability, to the loss of jobs, and to invasions of individual privacy."[11] As the Supreme Court has summarized, "[d]isruptive dinner calls, downright deceit, and more besides drew Congress' eye to the debt collection industry."[12] These costs – including marital instability, loss of employment, economic harm, and even physical harms –have been amplified by the proliferation of mobile phone use today.[13] This makes it imperative that the Bureau impose additional restrictions on debt collectors.

B. Debt Collection Practices Expose Consumers to Risks of Data Breach.

Unfair debt collection practices, inadequate security procedures, and misuse of consumer information can expose consumers' personal information in third-party disclosures or larger data breaches, resulting in economic, social, and psychological harms to the consumer. There are numerous examples of this happening to date, including an online debt marketplace which "posted at least twenty-one portfolios of purported debts...containing the unencrypted, unmasked, sensitive

[10] Federal Communications Commission, *Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services, Twentieth Report*, WT Docket No. 17-69, 38-39 (Sept. 27, 2017) [hereinafter *FCC Annual Report*] (noting that "prepaid subscribers may lack the credit background or income necessary to qualify for postpaid service").
[11] 15 U.S.C. 1692 § 802(a).
[12] *Henson v. Santander Consumer USA, Inc.*, 137 S. Ct. 1718, 1720 (2017).
[13] *FCC Annual Report, supra* note 10, at 11 (noting that nearly 400 million mobile wireless connections existed by the end of 2016).

personal information of more than 28,000 consumers"[14] and a debt sales website which "offered their debt portfolios for sale by posting them on this website in the form of unencrypted, unprotected Excel spreadsheets."[15] In one recent example involving a debt collector, the American Medical Collection Agency's inadequate security practices exposed the personal information of over 20 million consumers, including names, birth dates, social security numbers, addresses, phone numbers, medical information, credit card information, bank account numbers, and insurance information.[16] These consumers remain at risk from this data breach today and will remain at risk for the foreseeable future.

Improper disclosure of debt-related information can have dramatic consequences for consumers. As catalogued by the Government Accountability Office, the exposure of sensitive personal information leads to harms including: financial, tax refund, and government benefits fraud; medical, synthetic, and child identity theft; and lost time, emotional distress, lost privacy, reputational harm, and harm from state-sponsored espionage.[17] The costs can quickly balloon for consumers after a data breach. These costs begin with credit monitoring and repair services, but can snowball due to identity theft.[18] Data breaches often lead to unauthorized credit card purchases, tax

[14] *FTC v. Bayview Solutions, Tomko, and Ortiz*, No. 142-3226 (2014) (complaint), https://www.ftc.gov/system/files/documents/cases/111014bayviewcmp.pdf.
[15] *FTC v. Cornerstone and Company and Lambert*, No. 142-3211 (2014) (complaint), https://www.ftc.gov/system/files/documents/cases/141001cornerstonecmpt.pdf.
[16] Press Release, Office of the Attorney General of Maryland, *Consumer Alert: Attorney General Frosh Warns Marylanders of Massive Medical Data Breach* (June 12, 2019), http://www.marylandattorneygeneral.gov/press/2019/061219.pdf; Quest Diagnostics, *Unauthorized Access to Database at AMCA Containing Personal Information* (July 8, 2019), https://questdiagnostics.com/home/AMCA-data-breach-patients.html.
[17] U.S. Gov't Accountability Office, GAO-19-230, *Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services* 4–6 (2019), https://www.gao.gov/assets/700/697985.pdf [hereinafter *GAO Data Breaches*].
[18] Staff of Permanent Subcomm. on Investigations of the S. Comm. on Homeland Security and Governmental Affairs, 116th Cong., *How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach* 1 (2019) (noting that victims of data breaches "can be left with years of expense and hassle").

fraud, and fraudulent loans and medical expenditures.[19] This in turn destroys victims' credit scores, forces them to pay higher interest rates, prevents them from obtaining loans, leads to their utilities being cut off, and, in extreme cases, forces them to file bankruptcy or lose their homes. On the whole, two-thirds of identity-theft victims reported direct financial loss in 2016.[20] Victims of data breaches also experience heavy emotional costs, from problems with family and friends to severe distress.[21]

Unfair debt collection practices place consumers at particular risk because of the sensitive nature of the information involved in debt document and the insecure nature of debt collection practices and marketplaces. Debt documentation includes highly sensitive personal information, including "the consumer's name, social security number, home and work telephone number, and street address" and "financial information such as account number, original creditor name, current balance, date of last payment, and date of charge-off associated with the debt."[22] This data gets transferred between numerous parties in the debt collection process, increasing the risk of a data breach through unauthorized disclosure, unauthorized sale, or insecure storage of consumer information.[23] As summarized by the Bureau in a recent report, "the ease with which debts can be bought and sold online may increase the risk that debts – and the sensitive consumer information associated with them – will fall into the wrong hands."[24]

---

[19] *GAO Data Breaches*, *supra* note 16, at 4-6.
[20] Erika Harrell, Bureau of Justice Statistics, *Victims of Identity Theft, 2016*, at 7 (2019).
[21] *Id.* at 10-12.
[22] Consumer Financial Protection Bureau, *Market Snapshot: Online Debt Sales* 2 (Jan. 2017), https://files.consumerfinance.gov/f/documents/201701_cfpb_Online-Debt-Sales-Report.pdf [hereinafter *CFPB Market Snapshot*]; *see also* Fed. Trade Comm., *The Structure and Practices of the Debt Buying Industry* 34 (2013), https://www.ftc.gov/sites/default/files/documents/reports/structure-and-practices-debt-buying-industry/debtbuyingreport.pdf [hereinafter *FTC Debt Buying 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.").
[23] Proposed Amendment of Regulation F, *supra* note 1, at 23276.
[24] *CFPB Market Snapshot* at 2.

i. Unfair Debt Collection Practices Risk Exposure of Social Security Numbers.

The exposure of a consumers' social security number is particularly harmful. When a criminal gains access to an individual's SSN, he or she can obtain tax refunds and government benefits, receive medical goods and services, apply for employment, and even commit crimes in the victim's name.[25] SSNs are the key to our financial, government, and private sector records systems. No other form of identification plays a more significant role in record-linkage or poses a greater risk to personal privacy.[26] As both an identifier and authenticator, SSNs serve as both the username and password for an individual's identity.

To make matters worse, a stolen SSN, unlike a stolen credit card, cannot be effectively cancelled or replaced. While the Social Security Administration ("SSA") can issue replacement SSNs, it does so only in limited circumstances, such as "harassment, abuse, or life endangerment."[27] Identity theft victims must reach this desperate state before the agency will even consider issuing a replacement. Even if an identity theft victim has suffered such grievous harm to merit a replacement SSN, problems will continue. The SSA has acknowledged the inadequacy of replacement SSNs, stating that a "new number probably won't solve" your problems because "other governmental agencies" and businesses have records tied to the old number, and "credit reporting agencies will [still] use the number to identify your credit record."[28]

In fact, social security numbers and financial information are so valuable to criminals that there are black markets for this information that are dominated by "financially driven, highly

---

[25] Identity Theft Res. Ctr., *Identity Theft: The Aftermath* 13 (2014), http://www.idtheftcenter.org/images/surveys_studies/Aftermath2014FINAL.pdf.
[26] See EPIC, *Social Security Numbers* (2016), https://www.epic.org/privacy/ssn/.
[27] Soc. Sec. Admin., *Can I Change My Social Security Number?* (Mar 11, 2016), https://faq.ssa.gov/link/portal/34011/34019/Article/3789/Can-I-change-my- Social-Security-number.
[28] Soc. Sec. Admin., Identity Theft and Your Social Security Number 6 (Feb. 2016), https://www.ssa.gov/pubs/EN-05-10064.pdf.

organized, and sophisticated groups" and "can be more profitable than the illegal drug trade."[29] The dossiers of personal data that can be used to commit fraud—including name, address, and SSN in combination with financial data—are referred to as "Fullz" and can be sold in bulk for as much as $15 per victim.[30] Once the data breach occurs, the damage is already done, and there is nothing the victim can do to reclaim their personal information.

ii. The Structure of the Consumer Debt Marketplace Jeopardizes Consumers' Data.

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. As previously discussed, this sensitive consumer data located in debt documentation includes consumer names, addresses, phone numbers, social security numbers, and account numbers.[31] In addition to passing between buyers and sellers, this sensitive information is often shared with prospective buyers as part of a "bid file" a collection documents and information provided to help potential purchasers make bidding decisions.[32] These prospective buyers can include person located via telephone calls, mailing lists, clearinghouses, web advertisements, and email alerts, as well as well-established industry purchasers.[33] Even when some data in the bid files are redacted, there does not appear to be any consistency in or regulation of what data must be redacted when showing portfolios to prospective buyers.[34]

---

[29] Lillian Ablon, Martin C. Libicki, & Andrea A. Golayix, RAND Corp., *Markets for Cybercrime Tools and Stolen Data,* at ix, 11, 17 (2014).
[30] Dell SecureWorks, Underground Hacker Markets 14 (2016), https://www.secureworks.com/resources/rp-2016-underground-hacker- marketplace-report.
[31] *Supra* Part 1(B); *see also* Consumer Financial Protection Bureau, *Market Snapshot: Online Debt Sales* 2 (Jan. 2017), https://files.consumerfinance.gov/f/documents/201701_cfpb_Online-Debt-Sales-Report.pdf.
[32] *FTC Debt Buying Report* at 20.
[33] *Id.*
[34] *Id.* at 21.

If debt is resold to secondary buyers, "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."[35] 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."[36] Each selling junction creates another opportunity for a third-party disclosure or larger data breach.

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. On average, any given U.S. organizations has a 26.9% chance of experiencing a material data breach in the next two years.[37] In the case of debt documentation, the risk is increased because the information is held by several organizations. In addition, marketplaces for debt are known to have inadequate data security practices.[38]

Accordingly, debt collectors' desire to collect outstanding debt must be weighed against the risks of data breach for consumers. The need to regulate debt collection in order to prevent these harms is particularly pressing given the data breach crisis currently affecting America. The U.S. experienced 1,244 breaches in 2018, exposing almost 450 million records to risk of identity theft and financial fraud.[39] There have already been several major data breaches in 2019, most recently

---

[35] *Id.* at iii-iv.
[36] *Id.* at 1.
[37] Ponemon Institute, *2018 Cost of a Data Breach Study: Global Overview* 32 (2018), https://www.ibm.com/downloads/cas/861MNWN2.
[38] *CFPB Market Snapshot* at 2.
[39] Identity Theft Research Ctr., *2018 End-of-Year Data Breach Report* 1 (2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

including a Capital One data breach affecting 100 million U.S. consumers.[40] Every year, more and more consumers experience identity theft as a result of data breach. According to the most recent report by the Department of Justice, an estimated 26 million Americans experience identity theft annually—a 48% increase from DOJ's previous biennial report.[41] Consumers also filed 445,000 reports of identity theft with the Federal Trade Commission in 2018, a 20% increase from the 370,000 reports filed in 2017.[42] In order to combat this data breach crisis, CFPB must impose strict restrictions on debt collectors' use, storage, and transfer of personally identifying information.

II. EPIC's Recommendations on the Proposed Amendment of Regulation F

A. CFPB Should Clarify That Any Party Which "Regularly Collects" Debts Owned by Others or Whose Business Has a "Principal Purpose" of Debt Collection *Always* Qualifies As a "Debt Collector" Under the FDCPA.

Rather than merely restating the language in FDCPA § 803(6), the Bureau should explicitly clarify that companies which satisfy either the "regularly collects" or "principal purpose" prong of the FDCPA definition *always* qualify as debt collectors under the FDCPA, regardless of whether the specific debt that they are collecting is owned by themselves or by another party. The definition of "debt collector" under the FDCPA is not limited to third-party collection agencies and includes (1) any party that "regularly collects or attempts to collect" debt owned by others and (2) any party engaging in "any business the principal purpose of which is the collection of any debts."[43] If a

[40] Seena Gressin, *The Capital One data breach: Time to check your credit report*, Federal Trade Commission (July 30, 2019), https://www.consumer.ftc.gov/blog/2019/07/capital-one-data-breach-time-check-your-credit-report.
[41] *Compare* Harrell, *supra* note 19, at 1 (2019), *with* Erika Harrell, Bureau of Justice Statistics, Victims of Identity Theft, 2014, at 1 (Sept. 2015) (finding that an estimated 17.6 million consumers were victims of identity theft in the preceding year).
[42] *Compare* Fed. Trade Comm'n, *Consumer Sentinel Network Data Book 2018*, at 4 (2019), *with* Fed. Trade Comm'n, Consumer Sentinel Network Data Book 2017, at 3 (2018).
[43] 15 U.S.C. 1692 § 803(6).

company satisfies either of these prongs, then the company is an FDCPA-covered debt collector in any of its debt collection practices, including when it is collecting debts on its own behalf.

In *Henson v. Santander Consumer USA, Inc.*, the Supreme Court held that a company which has purchased debts originated by someone else may collect those debts on their own account without being an FDCPA-covered debt collector.[44] CFPB correctly identifies the narrow scope of this opinion, which explicitly did not address the "principal purpose" component of the FDCPA definition or the fact that a company may nonetheless qualify as a debt collector "because it regularly acts as a third party collection agent for debts owed to others."[45] The Supreme Court explicitly left open these other ways in which a company qualifies as a debt collector under FDCPA § 803(6). As such, the Bureau's definition must specify that it includes a company collecting any type of debt if the company meets either the "regularly collects" or "principal purpose" prong of the FDCPA definition.

B. CFPB Should Impose Limitations on Quantities of Texts and Emails.

The CFPB should prescribe daily limits for the number email and text communications and limits on the times of the day that consumers can be contacted. As a result of the dominance of text messaging and e-mails, prescribing limits on debt collectors' use of e-mails and text messages is essential to protecting consumer privacy.

Emails and text messages are omnipresent in the average consumer's life. Consumers look at their phones an average of 52 times every day, and 93 percent of consumers use text messaging.[46] In fact, "[t]exting, using a cellphone and sending and reading email messages are the most frequently

[44] 137 S. Ct. 1718, 1719 (2017).
[45] *Id.* at 1721.
[46] Deloitte, *Global Mobile Consumer Survey, US Edition* (2018), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-global-mobile-consumer-survey-extended-deck-2018.pdf.

used forms of non-personal communication for adult Americans."[47] Many phones display the content of text messages on a consumer's phone without requiring it to be unlocked, so the private issue of personal debt could be revealed to anyone who is within the consumer's vicinity at the time that of receipt.

Receiving text messages can be costly for low-income consumers on prepaid cellphone plans which impose restrictions on text messages. This is especially problematic because lower-income consumers are more likely to be targeted for contact by debt collectors.[48] 36 percent of Americans do not have smartphones, and many have cell-phone plans that restrict the number of texts they can send or receive.[49] As a result, texting can impose a real financial cost on low-income consumers; it is for this reason that the Federal Trade Commission concluded: "the law should incorporate a presumption that consumers will incur a charge for a call or text message made to their mobile phones."[50]

Text-messaging consumers poses very little to zero costs on the sender, which encourages debt collectors to use mass text messaging to harass consumers. For example, one bulk text messaging company advertises that its service for debt collection is "virtually free," that automatic payment reminders require minimal effort on the part of the debt collector, and that "[t]ext reminders create a sense of urgency."[51] The minimal costs of text messaging consumers incentivize debt

---

[47] Frank Newport, *The New Era of Communication Among Americans*, Gallup (Nov. 10, 2014), *available at* http://www.gallup.com/poll/179288/new-era-communication-americans.aspx.
[48] Consumer Finance Protection Bureau, *Consumer Experiences with Debt Collection* (Jan. 2017), https://files.consumerfinance.gov/f/documents/201701_cfpb_Debt-Collection-Survey-Report.pdf ("Lower-income consumers and consumers between the ages of 35 and 49, for example, were more likely than others to report having been contacted about a debt in collection").
[49] Aaron Smith, *U.S. Smartphone Use in 2015*, Pew Research Center (Apr. 1, 2015) https://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.
[50] Federal Trade Comm'n, *Collecting Consumer Debts: The Challenges of Change, a Workshop Report*, *available at* https://www.ftc.gov/sites/default/files/documents/reports/collecting-consumer-debts-challenges-change-federal-trade-commission-workshop-report/dcwr.pdf.
[51] Alexa Lemzy, *Actionable Ways to Use Text Messaging for Debt Collection*, TextMagic Blog (Oct. 20, 2017), https://www.textmagic.com/blog/text-messaging-for-debt-collection/.

collectors to harass consumers by sending as many text messages as possible — text messages that the consumer may actually have to pay for, if their cell phone plan requires it.

Debt collectors must be limited in the number of text messages they can send to consumers, especially during workplace hours. In many workplaces, cell phones have replaced the traditional workplace phone: 84 percent of working adults use their personal phones during working hours, so debt collection texts to a personal device can interrupt consumers at work.[52] Receiving a great number of text messages during the workday can create a red flag for an employer; indeed, repeated pings of text messages during workplace meetings may cause the embarrassment and reputational damage Congress sought to avoid by regulating workplace collection calls and prohibiting collectors from informing employers directly.[53]

Allowing debt collectors to text message consumers during workplace hours undermines the web of regulations and restrictions on workplace calls. Congress created a variable legal framework that regulates workplace calls, allowing them in some circumstances and disallowing them in others.[54] Failing to place limits on text messages would allow debt collectors to bypass the regulations that they otherwise face regarding contacting consumers in the workplace. An across-the-board daily limit on text messaging consumers would create a bright line rule that all parties can depend on.

---

[52] Deloitte, *Global Mobile Consumer Survey, US Edition* (2018), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-global-mobile-consumer-survey-extended-deck-2018.pdf.

[53] 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"); H.R. Rep. No. 95-131, at 6 (1977) (explaining that contact between an employer and a debt collector "constitutes an unwarranted invasion of the consumer's privacy and interference with the consumers employee-employer relationship").

[54] 15 U.S.C.A. § 1692c(a)(3) (2012).

Legal limits are essential because debt collectors have demonstrated a persistent failure to self-regulate. Collectors estimate they contact consumers more than a billion times a year.[55] In 2018, the CFPB received over 6,000 complaints specifically about debt collectors' communications tactics.[56] For example, a 2019 CFPB complaint reads, "Non stop repeated phone calls. no messages, calling family members phone numbers, not sure how they got the numbers. calling [from] unknown numbers. text messages to family members. calling on sunday mornings. called on easter sunday morning. weekends. all times."[57] A 2017 CFPB report demonstrated that 63 percent of consumers who had been contacted about a debt in collection felt that they were contacted too often. It also showed that 75 percent of consumers who requested that their debt collector stop calling them reported that the debt collectors did not honor their requests.[58] Corporations have even filed suit against debt collectors for persistent disruptive practices in contacting their employees.[59]

C. CFPB Should Not Provide a Safe Harbor for Debt Collectors Through "Limited-Content Messages."

CFPB's addition of a "limited-content message" delineation to its FDCPA regulations will provide a safe harbor for debt collectors when leaving an oral message or voicemail for a consumer.[60] This proposal places consumers in the position of having information about their debt

[55] Josh Adams, Methodological and Analytical Limitations of the CFPB Consumer Complaint Database 7 (2016), *available at* http://www.acainternational.org/assets/research-statistics/aca-wp-methodological.pdf.
[56] Consumer Complaint Database, Consumer Finance Protection Bureau, *available at* https://www.consumerfinance.gov/data-research/consumer-complaints/.
[57] Consumer Complaint No. 3228120, Consumer Finance Protection Bureau (May 1, 2019), https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/3228120
[58] Consumer Finance Protection Bureau, *Consumer Experiences with Debt Collection* (Jan. 2017), https://files.consumerfinance.gov/f/documents/201701_cfpb_Debt-Collection-Survey-Report.pdf.
[59] 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.
[60] The currently proposed definition requires the message to include "the consumer's name, a request that the consumer reply to the message, the name or names of one or more natural persons whom the consumer can contact to reply to the debt collector, a telephone number that the consumer can use to reply to the debt collector, and, if applicable, a disclosure explaining how the consumer can stop receiving messages through a

exposed to third-parties by debt collectors, who will nonetheless be protected from liability due to the technical designation of their message as a "limited content message." Without liability, debt collectors will have no incentive to minimize the number of messages left for consumers – despite the fact that the proposed "limited content messages" can still lead to an invasion of consumer privacy causing substantial harm.

This proposal is highly problematic for consumer privacy, as the proposed "limited-content messages" will not protect consumers from having third-parties see or hear information about their debt collection status.[61] In practice, it will be easy for third parties who hear the proposed "limited-content messages" to ascertain that the communication is about a debt collection. In the case of a third-party individual who speaks with a debt collector on the phone, he or she will likely be confused by the debt collector's reticence and thus suspect that the call is related to either debt collection or something more nefarious. Individuals are likely to ask follow-up questions when taking messages and will grow suspicious at the terse answers that they will receive under the restrictions. The word "account" will make most individuals suspect debt collection or financial fraud, creating additional confusion for the third-party while failing to protect the consumer from what effectively still becomes a third-party disclosure of the debt.

Third parties will be similarly suspicious of voicemails referencing an "account" that are left on a shared line with the debtor or erroneously directed to the third party. Because voicemails have become less popular with consumers,[62] often consumers only expect to receive voicemails from

---

particular medium." The message may also include a "salutation, the date and time of the message, a generic statement that the message relates to an account, and suggested dates and times for the consumer to reply to the message." The debt collector cannot share any additional information. Proposed Amendment of Regulation F, *supra* note 1, at 23379.

[61] *See id.* (citing a survey result indicating that nearly two-thirds of consumers say that it is very important that others do not hear or see a message from a creditor or debt collector).

[62] Teddy Wayne, *At the Tone, Leave a What? Millennials Shy Away from Voice Mail*, New York Times (June 13, 2014), http://www.nytimes.com/2014/06/15/fashion/millennials-shy-away-from-voice-mail.html.

parties like doctors or financial institutions and will be suspicious of voicemails left by debt collectors. If this rule is instituted, debt collectors will begin to leave these messages frequently, all of which will assume the same format. As more and more messages are left, it will become quickly apparent to any third party who hears the voicemails that the messages concern debt collection.

The same is true of text messages. Text messages are even more problematic, as a preview of messages received often automatically populates on consumers' smartphone lock screens. The deluge of uniform text messages that will begin to be sent to consumers under this proposed rule will clearly indicate to any third party who sees the consumers' phone screen that he or she is being pursued by a debt collector. There is thus a high-risk of third-party disclosures even when debt collectors are texting a line that is solely owned by the debtor.

CFPB's current proposal to limit limited-content messages to voicemail, text message, or oral transmission does not solve these issues in any way.[63] While the proposed rule correctly recognizes that email addresses may provide additional information that conveys information about a debt, it fails to recognize that the same is true for phone numbers. A quick Google search of a phone number often reveals the caller, either through public listings or consumer reports of previous calls from the number on websites like 800notes.com.[64] This is particularly true for debt collectors, as consumers are particularly likely to report information about callers like telemarketers or debt collectors online.[65]

---

[63] Proposed Amendment of Regulation F, *supra* note 1, at 23291.
[64] *See, e.g.*, Tim Fisher, *How to Use Google for a Reverse Phone Lookup*, Lifewire (July 1, 2019), https://www.lifewire.com/how-to-use-google-for-a-reverse-phone-lookup-3481893.
[65] Latoya Irby, *How Can I Find out Which Collection Agency I Owe?*, The Balance (June 25, 2019), https://www.thebalance.com/how-can-i-find-out-which-collection-agency-i-owe-960657 (recommending that consumers locate collection agencies by "typing the number into a search engine"" to see results from websites "where other people have shared information about who called from that number and the nature of the call).

If the proposed rule is implemented as it currently stands, debt collectors will employ near-constant text messages and voicemails to harass consumers. The Bureau cites concerns of debt collectors about not being able to leave messages for fear of FDCPA liability as the primary reason to implement the proposed rule regarding "limited content messages."[66] It follows that debt collectors will subsequently leave a large quantity of messages once they are freed from liability by the proposed rule. By only using language permitted under the proposed definition of "limited content message," debt collectors will escape liability for inappropriate behaviors such as third-party disclosures. They can text or leave a message for any phone number that could possibly be the consumer and be free from liability even if the number is in fact owned by a third-party and the consumers debt collection status is thus disclosed to that party. Depending on who receives, views, or hears the message, these types of disclosures can result in severe personal consequences such as marital distress or termination of employment.[67] Without FDCPA-liability, there is no reason for debt collectors to invest in avoiding third-party disclosures or restrain their messages in any way.

D. CFPB Should Impose Liability for Third-Party Disclosures by Email or Text.

The Bureau has also "proposed procedures that, when followed, would protect a debt collector from liability for unintentional violations of the prohibition against third-party disclosures when communicating with a consumer by email or text message."

Debt collectors must be required to verify the contact information of consumers prior to sending to an email or text with sensitive information. The alternative is incentivizing debt collectors to use email or text methods to contact debtors without concern for the potential release of sensitive information that could lead to identity theft or financial fraud. It is irrelevant whether the debt

[66] Proposed Amendment of Regulation F, *supra* note 1, at 23380.
[67] *Supra* Part I(A).

collector had the specific intent of violating the prohibition against third-party disclosures, especially because a violation would likely not occur out of malicious intent but rather out of a debt collector's carelessness; once the disclosure has been made, the damage to a consumer's personal or professional reputation has been done, while the risk of identity theft has been created.

Debt collectors must recognize that the design of text messages heighten the likelihood of third-party disclosures — which can cause substantial harm because debt is a sensitive issue. Most pertinently, many cell phones display messages on their phone without unlocking the phone; as a result, in an instant, anyone in the consumer's vicinity can be made aware of the consumer's private debt issues. At home, consumers risk hostility and even violence from family members.[68] Scholars have analyzed the link between domestic violence and consumer credit.[69] In fact, financial abuse plays a role in in most cases of domestic violence.[70] A consumer facing an abusive household or domestic violence could made even more vulnerable when an abuser recognizes that they are in debt. Debt collectors must recognize that careless text messaging could result in significant personal or professional consequences, and an incentive structure must encourage debt collectors to affirmatively protect consumer privacy.

Debt collectors frequently make mistakes about whether they have contacted the right person or whether the person contacted has any debt at all. In fact, according to a 2017 CFPB report, more than half of consumers who had been contacted by debt collectors or creditors said that at least one debt was in error.[71]

---

[68] 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

[69] 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/.

[70] *See id*. at 972.

[71] Consumer Finance Protection Bureau, *Consumer Experiences with Debt Collection* 24 (Jan. 2017), https://files.consumerfinance.gov/f/documents/201701_cfpb_Debt-Collection-Survey-Report.pdf.

Debt collector liability for disclosing sensitive personal and financial information is essential to prevent identity theft and financial fraud. Inadvertent or intentional third-party disclosures might very well include all the information that a savvy attacker needs to commit identity theft. Even if a third party only received an incomplete financial information from a debt collector, they could easily fill in the gaps via commercial databases, information easily available online on social media websites, or personal information sold online as a result of data breach.

Today's debt collection practices occur in a data environment that in which identity theft and financial fraud are easily enabled. Privacy Rights Clearinghouse estimated that 446 million personal records were exposed during the year of 2018 following data breaches in the public and private sectors.[72] As a result, 86 percent of consumers are concerned about companies sharing their personal data with third parties.[73] Debt collectors store millions of consumers' sensitive financial information and thus have an affirmative obligation to consumers to safeguard their privacy.

E. Debt Collectors Must Offer a Streamlined Process for Opt-Out on Any Given Medium.

EPIC agrees with the decision to "[c]larify that a consumer may restrict the media through which a debt collector communicates by designating a particular medium, such as email, as one that cannot be used for debt collection communications." It also agrees with the Bureau's proposal "to require that a debt collector's emails and text messages include instructions for a consumer to opt out of receiving further emails or text messages." The proposed option to unsubscribe is essential for consumer privacy.

---

[72] Identity Theft Resource Center, 2018 End-of-Year Data Breach Report (2018), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[73] Deloitte, *Global Mobile Consumer Survey, US Edition* (2018), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-global-mobile-consumer-survey-extended-deck-2018.pdf.

However, the CFPB should specify that this process must be streamlined for consumers. The proposed clarification must ensure that debt collectors make the process as easy as possible for consumers in order to avoid FDCPA liability.

The revocation of consent should not be limited to a single prescribed method because debt collectors are incentivized to make that method as difficult as possible. Instead, the CFPB should require debt collectors to give consumers simple methods for revoking consent. These methods should be accomplishable through the same medium in which the consumer wishes to no longer receive communication. This notification should be easy to understand and should be announced early in the message (i.e., the subscriber should not have to listen to the entire robocall or select menu options to hear the notice). Reasonable methods include: pushing a standardized code like "*7," or saying "stop calling" in response to a phone voicemail, replying "stop" to a text message, or clicking an "unsubscribe" button on an email. Debt collectors should be required to make it as easy as possible for consumers to adjust their preferences. This in turn will motivate consumers not to choose more burdensome methods, like mailing a letter — although these options should still remain available if a consumer prefers them.

Additionally, debt collectors must comply with a subscriber's revocation within 24 hours. Due to the frequency of some robocalls, a short compliance period is necessary to ensure that consumers' opt-out of communication is honored.

A streamlined opt-out process is essential because e-mails and other virtual communications allow debt collectors to invade consumers' privacy in ways that were not previously possible. One 2019 CFPB complaint reads: "I have a debt with XXXX but trueaccord has taken over this debt. This lady keeps emailing me constantly. She has even went so far as to tell me that she knows I am opening the emails. She is harassing me at this point. This lady has emailed me 17 times since

XX/XX//18. This is not okay. Please help me."[74] Debt collectors have used the internet to target individuals and continue to harass them: CFPB consumer complaints detail instances of debt collectors creating Facebook accounts to contact them on the social network and contacting family members on social media.[75]

F. CFPB Should Limit the Consumer Information That Can Be Included in Debt Validation Notices.

The Bureau has proposed to interpret FDCPA § 809(a) in § 1006.34(a)(1) and has requested commentary on its proposed rule.[76] The FDCPA does not specify any consumer information that must be included in the debt validation notice.[77] Accordingly, CFPB should follow the FDCPA's lead and minimize the personally identifying consumer information that debt collectors are permitted to include on debt validation notices. The Bureau should add a provision to the proposed rule specifying that debt collectors are not permitted to include additional personal consumer information other than name and address in the debt validation notice. The Bureau should also institute similar restrictions for debt collectors who provide the validation information orally.[78] Given the data breach crisis currently impacting debt collectors,[79] CFPB also must ensure that its recommended process to provide validation notice electronically maintains the security of the sensitive consumer information that is included in notices.

---

[74] Consumer Complaint No. 3160799, Consumer Finance Protection Bureau (Feb. 23, 2019), https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/3160799.
[75] Consumer Complaint No. 1735583, Consumer Finance Protection Bureau (Jan. 11, 2016), https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/1735583; Consumer Complaint No. 2352933, Consumer Finance Protection Bureau (Feb. 21, 2017), https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/2352933; Consumer Complaint No. 2365210, Consumer Finance Protection Bureau (Mar. 1, 2017), https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/2365210.
[76] 15 U.S.C. 1692 § 809(a); Proposed Amendment of Regulation F, *supra* note 1, at 23338.
[77] 15 U.S.C. 1692 § 809(a).
[78] *See* Proposed Amendment of Regulation F, *supra* note 1, at 23334.
[79] *Supra* Part I(B).

These restrictions are essential given the privacy concerns that arise with debt validation notices, including identity theft and the exposure of sensitive private facts to strangers.[80] Validation notices should never include any personal identifiers beyond name and address, including, but not limited to, birthdate, social security number, or medical conditions. While information such as a birthdate may appear somewhat innocuous, small amounts of data can be used to obtain more dangerous amounts of personal information, such as social security numbers. For example, Social Security numbers can be guessed with a 44% success rate by knowing an individual's birthdate and zip code.[81] As previously discussed, the exposure of a social security number is incredibly hazardous to consumers.[82]

Accordingly, CFPB must institute limits on the consumer information that can be included in debt validation notices in order to protect consumer privacy. These limits will not diminish the consumers' ability to identify the debt. As proposed by CFPB, validation notices should contain information specific to the debt in order to enable consumers to better identify the debts. Debt validation notices do not require information about the debtor when adequate information about the debt is provided instead.

The consumers' name and mailing address may be necessary to include for the purposes of physical mailings, however, CFPB should impose liability for debt collectors who send debt validation notices to incorrect or outdated addresses. Given the old age of many debts in collection, some consumer addresses on original debt documentation are be incorrect. This makes the Bureau's proposal to require the address merely to be "the most complete information that the debt collector obtained from the creditor or another source" too lax and highly problematic.[83] Debt collectors must

[80] *Supra* Part I(B).
[81] Alessandro Acquisti and Ralph Gross, *Predicting Social Security Numbers from Public Data,* 106(27) Proceedings Of The National Academy Of Science 10977 (2009).
[82] *Supra* Part I(A)(ii).
[83] Proposed Amendment of Regulation F, *supra* note 1, at 23339.

be incentivized to confirm addresses prior to sending sensitive information about the debt to the address of a third-party rather than the consumer. Furthermore, CFBP must not create a safe harbor for debt collectors who deliver a validation notice within the body of an email that is the debt collector's initial communication with the consumer. Unverified emails pose the same risks as mail to unverified addresses.

G. Debt Collectors Should Comply with the E-Sign Act's Consent Requirements

Debt collectors should be required to comply with the E-Sign Act before sending key notices electronically. Under the E-Sign Act, consumers must affirmatively consent in a manner that demonstrates they have access to the relevant records.[84] When the law requires that consumers receive important information, consumers must consent to replace paper with electronic records that they are capable of receiving.

Without the E-Sign Act's consent requirements, too many consumers will not receive critical disclosures. About sixty percent of U.S. residents of rural areas believe access to high speed internet is a problem in their area and about twenty-five percent believe it is a major problem in their area.[85] And ten percent of U.S. adults do not use the Internet.[86] Without confirmation that the consumer has received the electronic communications, the debt collector will not know whether it has been received by someone other than the intended recipient mistakenly. This presents a privacy problem, as others may have access to old accounts when users switch phone numbers and email addresses.

---

[84] 15 U.S.C. § 7001(c).
[85] Monica Anderson, *About a quarter of rural Americans say access to high-speed internet is a major problem*, Pew Research Center (Sept. 10, 2018), https://www.pewresearch.org/fact-tank/2018/09/10/about-a-quarter-of-rural-americans-say-access-to-high-speed-internet-is-a-major-problem/.
[86] Monica Anderson, Andrew Perrin, KingKing Jiang, and Madhumitha Kumar, *10% of Americans don't use the internet. Who are they?*, Pew Research Center (April 22, 2019), https://www.pewresearch.org/fact-tank/2019/04/22/some-americans-dont-use-the-internet-who-are-they/.

Conclusion

For the above reasons, EPIC recommends that the CFPB: (1) clarify the definition of debt collector, (2) impose limitations on quantities of texts and emails, (3) not provide a safe harbor for debt collectors through limited-content messages, (4) impose liability for third-party disclosures by email or text, (5) require debt collectors to offer a streamlined process for opt-out on any given medium, (6) limit the consumer information that can be included in debt validation notices, and (7) require debt collectors to comply with E-Sign Act consent requirements.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Christine Bannan*
Christine Bannan
EPIC Consumer Protection Counsel

/s/ *Sarah Parker*
Sarah Parker
EPIC Law Clerk

/s/ *Sonali Seth*
Sonali Seth
EPIC Law Clerk