



ROPE & GRAY LLP  
THREE EMBARCADERO CENTER  
SAN FRANCISCO, CA 94111-4006  
WWW.ROPEGRAY.COM

October 19, 2020

Melissa Bender  


**VIA ELECTRONIC SUBMISSION**

Vanessa A. Countryman  
Secretary  
Securities and Exchange Commission  
100 F Street, N.E.  
Washington, DC 20549-1090

Re: Proposed Rule 15 to Regulation S-T; Administration of the Electronic Data Gathering, Analysis, and Retrieval System; Rel. No. IC-33974; File Number S7-11-20

Dear Ms. Countryman:

Ropes & Gray LLP appreciates the opportunity to provide these comments to the Securities and Exchange Commission (the “Commission”) on the above-referenced matters.

Our firm represents the interests of many registered investment companies, asset management firms, and various other filers responsible for submitting forms and related documents via the EDGAR system. The proposed addition of 17 C.F.R. 232.15 (“Rule 15” or the “Rule”) to Regulation S-T is intended to promote the reliability and integrity of EDGAR by enabling the Commission to take certain corrective actions that will facilitate the administration of EDGAR and EDGAR submissions.<sup>1</sup> We are writing to provide our views on certain aspects of the proposed Rule 15.

As described in more detail below, we recommend that (i) consistent with modern expectations of privacy, as reflected in privacy regulations that have been adopted in the United States and abroad, the Commission should interpret the definition of “Sensitive PII” broadly, and (ii) the Commission should clarify that filers may request that the Commission redact or remove information from filings – including filings made prior to the effective date of the Rule – and that if the filer demonstrates that a filing contains Sensitive PII, the Commission must redact or remove information from the historical filing upon request.

---

<sup>1</sup> See Administration of the Electronic Data Gathering, Analysis, and Retrieval System, 85 Fed. Reg. 58018–23 (proposed Sep. 17, 2020) (“Proposing Release”) (to be codified at 17 C.F.R. Pt. 232).

1. PII within the meaning of Rule 15(a)(1) should be interpreted broadly.

We commend the inclusion of Section (a)(1) of Rule 15, which would enable the Commission to redact, remove, or prevent the dissemination of personally identifiable information (“PII”) that, if released, could result in financial or personal harm to an individual (“Sensitive PII”).<sup>2</sup> We encourage the Commission to interpret the definition of Sensitive PII broadly to reflect modern expectations of privacy and physical and financial security risks.

The Proposing Release does not specify which types of PII constitute “personally identifiable information that if released may result in financial or personal harm to an individual” for purposes of Rule 15, and the Commission notes that “Sensitive PII may comprise a single item of information (for example, a Social Security Number) or a combination of two or more items (for example, a full name and financial, medical, criminal, or employment history).”<sup>3</sup> The Proposing Release does refer to amendments made in 2018 to certain forms and schedules filed under the Securities Exchange Act of 1934, as amended, to eliminate certain provisions of such forms and schedules requesting sensitive PII of natural persons.<sup>4</sup> The 2018 Release contemplated removal of the following categories of Sensitive PII that were included in such forms and schedules: social security numbers, foreign identity numbers, dates of birth, and places of birth.<sup>5</sup> We would view the information referred to in the 2018 Release as the minimum of what should constitute “Sensitive PII” for purposes of Rule 15.

We respectfully submit that, to promote the integrity and reliability of EDGAR submissions, the Commission should interpret Sensitive PII as used in Rule 15 to include information such as bank account numbers and balance information, wire transfer instructions and related information (such as the sender or recipient’s name, phone number, address, bank name, etc.), and credit card numbers. Furthermore, for the purposes of Rule 15, we believe that sensitive or personally identifiable financial information should be considered broadly in light of the prominence of the internet, the ubiquity of online banking, and the increasing sophistication of financial criminals and bad actors who are able to use pieces of personal information as part of spear-phishing attacks designed to compromise corporate systems and divert funds. For example, we propose that sensitive or personally identifiable financial information should include (and thus Rule 15 should enable the Commission to redact or remove from EDGAR submissions) the following types of information, among others:

- Email addresses and mobile phone numbers, especially those linked to individuals’ bank account(s), trading account(s), or similar account(s);

---

<sup>2</sup> See Proposing Release at 58019, 58022.

<sup>3</sup> See *id.* at n.8.

<sup>4</sup> See Amendments to Forms and Schedules To Remove Provision of Certain Personally Identifiable Information, 83 Fed. Reg. 22190–93 (effective May 14, 2018) (the “2018 Release”) (codified at 17 C.F.R. Pt. 232, 17 C.F.R. Pt. 249).

<sup>5</sup> See *id.* at 22191.

- Physical addresses, especially when persons working or residing at that address are susceptible to theft or extortion, such as persons of public status, politically exposed persons, persons known to possess valuable bearer-type instruments or large amounts of cash, or persons related to such individuals;
- Login information for any bank account, trading account or similar account, such as the username, password, or security questions associated with the account; and
- Information associated with an individual’s digital asset accounts, such as the account or wallet address, any private or public key information, an associated email address or mobile phone number or the recovery phrase associated with a given account or wallet.

In the event any of the above information about an individual is misappropriated by bad actors, especially in conjunction with other PII about the individual such as their full name or physical address, there is a risk that the individual could suffer both personal and financial harm as a result, including “costs related to ongoing identity protection and monitoring, as well as reputational costs, operational costs, and losses from theft.”<sup>6</sup> For example, if the personal email address or physical home address of a trustee to the board of a registered investment company were inadvertently included in a submission and made publicly available through EDGAR, this information, combined with the individual’s known status as a trustee, would enable criminal third parties to locate, harass, and threaten the individual for financial gain or to use the information for identity theft, further financial fraud, or spear-phishing. Furthermore, there is no public or securities regulatory interest in having this information publicly available.

Similarly, in light of the nature of digital assets as bearer-like instruments, the methods by which digital assets are earned, stored and transferred, and the increased value of and market interest in digital assets in recent times, if information relating to individuals known to own a large amount of digital assets, such as their physical home or office address or an email address associated with their digital wallet, were inadvertently included in a submission and made publicly available through EDGAR, it would render those individuals susceptible to physical and financial security risks, including the coercive or criminal efforts of third parties. We note that there have been multiple documented instances of extortion and illegal seizure of both digital assets and the persons who own them.<sup>7</sup>

In our practice we have observed clear regulatory trends both in favor of (1) expanding the categories of information which are considered “sensitive” or “personal” and (2) facilitating safeguards for PII

---

<sup>6</sup> *See id.*

<sup>7</sup> *See e.g.*, Dante Disparte, *Crypto Crime Is Taking A Violent Turn* (Jan 28, 2019) (*available at* <https://www.forbes.com/sites/dantedisparte/2019/01/28/crypto-crime-is-taking-a-violent-turn/#5da7c20815a5>); Nathaniel Popper, *Bitcoin Thieves Threaten Real Violence for Virtual Currencies* (Feb. 18, 2018) (*available at* <https://www.nytimes.com/2018/02/18/technology/virtual-currency-extortion.html>).

generally. Emerging privacy regimes such as the California Consumer Privacy Act<sup>8</sup> (“CCPA”) and the General Data Protection Regulation<sup>9</sup> (“GDPR”) in Europe demonstrate that modern expectations of privacy are evolving in light of the increasingly global and technological nature of the investment industry and the business world at large. We note, for example, that both the CCPA and GDPR expressly consider email addresses to be a type of PII, and are in practice often interpreted to cover other types of information such as mobile phone numbers.

Because of the aforementioned risks, we believe the Commission should consider sensitive or personally identifiable financial information of this nature to be PII subject to redaction or removal under Rule 15(a)(1).

2. The Commission should clarify that filers may initiate a request for redaction or removal of information from a filing containing Sensitive PII and that the Commission shall redact or remove such information if the filer demonstrates that the submission contains Sensitive PII.

We appreciate that Rule 15 is not intended to “change filers’ obligations under the federal securities laws to ensure the accuracy and completeness of information in their EDGAR submissions,” and that the Commission “intend(s) to continue to rely upon filer corrective disclosure to remedy most submission errors”<sup>10</sup> even if Rule 15 is adopted, and we agree that the general onus of submission accuracy is with the EDGAR filers. However, we note that inclusion of Sensitive PII in historical EDGAR submissions (whether inadvertent or intentional) cannot be retroactively corrected by making an additional filer corrective disclosure. For example, if the social security number or home address of a member of the board of directors of a public company were inadvertently included in an exhibit to a proxy statement that was submitted to EDGAR, a subsequent corrective disclosure would not result in the removal of the original disclosure containing the Sensitive PII on EDGAR and therefore such Sensitive PII would remain publicly accessible.

We also note that the Rule does not specify whether the Commission and its staff will accept requests from filers to remove or redact Sensitive PII, and it does not necessarily require the Commission to remove or redact Sensitive PII even if a filer demonstrates that the release of that PII may result in

---

<sup>8</sup> See *California Consumer Privacy Act (CCPA)*, State of Cal. Dep’t of Justice, available at <https://oag.ca.gov/privacy/ccpa> (last visited September 23, 2020) (“Personal information is information that identifies, relates to, or could reasonably be linked with you or your household. For example, it could include your name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints, and inferences from other personal information that could create a profile about your preferences and characteristics.”).

<sup>9</sup> See *GDPR personal data – what information does this cover?*, available at <https://www.gdpreu.org/the-regulation/key-concepts/personal-data/> (last visited September 23, 2020) (“Personal data covers a much broader definition than the previous legislation demanded. While it includes the obvious personal information such as This [sic] includes credit card number, email address, name and date of birth, it also covers political opinions, race, gender and much more.”).

<sup>10</sup> See Proposing Release at 58019.

financial or personal harm to an individual. We respectfully submit that the Commission interpret Rule 15 to (i) allow filers to initiate a request for redaction or removal of a filing containing Sensitive PII, including any filings made prior to the effectiveness of the Rule, and (ii) require the Commission to redact or remove such information if the filer demonstrates that the submission contains Sensitive PII (*i.e.*, if the filer demonstrates that the PII, if released or allowed to remain publicly available, may result in financial or personal harm to an individual).

\* \* \* \* \*

Again, we thank you for the opportunity to provide these comments. We stand ready to provide additional comments or to answer any questions you may have.

Very truly yours,

  
Melissa C. Bender