March 31, 2023

Dear Commissioners:

I am an employee at the Securities and Exchange Commission and I write to express my grave concerns about the proposed requirement that SEC employees give a third-party service provider access to our financial accounts (hereinafter, "Third Party Access Requirement"), as written in the Proposed Rule regarding Supplemental Standards of Ethical Conduct for Members and Employees of the Securities and Exchange Commission (5 CFR Part 4401, Release No. 34-96768, File No. S7-02-2) (hereinafter, "Proposed Rule").

I urge the Commission to remove the Third Party Access Requirement because it (1) increases the cyber and operational risks to our financial accounts, (2) envisions the use of an unregulated entity that has no obligations to protect our data, (3) arbitrarily and capriciously conflicts with the spirit of other proposed SEC rules, (4) puts no limits on the scope of information being automatically reported to the Commission, (5) provides no indemnification in the event of theft or other cyber incident, (6) forces employees to agree to a new term of employment that was not previously bargained for, (7) constitutes a model of automatic reporting completely different from the industry standard, and (8) coerces employees to modify under duress the terms of their contract with their financial institutions.

Below, I address each of these points in further detail.

1. The Third Party Access Requirement Unduly Expands the Cyber and Operational Risks to Our Financial Accounts

In the cybersecurity community, it is commonly known that third party service providers add a significant level of risk to any organization using them. In an industry survey of cybersecurity professionals conducted in November 2022 regarding their experiences in the preceding 24 months, more than half of all respondents (57%) reported that their organizations were the victims of an IT security incident that originated from a third-party partner. *See* "Security Pros Say Third Parties Are Increasingly the Cause of Cybersecurity Incidents," SC Magazine, January 19, 2023, *available at* https://www.scmagazine.com/research-article/third-party-risk/security-pros-say-third-parties-are-increasingly-the-cause-of-cybersecurity-incidents. The financial sector, where SEC employees' financial accounts reside, is not immune from these grave threats. For that reason, the G7 recently published guidance for the financial sector to think proactively about this problematic source of risk. *See* G7 Fundamental Elements for Third Party Risk Management in the Financial Sector, *available at* https://www.ecb.europa.eu/paym/pol/shared/pdf/October_2022-G7-fundamental-elements-for-third-party-cyber-risk-management-in-the-financial-sector.en.pdf.

The Proposed Rule gives a designated Commission official the authority to require all employees to give a third party service provider access to our financial accounts. This requirement would significantly expand the cyber and operational risks to our financial accounts by giving another entity access to accounts where our financial assets are held. If that third party service provider is breached by hackers, our financial accounts could in turn be easily compromised.

This significant incursion into our private accounts confers no discernable benefit. We, the employees of the SEC, currently upload financial statements via the Annual Certification of Holdings process. The Commission is not receiving better information just because a third party service provider is doing the uploading.

2. The Third Party Access Requirement Envisions the Use of an Unregulated Entity that Has No Statutory or Regulatory Obligations to Protect SEC Employees' Private Data

My second point builds upon my first point. To the best of my knowledge, third party service providers are not directly regulated by the SEC or any other financial-sector agency. The only time that third party service providers may be subject to the jurisdiction of a financial-sector regulator is when the Federal Reserve determines that it is necessary and appropriate under the circumstances to invoke its broad exam authority to conduct an examination of a particular third party service provider. Aside from these limited instances, third party service providers fall outside the regulatory perimeter.

A cursory review of the SEC's own existing regulations on cyber and operational risks – applicable to the SEC's directly regulated entities – would yield some insights about the free rein enjoyed by third party service providers. Regulation S-P requires registered broker-dealers, investment companies, and investment advisers to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. Regulation S-ID requires registered broker-dealers, registered investment companies, and some registered investment advisers to establish a program that is designed to detect, prevent, and mitigate identity theft in connection with any accounts that are primarily used for personal, family, or household purposes. Regulation SCI, the most stringent of the Commission's cyber-risk regulations, applies to "SCI entities," a term which includes, among other things, stock and options exchanges, registered clearing agencies, FINRA and the MSRB, and alternative trading systems. The regulation requires SCI entities to take corrective action with respect to SCI events (defined to include systems disruptions, systems compliance issues, and systems intrusions), notify the Commission of such events, and disseminate information about certain SCI events to affected members or participants.

This constellation of requirements helps protect us customers and investors from having our most sensitive private data stolen. They are imposed by the SEC on its directly regulated entities. But since third party service providers fall outside the Commission's purview, they are not obligated by statute or regulation to do any of the above. We, the employees, are being instructed to use an entity that has no government oversight and has no statutory obligation to keep our data safe.

3. The Third Party Access Requirement Arbitrarily and Capriciously Conflicts with the Spirit of Other Recently Proposed SEC Rules Governing Cyber Risk

The requirement to use a third party service provider also runs counter to the SEC's recent pronouncements on the risks associated with these third parties. In October 2022, the Commission proposed a new rule to prohibit registered investment advisers from outsourcing

certain services and functions without conducting due diligence and monitoring of the service providers. In the proposal, the Commission cited the increased operational risk stemming from outsourcing as the motivation for proposing this rule. *See* Proposed Rule on Outsourcing by Investment Advisers, *available at* https://www.sec.gov/rules/proposed/2022/ia-6176.pdf. Then, in March 2023, the Commission just proposed a series of new cyber-related rules and rule changes, which also recognized the increased risks that stem from third party service providers. For example, in the proposing release to change Regulation S-P, the Commission stated: "These outsourcing relationships or activities may expose covered institutions and their customers to risk through the covered institutions' service providers, including risks related to system resiliency and the ability of a service provider to protect customer information and systems (including service provider incident response programs)." *See* Proposed Rule on Regulation S-P, *available at* https://www.sec.gov/rules/proposed/2023/34-97141.pdf.

If the Commission is so concerned about the cyber and operational risks that the general public is exposed to when a third party service provider is used, then the Commission should also be concerned for its own employees. We, too, are part of the investing public that the Commission is charged with protecting. If the Commission insists on enacting the Third Party Access Requirement, showing no regard for the operational risk associated with third parties, then such an enactment would call into question the legitimacy of the recent cyber-related proposals. Parties that wish to challenge those other regulations would have a solid argument that the Commission is engaged in the arbitrary and capricious interpretation of its statutes.

4. The Third Party Access Requirement Puts No Limits on the Scope of Information Being Automatically Reported to the Commission

The Proposed Rule also presents a number of practical concerns. It is broadly worded, such that a fair reading is that the third party would have access to all of the information in our financial accounts. I, like many investors, use a large brokerage firm that provides me with both a brokerage account and a check-writing cash management account. The two accounts are integrated, require only one log-in, and live on the same screen when I log into the platform. That means that the third party service provider would be able to view every single financial transaction in my life, including the checks I wrote to political candidates and the payments I made for medical procedures.

Since the Proposed Rule envisions no control on the part of the employee in what is automatically reported to the Commission, the employee would have no idea if and when the third party service provider makes mistakes and starts reporting non-securities transactions such as the ones mentioned above. When that happens, it would be an unprecedented invasion of privacy by a government agency and would be legally actionable.

5. The Third Party Access Requirement Provides No Indemnification in the Event of Theft or Other Cyber Incident

Expanding on the topic of practical concerns, I contend that the Proposed Rule also provides no recourse for the employee if his/her data or money is stolen by a cyber incident originated with the third party service provider. It is grossly unfair to ask the employee to bear all such risk on

his/her own. If the Commission provides no indemnification provision whatsoever, it is also an invitation for lawsuits in the future if something were to happen.

6. The Third Party Access Requirement Forces Employees To Agree To a New Term of Employment That Was Not Previously Bargained for

The unfairness discussed above is illustrative of a much broader issue. Current SEC employees were under no constructive notice that our privacy would be so severely affected. We do currently upload our financial statements for the Ethics Office to review. But during the upload process we have the ability to redact everything that we are not legally required to provide the Commission. That controlled dissemination of information is a far cry from giving a third party access to all our accounts and losing all semblance of control. The former is an expected provision of information consistent with general government ethical obligations; the latter, an invasion.

7. The Third Party Access Requirement Constitutes a Model of Automatic Reporting Completely Different From the Industry Standard

The Commission might counter that its proposed automatic reporting is a securities-industry standard, as explicated in the proposing release. This assertion is manifestly untrue. In the securities industry, brokers working for a financial institution are generally required to keep their personal trading accounts at that exact financial institution. When the financial institution conducts automatically reporting on the broker's personal trading activity, the institution is doing so on its own, in-house. This industry standard does not involve a third party service provider.

But even if the Commission's assertion is true, the argument advanced in the proposing release is still unconvincing. The Commission is not a financial institution. The Commission is part of the United States government and must therefore consider how the government ought to conduct itself. The private sector should not be the model for how the government behaves. The government is here to serve, not to reap a profit.

8. The Third Party Access Requirement Coerces Employees to Modify Under Duress the Terms of Their Contract With Their Financial Institutions

Further to the topic of how the government should behave, I would point out the significant litigation risk associated with coercing employees to modify the terms of their contract with their financial institutions. Our existing contracts envision our financial institution to be the guardian of our data and assets. The Commission's proposing release characterizes the third party as an innocuous interloper who is there just to obtain access and engage in automatic reporting. But as soon as another entity gains control of our financial accounts, that constitutes a modification of the contractual relationship between the financial institution and the customer. The customer is now being asked to deal with two institutions, not one.

Since we are being required to provide such access as a condition of our employment, a fair reading of this situation is that we are being coerced into modifying our contract with our

financial institution under conditions of duress. I would urge the Commission to further review the proposal from this angle. In my view, the proposal is invalid under principles of contract law.

For the reasons stated above, I urge the Commission to remove the Third Party Access Requirement from the Proposed Rule.

Sincerely,

SEC Employee