Comments to the Federal Trade Commission

regarding the

Telemarketing Sales Rule Regulatory Review

16 CFR Part 310
RIN 3084-AB19
R411001

89 Fed. Reg. 26798 (Apr. 16, 2024)
Notice of Proposed Rulemaking

submitted by
Electronic Privacy and Information Center and
National Consumer Law Center (on behalf of its low-income clients)

June 17, 2024

Chris Frascella, Counsel
Frascella@epic.org
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036

Margot Saunders, Senior Counsel
MSaunders@nclc.org
National Consumer Law Center
1001 Connecticut Ave, NW
Washington, DC 20036

Introduction

The Federal Trade Commission (FTC or Commission) has released a Notice of Proposed Rulemaking (NPRM) amending the Telemarketing Sales Rule (TSR or Rule) to require that inbound technical support calls in response to solicitations comply with the Rule.[1] As we stated in previous comments filed on behalf of multiple national and state consumer and privacy advocacy organizations,[2] the **Electronic Privacy Information Center** (EPIC),[3] and the **National Consumer Law Center** (NCLC), on behalf of our low-income clients,[4] strongly support the FTC's proposal.[5] We do, however, urge the FTC to make one clarifying change to the language of the regulation, and to clarify the new regulations to the FTC's Business Guidance on the TSR.[6]

---

[1] Telemarketing Sales Rule, 89 Fed. Reg. 26,798 (Apr. 16, 2024), https://www.govinfo.gov/content/pkg/FR-2024-04-16/pdf/2024-07182.pdf [hereinafter "NPRM"], also available at https://www.federalregister.gov/documents/2024/04/16/2024-07182/telemarketing-sales-rule.

[2] These comments are in furtherance of our ANPRM comments. *See* Comments to the Fed. Trade Comm'n, Telemarketing Sales Rule Regulatory Review, RIN 3084-AB19, 87 Fed. Reg. 33662, FTC-2022-0033-0017 (Aug. 2, 2022), available at https://www.regulations.gov/comment/FTC-2022-0033-0017 (sign-on organizations included Center for Digital Democracy, Consumer Action, Consumer Federation of America, FoolProof, Mountain State Justice, National Consumers League, New Jersey Citizen Action, Patient Privacy Rights, Public Good Law Center, Public Justice Center, Public Knowledge, South Carolina Appleseed Legal Justice Center, and Cathy Lesser Mansfield (Senior Instructor in Law, Case Western Reserve University School of Law).

[3] Electronic Privacy Information Center (EPIC) was established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. EPIC has played a leading role in developing the authority of the FTC to address emerging privacy and cybersecurity issues and to safeguard the privacy rights of consumers. EPIC routinely files comments in response to proposed FTC rules and consent orders as well as complaints concerning business practices that violate privacy rights. Additionally, in conjunction with the National Consumer Law Center (NCLC), EPIC has filed numerous comments to the Federal Communications Commission (FCC) on matters involving illegal and unwanted robocalls and other phone-based scams.

[4] Since 1969, the nonprofit National Consumer Law Center (NCLC) has used its expertise in consumer law and energy policy to work for consumer justice and economic security for low-income and other disadvantaged people, including older adults, in the United States. NCLC's expertise includes policy analysis and advocacy; consumer law and energy publications; litigation; expert witness services, and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitive practices, help financially stressed families build and retain wealth, and advance economic fairness.

[5] NPRM at 26804, Q5 ("Do you support the proposal to add technical support services to the list of calls that do not qualify for the exemptions for calls in response to advertisements and direct mail solicitations in § 310.6(b)(5) and § 310.6(b)(6)? Should the Commission consider other modifications to the Rule to address tech support scams?").

[6] Complying with the Telemarketing Sales Rule, FTC, https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule [hereinafter "Complying with the TSR"].

I. The Commission should finalize the proposed rule with one modification, and additional clarifications included in the FTC's Business Guidance.

We recommend that the Commission expand the definition of "technical support service" in proposed 16 C.F.R. § 310.2(ff) to explicitly include *device components and software*, not merely the device that runs code itself, as well as *replacement and compensation programs*.

Additionally, we request the Commission to include four specific clarifications in the Business Guidance related to the TSR. These explanations will make the rule more comprehensive and protective:

- First, to explain that the definition of "any device on which code can be downloaded, installed, run, or otherwise used, such as a computer, smartphone, tablet, or smart home product" (in proposed § 310.2(ff)) is not limited to devices that currently use code, and the list of types of devices is illustrative and not exhaustive;

- Second, to explain that the exclusion for inbound calls relating to technical support in which the person providing the repair has physical possession of the device in § 310.2(ff), does not mean that calls from repair persons to consumers soliciting in-person repair services are excluded;

- Third, to state that the rule does not regulate free product updates that contain no upselling (assuming the Commission implements our proposed interpretive guidance on non-monetary consumer transactions, immediately below); and

- Fourth, to clarify that the rule covers situations in which consumers have provided something of value other than money—such as the collection of data—in return for goods and services.

II. The Commission should expand the definition of "technical support service" in its proposed 16 C.F.R. § 310.2(ff) to ensure that "device" includes all components of the device, as well as software programs, and compensation or replacement programs.

The Commission asks whether its definition of "technical support service" is overinclusive or underinclusive in any way.[7] We believe that the definition is underinclusive. We urge the Commission to expand the definition to include software programs used on devices[8] and to clarify that a "device" is inclusive of all its components (including hardware and firmware).[9] We note that the Commission included both software and hardware marketed to maintain a computer in its definition of "technical support product(s) or service(s)" in a consent order related to tech support

[7] NPRM at 26804, Q3. (Is the definition of "technical support service" appropriately tailored? Is it overinclusive or underinclusive in any way? How, if at all, should it be improved?).

[8] For example, Microsoft Edge or Facebook Messenger.

[9] Although firmware is a type of software, firmware is more closely associated with the essential functionality of a device than software programs or applications more generally. *See* "Firmware", Computer Security Resource Center, Nat'l Inst. for Standards and Tech, https://csrc.nist.gov/glossary/term/firmware.

scams that included TSR violations.[10] We also urge the Commission to include insurance, warranty, and other compensation and replacement programs pertaining to a covered device within the scope of "technical support service" in this rule amendment.

We recommend several specific additions to the proposed 16 C.F.R. § 310.2(ff):

1. The performance or security of software programs or applications should be included.

2. The language "performance or security of any device" should specifically include the performance and security of both hardware components and firmware used in conjunction with the device, even if the telemarketing offer does not make explicit reference to the device with which those components may be used.[11]

3. Offers for insurance, extended warranty, or similar plans for devices and software should fall within the scope of the Commission's "technical support service" amendment to the TSR because the purpose of this rule amendment is to protect consumers from tech support scams including worthless warranty programs.[12]

To accomplish this, we recommend the following bolded language should be added to proposed 16 C.F.R. § 310.2(ff):

> (ff) Technical Support Service means any plan, program, software, ~~or~~ service**, or insurance** that is marketed to repair, maintain, or improve the performance or security of any device on which code can be downloaded, installed, run, or otherwise used, such as a computer, smartphone, tablet, or smart home product, **and any software or application run on such a device, warranty offer, or any plan associated with replacing such a device. This includes device components such as hardware or firmware, even if the telemarketer makes no reference to the device through which the device components may be used.** Technical support service does not include any plan, program, software, or services in which

[10] *See* Stipulated Order, FTC v. In re NTS IT Care Inc., and Jagmeet Singh Virk, FTC File No. 1923116 | X200038, Case No. 4-20-cv-03388-PJH at 3 ¶ c (Dec. 4, 2020), https://www.ftc.gov/system/files/ftc_gov/pdf/nts_final_order.pdf (" 'Technical Support Product(s) or Service(s)' means any product, service, plan, program, software, or hardware marketed to clean, repair, or maintain a computer, or improve its performance or security, including antivirus programs, registry cleaners, and computer or software diagnostic, maintenance, cleaning, or repair services.").

[11] For example, a telemarketer reference to the performance of a laptop's battery rather than to the laptop itself or to the performance of an analog speaker rather than to the computer itself should not make the TSR's consumer protections inapplicable, even if the telemarketer does not refer to the specific device with which the battery or speaker (or any other hardware component) may be used. Some (but not all) components do include code executed by the host device (or execute code themselves). *See, e.g.*, "Firmware" note 9 *supra* ("[c]omputer programs and data stored in hardware"); HOWTO: Use GPU in Python, Ohio Supercomputer Center, https://www.osc.edu/resources/getting_started/howto/howto_use_gpu_in_python (last visited June 17, 2024).

[12] *See, e.g.*, Tech Support Scams, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/tech-support-scams ("Try to enroll you in a worthless computer maintenance or warranty program").

the person providing the repair, maintenance, or improvement obtains physical possession of the device being repaired.

III. The Commission should clarify several remaining issues in its TSR interpretive guidance.

In addition to adding language to the regulation itself, the Commission should also add several clarifying points to the TSR Business Guidance. The questions asked in this NPRM[13] indicate that there remain outstanding issues to be resolved. We recommend that these issues be addressed in the Business Guidance FAQs.[14]

a. Emphasizing capacity of equipment, not actual use.

The language in the proposed regulation indicates that it covers "any device on which code *can be* downloaded, installed, run, or otherwise used, *such as* a computer, smartphone, tablet, or smart home product" (emphasis added). This language means that the regulation is not limited to devices that *have or currently do* download, install, run, or otherwise use code (as evidenced by the Commission's use of "can be"). The language also indicates that the list of types of devices provided are not meant to be exhaustive (as evidenced by the "such as" language). It would helpful if the Commission explicitly addressed the open-ended nature of these terms by including something like the following in its FAQs:

> The Rule lists computers, smartphones, tablets, and smart home products as examples of devices subject to the inbound call exemption for technical support services, but this list is not exhaustive; other devices may meet the definition and fall within the scope of the TSR. Devices need not currently download, install, run, or otherwise use code to be subject to the inbound call exemption for technical support services—the mere capacity to do any of these things is sufficient to bring a device within the scope of the TSR's inbound call exemption.

b. Clarifying that outbound in-person calls are still subject to the TSR.

The Commission should also clarify in its FAQs that the modification of the TSR for "technical support service" only applies in the context of exemptions for *inbound calls*. In other words, the proposed rule does not change a business's obligations for *outbound calls* to consumers soliciting in-person repair services. As with our first suggested addition to the FTC's business guidance, this seems to be the only reasonable interpretation of the text of the Rule. However, things can get confusing when talking about exclusions from exemptions, and industry and consumers would likely both benefit from a clear articulation of how the modified rule would apply

---

[13] *See* NPRM at 26805, Q 2 (asking whether its definition of "technical support service" is clear and understandable); Q 4 (asking whether commenters support excluding in-person repair from the definition of technical support); Q 6 (asking whether the rule imposes burdens on technical support operations that do not engage in deceptive acts or practices); and Q 9 (asking whether the regulation will disproportionately burden original equipment manufacturers).

[14] *See* Complying with the TSR, note 6 *supra*.

and where it would not apply. The Commission might include something like the following in its FAQs:

> The Rule notes that its inbound call exemption for technical support service does not apply to in-person repair services. In-person repair services are still subject to the TSR's requirements for *outbound* calls. This means that a business would not have to issue TSR-required disclosures if a consumer calls about in-person repair services, but TSR disclosures would be necessary if the business initiated a call to a consumer about in-person repair services, if no other exemption applied (e.g., if the call was not part of a transaction that involves a face-to-face sales presentation).

c. Clarifying that inducing consumers to call about product updates or upgrades is not covered by the TSR if the updates are truly without cost.

The Commission should clarify that a company that is only encouraging its existing customers to reach out if they have questions about a software security update or a product recall is not affected by the proposed "technical support service" inbound call amendment, but remains outside the scope of the TSR. We stress however that this should be coupled with our recommended guidance about consumer data collection immediately below; as one example, if in exchange for a "product update" a company tricks customers into turning over their data so the company can resell it, that activity should not be considered exempt from the TSR's protections. The Commission might include something like the following in its Business Guidance:

> The Rule only pertains to telemarketing, which is defined as "a plan, program, or campaign…to induce the purchase of goods or services or a charitable contribution" involving more than one interstate telephone call. A call campaign encouraging consumers to reach out if they have questions about a software update would not be subject to the TSR if the campaign does not involve an attempt to upsell or otherwise induce a purchase of goods or services.

d. Clarifying that non-monetary transactions are covered by the TSR.

Finally, the Commission should clarify that a consumer who provides value in a form other than money in exchange for goods or services is protected by the amended rule. For example, a "free" software update that surreptitiously collects data about the user who chooses to download and install it is not truly without cost to the consumer. The primary purpose of the proposed regulation is to cover the subsequent transactions that occur when a consumer sees an ad about tech support service and calls the number provided.[15] Where the telemarketer or seller does not take cash from a consumer but instead takes data beyond

[15] The animating purpose of the TSR includes "to combat telemarketing fraud, giv[e] consumers added privacy protections and defenses against unscrupulous telemarketers, and hel[p] consumers tell the difference between fraudulent and legitimate telemarketing." *See* "Introduction", Complying with the TSR, https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#Introduction; U.S. Code Title 15, Chapter 87, Sec. 6101(2) https://www.govinfo.gov/content/pkg/USCODE-2022-title15/pdf/USCODE-2022-title15-chap87-sec6101.pdf ("Interstate telemarketing fraud has become a problem of such magnitude that the resources of the Federal Trade Commission are not sufficient to ensure adequate consumer protection from such fraud.").

the scope of what is strictly necessary to provide the consumer with the purchased goods or services the consumer is expecting, the company (or cyber-criminal) is receiving something of value from the servicing of the device or software. In part, the FTC's proposed rule amendment arises in response to precisely this kind of data collection.[16]

Many companies monetize the consumer data they collect, and collecting data from consumers in the context of a technical support services call could potentially be a more significant exchange of value than collecting money from the consumer.[17] It would be contrary to the goals of the TSR to exempt non-monetary transactions from consumers, especially when companies seek to extract all the monetary value they can from the consumer data they acquire.[18]

There is ample evidence that consumer data in the form of "telemarketing leads" are often sold and resold, and often to justify calls that would be otherwise illegal.[19] The commodification of other consumer data is also likely to be an unfair or deceptive act or practice in many circumstances.[20] However, in light of the Supreme Court's decision in *AMG Capital Management*, the articulation that specific activity is a violation of explicit

---

[16] *See, e.g.*, Tech Support Scams, note 12 *supra* ("Ask you to give them remote access to your computer — which lets them access all information stored on it, and on any network connected to it").

[17] *See, e.g.*, Kaitlyn Tiffany, Angry Birds and the end of privacy, Vox (May 14, 2019), https://www.vox.com/explainers/2019/5/7/18273355/angry-birds-phone-games-data-collection-candy-crush; FTC Cracks Down on Mass Data Collectors: A Closer Look at Avast, X-Mode, and InMarket (Mar. 4, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/03/ftc-cracks-down-mass-data-collectors-closer-look-avast-x-mode-inmarket (discussing antivirus software selling consumer data).

[18] *See, e.g.*, Justin Sherman, Examining data broker Equifax's relationships with millions of employers, Duke Sandford School of Public Policy (Aug. 24, 2022), https://techpolicy.sanford.duke.edu/blogroll/examining-data-broker-equifaxs-relationships-with-millions-of-employers/; Alfred Ng and Maddy Varner, The Little-Known Data Broker Industry Is Spending Big Bucks Lobbying Congress, The Markup (Apr. 1, 2021 08:00 ET), https://themarkup.org/privacy/2021/04/01/the-little-known-data-broker-industry-is-spending-big-bucks-lobbying-congress; R.J. Cross, How Mastercard sells its 'gold mine' of transaction data, U.S. PIRG Education Fund (Sept, 20, 2023), https://pirg.org/edfund/resources/how-mastercard-sells-data/; Timothy Morey, Theo Forbath, and Allison Schoop, Customer Data: Designing for Transparency and Trust, Harvard Business Review (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust; Mark Rolston, The free internet makes us the product—we need to stop it, The Next Web (Oct. 6, 2018 4:30pm), https://thenextweb.com/news/the-free-internet-makes-us-the-product-we-need-to-stop-it.

[19] *See, e.g.*, Comment of Responsible Enterprises Against Consumer Harassment, CG Dockets Nos. 21-402, 02-278, at 3 (May 9, 2023), *available at* https://www.fcc.gov/ecfs/document/10509951114134/1 (in the context of web forms: "once the consumer has submitted the consent form the company seeks to profit by reselling the "lead" multiple—perhaps hundreds—of times over a limitless period of time. Since express written consent does not expire, the website is free to sell the consent forever"); Privacy Enforcement Actions, State of California Dep't of Justice, Office of the Att'y Gen., https://oag.ca.gov/privacy/privacy-enforcement-actions ("The investigation found that DoorDash customer data was subsequently disclosed to businesses that were not participants of the marketing co-operatives, including to a data broker that re-sold the customer data many times over").

[20] To be clear, EPIC and NCLC do not endorse the commodification of consumer data.

regulations facilitates obtaining consumer redress.[21] As there is not currently an explicit rule prohibiting out-of-context secondary uses of data across all sectors,[22] and in the absence of a comprehensive federal privacy law, the Commission should implement consumer protections regarding any data collection subject to the TSR's rules.

We emphasize that where there is a TSR violation, it occurs prior to the point of sale. When considering traditional monetary purchases, the Commission does not wait for the telemarketer to spend the money it obtains before it can find a TSR violation; the violation occurs no later than the point of purchase (or at the moment the telemarketing call is made with deficient disclosures). Here too, the violation occurs at the point of collection (or sooner). This is an especially important point because companies try to evade disclosures by characterizing their conduct as something other than a "sale."[23] "Sharing" data, even with

---

[21] *See, e.g.*, NPRM at 26802, https://www.federalregister.gov/d/2024-07182/p-104 ("As a result [of the Supreme Court's decision in AMG Capital Management, LLC v. FTC], the Commission is now limited in its ability to obtain monetary relief from tech support scams whose business practices, in some cases, arguably place the scams beyond the reach of the Rule. Amending the Rule will clarify all tech support scams are potentially subject to the Rule.").

[22] *See, e.g.*, EPIC & Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, (Jan. 2022), https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/. There have been FTC enforcement actions from which a rule could be inferred. *See, e.g.*, Complaint for Permanent Injunction and Other Relief, FTC v. Kochava, Inc., 2:22-cv-00377-DCN, 9 (D. Idaho filed Aug. 29, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf ("information can be sold multiple times to companies that consumers have never heard of and never interacted with"); FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads (May 25, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads. This also has implications for data retention practices. *See, e.g.*, Complaint, In re Drizly, LLC, FTC File No. 2023185 at ¶ 13(f) (Oct. 24, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Complaint.pdf; Complaint, In re Chegg, Inc., FTC File No. 2023151 at ¶ 9(f) (Jan. 26, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/chegg.

[23] *See, e.g.*, Bennet Cyphers, Google Says It Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits It, Electronic Frontier Foundation (Mar. 19, 2020), https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and; Press Release, Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act (Aug. 24, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement (finding company engaged in "sale" of data under California Consumer Privacy Act even absent monetary compensation); Comments of EPIC and Public Knowledge to the Fed. Commc'ns Comm'n, In re Supporting Survivors of Domestic and Sexual Violence FNPRM WC Dkt. No. 22-238 at fn 27 (May 23, 2024), https://epic.org/documents/in-re-supporting-survivors-of-domestic-and-sexual-violence-fnprm/#_ftn27 (discussing discrepancy between Honda's letter to FCC Chairwoman Jessica Rosenworcel and the published results of Mozilla's investigation); Fed. Trade Comm'n, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* iii (2021), *available at* https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf ("three of the ISPs in our study reserved the right to share their subscribers' personal information with their parent companies and affiliates, which seems to undercut the promises not to sell personal information.").

subsidiaries and affiliates, is a data transfer for a commercial purpose and falls within the scope of the TSR. In many instances, the collection and transfer of this data is not consistent with the consumers expectations or even known to the consumer. We urge the Commission to build on the interpretive guidance it has already offered regarding subsidiaries and make explicit that sharing data could constitute a TSR violation.[24]

Additionally, even absent any intent by the caller or seller to monetize consumer data, repositories of consumer data accessed without authorization can exacerbate the risks of compromising consumer financial accounts or other sensitive data via fraud. Absent meaningful deterrence, companies are unlikely to invest in cybersecurity to safeguard this consumer data, placing it at heightened risk.[25] Commingling data among subsidiaries in particular, absent any purpose limitations, frustrates baseline security practices such as data mapping[26] and access controls.[27] There is also the obvious and more direct example of the fraudster not selling anything but using the tech support phone call to obtain valuable data from a consumer.[28] TSR enforcement can provide the deterrence necessary to promote the cybersecurity practices that more effectively safeguard this data, as well as to hold those who assist or facilitate the telemarketers and sellers accountable for the resulting consumer harm. The Commission might include something like the following in its Business Guidance:

> The Rule protects consumers from telemarketing fraud, and gives consumers added privacy protections and defenses against unscrupulous telemarketers. The rule also protects consumers from transactions which inappropriately access consumers' data when the transaction occurred over the phone. This occurs when more consumer data is collected than is strictly necessary to provide the goods or services expected by the consumer. These calls must include TSR-required disclosures, such as identifying the nature of the goods or services being offered, and other material information,[29] including the nature of the data collection.

---

[24] *See* "The Established Business Relationship Exemption", Complying with the TSR, https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#businessrelationship ("The test for whether a subsidiary or affiliate can claim an established business relationship with a sister company's customer is: would the customer expect to receive a call from such an entity, or would the customer feel such a call is inconsistent with having placed his or her number on the National Do Not Call Registry?").

[25] *See, e.g.*, Bruce Schneier, The Uber Hack Exposes More Than Failed Data Security, The New York Times (Sept. 26, 2022), https://www.nytimes.com/2022/09/26/opinion/uber-hack-data.html.

[26] *See, e.g.*, Comments of EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*, Federal Trade Commission 198-99 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf.

[27] *See id.* at 199-200.

[28] This also occurs in other contexts, for example utility scams. *See, e.g.*, Jérôme Segura, US residents targeted by utility scammers on Google, Malwarebytes Labs (June 4, 2024), https://www.malwarebytes.com/blog/scams/2024/06/utility-scams-update.

[29] *See* "Sellers and Telemarketers Must Disclose Material Information", Complying with the TSR, https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#materialinfo.

Conclusion

Thank you for considering these suggestions for strengthening the Telemarketing Sales Rule. We would be happy to discuss these and any other issues with you.

Respectfully submitted, this the 17th day of June 2024, by:

Chris Frascella, Counsel
Frascella@epic.org
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036

Margot Saunders, Senior Counsel
MSaunders@nclc.org
National Consumer Law Center
1001 Connecticut Ave, NW
Washington, DC 20036