INVESTMENT COMPANY INSTITUTE®

Paul Schott Stevens, PRESIDENT AND CEO

1401 H Street, NW, Washington, DC 20005-2148, USA
202/326-5800 www.ici.org

202/326-5901 FAX: 202/326-5806
paul.stevens@ici.org

March 15, 2019

The Honorable Mike Crapo
Chairman
Committee on Banking, Housing
and Urban Affairs
United States Senate
Washington, DC 20510

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing
and Urban Affairs
United States Senate
Washington, DC 20510

Re: Feedback on Data Privacy, Protection and Collection

Dear Chairman Crapo and Ranking Member Brown:

On behalf of the Investment Company Institute,[1] I am pleased to submit this response to the Committee's February 13, 2019 release soliciting feedback from interested stakeholders on the collection, use, and protection of sensitive information by financial regulators and private companies. Cybersecurity and data protection are a top priority for the regulated fund industry. We thank the Committee for your leadership and interest in these important issues.

Companies of all types, including financial services companies, are collecting and using increasing amounts and types of data to operate and perform their business functions. This data can include an extensive range of business and proprietary information and numerous forms of nonpublic personal information ("NPPI"). The integrity, confidentiality and security of the NPPI held by financial companies, including ICI members, is exceptionally important to protect individuals from fraud, identity theft, and other criminal threats to their personal and financial security. The regular occurrence of high-profile data breaches highlights the vital importance of safeguarding the full array of such information. ICI member companies accordingly dedicate substantial resources to maintain effective information security programs. Informal estimates place our members' aggregate spending at well over a billion dollars annually to ensure the integrity of their networks.

[1] The Investment Company Institute (ICI) is the leading association representing regulated funds globally, including mutual funds, exchange-traded funds (ETFs), closed-end funds, and unit investment trusts (UITs) in the United States, and similar funds offered to investors in jurisdictions worldwide. ICI seeks to encourage adherence to high ethical standards, promote public understanding, and otherwise advance the interests of funds, their shareholders, directors, and advisers. ICI's members manage total assets of US$21.9 trillion in the United States, serving more than 100 million US shareholders, and US$6.6 trillion in assets in other jurisdictions. ICI carries out its international work through ICI Global, with offices in London, Hong Kong, and Washington, DC.

The critical importance of data security also has led the government to place increased demands on private companies. For the regulated funds industry, this has led to increased scrutiny of firms' data protection and security systems by the Securities and Exchange Commission (SEC). Indeed, cybersecurity has been one of the SEC's examination priorities for many years.[2] State laws also affect regulated funds and their data protection policies and procedures. Many states have rules mandating specific protocols if there is a breach, such as notification requirements. Some states also are considering ways to give individuals more control over their personal data.[3]

Government's focus on cybersecurity has been important to strengthening data protection protocols for the private sector. It is imperative, however, that close attention also be paid to the strength and effectiveness of government agencies' own information security programs. There have been serious high-profile breaches of numerous government systems, such as the recent EDGAR[4] breach at the SEC and the 2015 breach of the Office of Personnel Management (OPM).[5] The Government Accountability Office (GAO) has highlighted the need for government agencies to substantially improve their cyber incident detection, response and mitigation, and to better protect personally identifiable information.[6] With respect to the SEC, the GAO has raised concerns about information

---

[2] See *2019 Examination Priorities*, Office of Compliance Inspections and Examination, available at https://www.sec.gov/files/OCIE%202019%20Priorities.pdf; *OCIE Cybersecurity Initiative*, National Exam Program Risk Alert, Volume IV, Issue 2 (April 15, 2014), available at https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf; *Observations from Cybersecurity Examinations*, National Exam Program Risk Alert, Volume VI, Issue 5 (August 7, 2017), available at https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf. For a description of the SEC's Cyber Enforcement Actions, see https://www.sec.gov/spotlight/cybersecurity-enforcement-actions, in particular, the headings "Account Intrusions," "Hacking/Insider Trading," and "Safeguarding Customer Information." Also, more generally, see https://www.sec.gov/spotlight/cybersecurity.

[3] California enacted the California Consumer Privacy Act of 2018, to provide California consumers with the right (1) to know what personal information a business collects about them; (2) to know which of this personal information a business discloses for business purposes or sells; and (3) to opt out the sales of such information. Other states are considering similar legislation.

[4] The SEC operates the Electronic Data Gathering, Analysis and Retrieval system, known as "EDGAR." Publicly traded companies use EDGAR when submitting required documents to the SEC, and the public can search EDGAR to access these filings.

[5] See *Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident*, US Office of Personnel Management (September 23, 2015), available at https://www.opm.gov/news/releases/2015/09/cyber-statement-923/. See Section II below for a description of the 2015 EDGAR breach. See also, e.g., Alfred Ng, *Hackers Use College Student Loans Tools to Steal $30 Million*, CNET (April 17, 2017) available at https://www.cnet.com/news/hackers-used-college-student-loans-tool-to-steal-30-million/; Joe Uchill, *FDIC believes it was breached more than 50 times in 2015 and 2016*, The Hill (October 6, 2017), available at https://thehill.com/business-a-lobbying/354223-fdic-believes-it-was-breached-more-than-50-times-in-2015-and-2016.

[6] See *Cybersecurity: Actions Needed to Strengthen US Capabilities*, GAO Testimony Before the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, House of Representatives (GAO-17-440T) (February 14, 2017), available at https://www.gao.gov/assets/690/682756.pdf; *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, GAO Report to Congressional Committees (GAO-17-549) (September 2017), available at https://www.gao.gov/assets/690/687461.pdf.

security, and reports from the SEC's OIG likewise have highlighted the need for the SEC to strengthen its information security systems.[7] We are encouraged that the SEC has been working to strengthen cybersecurity within the agency,[8] as it is critically important to the industry and investors that the SEC succeed in its work to strengthen its information security program.

The crucial importance of securing the data held by financial regulators like the SEC cannot be overstated. Market sensitive data collected from across the regulated industry and aggregated in the network of a federal agency represents an inviting target and a single point of vulnerability. As described in more detail below, the SEC currently holds vast amounts of sensitive information and soon will require collection of yet more. This includes both information related to the operations and activities of firms the SEC regulates and information about their customers and clients. Federal law requires that our members collect both types of information, such as for specific reporting, record keeping, or ensuring compliance with anti-money laundering or "know your customer" requirements. Anyone who successfully gains unlawful access to SEC systems, whether from within or outside the agency, will have access to some of the most sensitive information that the SEC collects from SEC registrants and others subject to its jurisdiction. The EDGAR breach is only a small illustration of the substantial harm that could ensue for markets, investors and registrants from a breach or other unlawful access and use of the information held within SEC systems.

I. The SEC collects a large, and growing, amount of data related to securities holdings and transactions by funds and individuals

Since the financial crisis, the SEC has sought to improve the information that it collects from registrants and the markets to modernize and strengthen its monitoring and supervision of our financial markets. We describe below three areas in which the SEC has amplified the amount of data collected. First, the SEC's efforts have included increasing the information it collects when it conducts inspections of registrants, such as mutual fund complexes, as it increasingly employs technology and data analytics in conducting exams. Second, with the introduction of the new Form N-PORT, the SEC has expanded greatly the amount of portfolio holding information it collects from registered investment companies. Finally, implementation is underway on the creation of the SEC-mandated consolidated audit trail, which will warehouse all order and trade information for US exchange-listed equities and options, an immense amount of sensitive data.

---

[7] See *Information Security: SEC Improved Control of Financial Systems but Needs to Take Additional Actions* (GAO-17-469) (July 2017) , available at https://www.gao.gov/assets/690/686192.pdf; *Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014*, SEC OIG Report No. 552 (December 17, 2018), available at https://www.sec.gov/files/FY-2018-Independent-Eval-SEC-Implementation-of-the-FISMA-of-2014-Report-No-552.pdf.

[8] See Chairman Clayton's Public Statement on Cybersecurity, (September 20, 2017), available at https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20.

A. Data Collection by OCIE

The federal securities laws provide the SEC broad authority to conduct exams of SEC registrants, to ensure that they are in compliance with the federal securities laws. Last year, the SEC's Office of Compliance Inspections and Examination (OCIE) conducted more than 3,000 examinations and is responsible for overseeing more than 25,000 investment advisers, broker-dealers, mutual funds and exchange traded funds.[9] In the past, when OCIE conducted inspections, it typically visited a registrant and conducted a random sampling of records to assess a registrants' compliance with the federal securities laws. Today, OCIE's inspection process more often involves a collection of substantial amounts of nonpublic data, including NPPI. This is in part because the SEC has developed sophisticated electronic tools to analyze data for regulatory purposes,[10] including using technology and data analytics to identify high-risk exam candidates and potential regulatory concerns.[11]

When OCIE initiates an inspection of a registrant, the process typically begins with a document request that lists the various documents that OCIE wants electronically. In contrast to the past

---

[9] The mission of the National Exam Program (NEP) is to protect investors, ensure market integrity, and support responsible capital formation through risk-focused strategies that (1) improve compliance with Federal securities laws, (2) prevent fraud, (3) monitor risk, and (4) inform the SEC's regulatory policy. For a description of the current focus of OCIE's exams, see *2019 Examination Priorities* at footnote 2, *supra*.

[10] For example, one tool used by OCIE is the National Exam Analytics Tool (NEAT) developed by a team of OCIE financial engineers to facilitate the analysis of trading blotters. The NEAT and OCIE's use of data is described in its *2018 National Exam Program Examination Priorities*, Office of Compliance Inspections and Examinations, available at https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2018.pdf (Also noting "Our sophistication in using data analytics…is ever growing.") Generally, SEC has not disclosed specific details regarding the analytical tools it has developed. However, the sophistication of its tools is demonstrated by one that the SEC has made public—its Markets Data Analytics System, or MIDAS. According to SEC's MIDAS webpage, "***Every day MIDAS collects about 1 billion records*** from the proprietary feeds of each of the 13 national equity exchanges time-stamped to the microsecond. MIDAS allows us to ***readily perform analyses*** of thousands of stocks and over periods of six months or even a year, ***involving 100 billion records at a time.***" (emphasis added). See https://www.sec.gov/marketstructure/midas.html#.XH5-RIhKiUk.

[11] A 2015 speech by the SEC's Chief of Staff, Andrew Donohue, discussed OCIE's mining of "large amounts of data" to assess registrants' compliance:

> OCIE's Risk Analysis Examination Group is continuing to leverage technology in exams of clearing firms and large broker-dealers by analyzing transactions cleared by selected firms over a period of years and then using that data to identify potential problematic behavior across multiple firms, including unsuitable recommendations, misrepresentations, inadequate supervision, churning, and reverse churning.
>
> SEC examiners also are mining large amounts of data to assess how large firms have implemented their compliance programs. …

See *Remarks at NRS 30th Annual Investment Adviser and Broker-Dealer Compliance Conference,* Andrew J. Donohue, Chief of Staff (October 14, 2015), available at: https://www.sec.gov/news/speech/donohue-nrs-30th-annual.html.

approach of sampling such materials, document requests now typically seek complete files.[12] As a result, over time, OCIE's requests have become extraordinarily broad.[13]

For example, we understand that OCIE, in a recent exam of a major industry transfer agent, requested literally *all* shareholder data, including NPPI, held on the transfer agent's system. How vast a collection of NPPI this represented cannot be overstated. In another recent exam involving an investment adviser, OCIE's document request sought production of a variety of client information for various types of adviser accounts. Information requested included: the client's name, address, date of birth, risk tolerance level, net worth, income, account number, type of account (e.g., IRA, 401(k), trust), market value of the account, and the names of certain people associated with the account (e.g., account custodian, person who solicited or otherwise helped to obtain the client).[14] As mentioned above, these requests require the registrant to provide this information to OCIE electronically so OCIE has a copy of it in their database.[15] Needless to say, investors are likely wholly unaware that this very personal and nonpublic information about them may reside in the SEC's files. From an information security perspective, the amount and sensitivity of data the SEC holds on registrants' clients and investors should not be underestimated.

The data obtained by OCIE during an exam is collected on an *ad hoc* basis by examiners in the field. Of genuine concern to our members is that the safety and security of this data depends, in large part, on the care taken by individual SEC examiners and staff members who obtain or have access to this data.[16] While OCIE has established policies and procedures for examinations, there is little information available to the public about how the SEC secures and protects the information it

---

[12] See the SEC's "Data Delivery Standards," which are available at: https://www.sec.gov/divisions/enforce/datadeliverystandards.pdf.

[13] We understand that, in conducting reviews of mutual fund complexes, OCIE's information requests often consists of several pages listing the documents OCIE wants produced. These documents typically consist of detailed non-public and often sensitive information relating to the fund's adviser, transfer agent, principal underwriter, fund administrator, and custodian.

[14] This information was only one portion of a much longer information request list.

[15] When registrants have asked OCIE staff if they can redact certain elements of this NPPI to better protect the confidentiality of shareholders' information, they have been told that they must provide OCIE the information in the same form that the registrant maintains it in their records.

[16] It is not uncommon for examiners to utilize SEC-issued laptops in conducting exams. In 2008, the SEC's OIG issued a report finding "effective accountability of laptop computers [at the SEC] simply did not exist." See *Control Over Laptops*, SEC Office of Inspector General (Inspection Report No. 441, March 31, 2008), which is available at https://www.sec.gov/about/oig/audit/2008/ir441.pdf. In 2014, the OIG did a follow up review of the SEC's inventory of laptop computers and found "we questioned the reliability of the SEC's IT inventory and estimated that it may reflect incorrect information for over 1,000 laptops. Furthermore, we estimated that as many as 2,002 laptops assigned to the locations we reviewed may be unaccounted for. By not ensuring that inventory records are accurate and that all laptops are accounted for, the SEC is not consistently safeguarding sensitive assets and may be unaware of lost or stolen laptops." See *Controls Over the SEC's Inventory of Laptop Computers*, SEC Office of Inspector General (Inspection Report No. 524, September 22, 2014), which is available at https://www.sec.gov/files/524.pdf.

collects, who within the SEC has access to the data, and when and how such information is securely purged from SEC systems. Cybersecurity has been one of OCIE's examination priorities for many years, and, as OCIE describes, those examination "have and will continue to focus on, among other things, governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response."[17] We would hope that OCIE would apply the same standards to itself regarding protection of all of the data it has collected from registrants during the examination process. There is, however, no information available to the public to this effect. OCIE should provide a level of transparency regarding its policies and procedures on data protection equal to that it demands of regulated entities, providing registrants appropriate assurances of confidentiality when they are required to share this sensitive data.

It bears emphasizing that we strongly support an effective inspection and examination program at the SEC. This is very much in the interest of shareholders, funds, and fund advisers. We also fully appreciate the SEC's need to collect and analyze certain data for these purposes. Our concerns relate instead to the ever-increasing amount and type of data collected by OCIE and the SEC's ability to protect this data. A breach of the SEC's systems – not unlike the EDGAR breach – could result in serious harm, potentially exposing the NPPI of millions of fund shareholders, as well as proprietary information relating to fund management. Such a breach might even go unreported as the SEC would have no legal duty to provide public notice of it.

B. Expanded Fund Reporting on Form N-PORT

In 2016, the SEC adopted sweeping rules to expand the information that it collects from registered investment companies. The SEC stated that its new rules would assist it in fulfilling its mission to protect investors, maintain fair, orderly and efficient markets and facilitate capital formation.[18] Under the SEC's rules, regulated funds must collect and report on Form N-PORT detailed monthly portfolio holdings information and other proprietary and sensitive information (e.g., portfolio-level and position-level risk metrics, securities lending activities, and "miscellaneous securities" holdings that typically are not disclosed in filings).[19] Some of the portfolio holding information will be available to the public while some information will be nonpublic and held only by the SEC. With N-PORT, the SEC will have a large, unique repository of data about fund investments, both fund by fund and the industry as a whole. ICI has shared its concerns that unauthorized access to this data

[17] *2018 National Exam Program Examination Priorities*, Office of Compliance Inspections and Examination, available at https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2018.pdf; also see 2019 Examination Priorities, supra at footnote 2.

[18] Investment Company Reporting Modernization, Investment Company Act Release No. 32314 (Oct. 13, 2016) [81 FR 81870 (Nov. 18, 2016)], available at https://www.sec.gov/rules/final/2016/33-10231.pdf.

[19] The new Form N-PORT replaces Form N-Q, on which funds currently are required to report their complete portfolio holdings to the SEC for the first and third fiscal quarters. In addition to requiring more frequent reporting, Form N-PORT requires additional information concerning fund portfolio holdings that is not currently required under Form N-Q in a structured data format. This includes detailed information about a fund's assets and liabilities (including borrowings), return information, and investment flows.

could expose funds and their investors to predatory trading practices, including front-running of fund trades, "free riding" of fund investment research, and reverse engineering or "copycatting" of fund investment strategies.

To its great credit, the SEC has taken significant steps since adopting these rules to address such concerns. In 2017, the SEC delayed by nine months the requirement to file Form N-PORT, to allow time for improvements to the "functionality and security" of the SEC's EDGAR filing system.[20] Most recently, in late February of this year, the SEC made critical changes to the submission schedule for this new form to address concerns about the sensitivity of the data.[21] Funds would have been required to file nonpublic monthly reports within 30 days after the end of each month. Under the modified schedule, funds instead must maintain the relevant information in their records (available to the SEC upon request), and file all three monthly reports with the SEC no later than 60 days after the end of each fiscal quarter. The time lag, up to 120 days for some of the data, meaningfully attenuates the market sensitivity of this data. As was the case previously, only the third monthly report of each quarter will be publicly available upon filing (other than certain excepted data items which will be nonpublic).

In announcing this change, the SEC stated that it had reviewed the risks and its need for the data and determined that allowing funds to report monthly data on a more delayed basis would reduce its potential cybersecurity risks, decreasing the sensitivity of the information collected, while still allowing the SEC to fulfil its mission. This delay in reporting will allay substantially the security risks posed by the original rule, a step that ICI greatly applauds.[22]

C. Consolidated Audit Trail

A third category of increased and new data collection required by the SEC is the consolidated audit trail (CAT). Unlike the two categories of information described above, information in the CAT is not held by the SEC, nor under the direct control of the SEC; however, SEC staff will have access to the CAT and has authority to mandate enhanced information security protections for CAT data (if it deems appropriate).[23]

---

[20] Investment Company Reporting Modernization, Securities Act Release No. 10442 (Dec. 8, 2017) [82 FR 58731 (Dec. 14, 2017)], available at https://www.sec.gov/news/press-release/2017-226.

[21] See SEC Press Release (February 27, 2019), available at https://www.sec.gov/news/press-release/2019-23.

[22] While it is a very considerable improvement, this change does not completely eliminate the security risk posed by the information available from N-PORT filings. The EDGAR system will still retain an extensive repository of sensitive non-public information from registered investment companies on the Form N-PORT, including the holdings reported for the first two months of each quarter, as well as certain data that will remain nonpublic (e.g., position-level risk metrics, and the reporting of each investment's country of risk and economic exposure).

[23] The SEC can also amend Rule 613 of Regulation National Market System (NMS), which mandates creation of the CAT and lists specified requirements that the CAT must meet, including details of the data elements to be collected, the timing of data transmissions, and specific standards for data formatting.

In response to volatile trading in the equity markets in 2010, the SEC approved a rule mandating the creation of a CAT to warehouse all order and trade information for US exchange-listed equities and options. The SEC explained CAT would "increase the data available to regulators investigating illegal activities such as insider trading and market manipulation, and it will significantly improve the ability to reconstruct broad-based market events in an accurate and timely manner."[24]

Rather than operating the CAT directly, the SEC directed the self-regulatory organizations (SROs)(i.e., the exchanges and FINRA) to create a national market system plan to govern and operate the CAT. When fully implemented, SROs and their members (i.e., broker-dealers) will be required to submit to the CAT extensive trade and order information, including data concerning an order's origination, routing, modification/cancellation, and execution.[25]

The CAT's central repository will contain an immense trove of information about the US equity and options markets strategies of all market participants. Further, because CAT data will be reported at the customer level and close to real time, any data breach risks exposing many thousands of funds and other investors to predatory trading practices, potentially causing great damage to public confidence in our capital markets. Unquestionably, CAT data will have tremendous commercial value. Cyber criminals will exert every effort to access and use such data for their personal gain, at the expense of all legitimate investors, including funds and their shareholders.

The CAT project was launched well before he came to the SEC, and Chairman Clayton to his credit has expressed concern regarding the security of the data the CAT will hold. In particular, he has cited the need to protect investors' personal information that will be stored in the CAT.[26] Protection of NPPI is imperative, but the CAT poses additional concerns. NPPI would constitute only a small portion of the most valuable data held by the CAT. A cybercriminal likely would profit more by exploiting live trading strategies of institutional investors, including registered funds. To this end, ICI has provided suggestions to the SEC regarding its governance of the CAT and the protection of the data.[27] We also have offered the expertise of mutual fund chief information security officers to representatives of the SROs who are formulating the CAT's information security policies.

---

[24] See SEC Press Release (July 11, 2012), available at https://www.sec.gov/news/press-release/2012-2012-134htm.

[25] "When fully complete, the CAT will ingest in excess of 58 billion records per day to be the world's largest data repository of information on securities transactions, tracking all orders throughout their life cycle." CAT NMS News Release (February 27, 2019), available at https://www.catnmsplan.com/wp-content/uploads/2019/02/CAT_FINRA_Press_Release_FINAL.pdf.

[26] See Chairman Jay Clayton's testimony on "Oversight of the U.S. Securities and Exchange Commission" before the Senate Committee on Banking, Housing and Urban Affairs (December 11, 2018) available at https://www.sec.gov/news/testimony/testimony-oversight-us-securities-and-exchange-commission-0.

[27] ICI staff recently met with the SEC to discuss our concerns, namely that SEC should address the serious information security concerns that market participants have with this data collection and should remedy the seriously flawed governance model of the CAT. We previously described our concerns in a comment letter on the proposed NMS plan to implement the CAT. See letter from David W. Blass to Brent J. Fields, Secretary, U.S. Securities and Exchange Commission (July 18, 2016), available at https://www.ici.org/pdf/30042.pdf.

Reporting under the plan was scheduled to phase-in beginning in November 2017, but implementation has been delayed for various reasons, including questions about the information security program protecting CAT data. Presently, exchanges are reporting to the CAT, but broker-dealers are not.

As stated above, we fully appreciate that the SEC benefits from access to this type of data to better carry out its mission. Nonetheless, the sheer volume of data that the SEC now collects (or directs the collection of), has increased exponentially—and with it both the information security of the agency and the adverse consequences of a security breach.

II. Government assessments of information security and breaches of government systems highlight the importance of regulators' focus on safeguarding information

Both the GAO and the SEC's OIG have reported on deficiencies within the SEC information security program.[28] In their most recent reports, both found that, although the SEC has made improvements, these deficiencies continue to put financial data at risk.[29]

The security risks associated with data held by the SEC are illustrated by the 2016 breach of the SEC's EDGAR system when a hacker gained access to nonpublic information which he sold to others who used it to profitably trade securities. The SEC did not detect the breach for approximately five months and then did not publicly disclose the breach for an additional year. In 2016, the hacker launched several concurrent efforts to penetrate EDGAR and successfully infected several SEC computer workstations.[30] The hacker then gained access to test filings, which companies using the EDGAR system may submit prior to submitting their required filings. As the SEC explains, "[t]est filings are draft versions of EDGAR filings that are meant to ensure that an EDGAR filing is in the

---

[28] The GAO was expressing concern with the "significant deficiencies" in the SEC's information security controls as early as 2007. See Financial Audit, Securities and Exchange Commission's Financial Statements for Fiscal Years 2007 and 2006 (GAO-08-167) (Nov. 2007) at pp.10-11. In the intervening years, GAO has repeatedly cited the SEC for its lax security controls. For examples of OIG reports, see footnotes 7 and 15 *supra*, and footnote 31 *infra*.

[29] See "Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014," US SEC Office of Inspector General Office of Audits (December 17, 2018) available at https://www.sec.gov/files/FY-2018-Independent-Eval-SEC-Implementation-of-the-FISMA-of-2014-Report-No-552.pdf (the independent auditor found that the SEC's information security program did not meet the FY 2018 IG FISMA Reporting Metrics' definition of "effective" because the program's overall maturity did not reach Level 4: Managed and Measurable); Information Security: SEC Improved Control of Financial Systems but Needs to Take Additional Actions," US Government Accountability Office (July 2017), available at https://www.gao.gov/assets/690/686192.pdf (GAO concluded that "[i]nformation security control deficiencies in the SEC computing environment may jeopardize the confidentiality, integrity, and availability of information residing in and processed by its systems. ...Until SEC mitigates its control deficiencies, its financial and support systems and the information they contain will continue to be at unnecessary risk of compromise.").

[30] The hackers apparently induced SEC computer users to open documents containing malware that was sent via spoofed, phishing emails that falsely represented that they had been sent by SEC security personnel.

correct format, free from errors, and will be accepted for filing by EDGAR."[31] Upon successfully gaining access, the hacker was able to deploy a program to surreptitiously poach the test filings on an automated basis, to achieve greater scale. The hacker provided the information to traders, who were able to use the nonpublic information to place profitable trades. The profits from this activity exceeded $4.1 million.

Approximately five months after the initial breach, the SEC's IT personnel detected an attack on the system and patched the EDGAR software, preventing the hacker from gaining any additional test filings. The SEC believes the intrusion did not result in unauthorized access to NPPI, jeopardize the operations of the SEC, or result in systemic risk to US markets.

Upon learning of the hacking, Chairman Clayton immediately commenced an internal investigation of the incident. In 2019, civil and criminal actions were brought against the hackers.[32] According to the OIG's report of this incident, the OIG determined that "between fiscal years 2015 and 2017, the EDGAR system lacked adequate governance commensurate with the system's importance to the SEC's mission." It also determined that "certain preventive controls either did not exist or operate as designed" and "the SEC lacked an effective incident handling process." As a result, "[t]hese weaknesses potentially increased the risk of EDGAR security incidents and impeded the SEC's response efforts."[33] The OIG noted that, since the incident, the SEC has "strengthened EDGAR's system security posture, including the handling of and response to vulnerabilities." We commend the Chairman for hardening EDGAR's security defenses, and we support his efforts to take other steps as required.

---

[31] See the SEC's complaint in footnote 32, infra.

[32] See *U.S. Securities and Exchange Commission v. Oleksandr Ieremenko, et al.,* District of New Jersey, Civil Action No. 19-cv-505, (January 15, 2019) (the "Complaint"), which is available at: https://www.sec.gov/litigation/complaints/2019/comp-pr2019-1.pdf. The press release the SEC issued about this action is available at: https://www.sec.gov/news/press-release/2019-1. Two of the Defendants in the SEC's civil case were also criminally charged for their conduct according to an indictment in the U.S. District Court for the District of New Jersey that was unsealed January 14, 2019. The indictment in this case, U.S. v. Artem Radchenko and Oleksandr Ieremenko is available at: https://www.justice.gov/usao-nj/press-release/file/1124251/download.

[33] See *Evaluation of the EDGAR System's Governance and Incident Handling Processes,* SEC OIG Report No. 550 (Sept. 21, 2018). The executive summary is available at https://www.sec.gov/files/Eval-of-the-EDGAR-Systems-Governance-and-Incident-Handling-Processes.pdf. While the OIG did not issue its full report publicly because it contained sensitive information about the SEC's information security program, the public portion of the report notes that the OIG "made 14 recommendations to improve the SEC's EDGAR system governance, security practices, and incident handling processes." It "also noted that *open recommendations from prior OIG work* should address some of [OIG's] observations..." [Emphasis added.]

III. Improving safekeeping of data SEC holds or requires

Both the GAO and the SEC's OIG periodically assess the security of the SEC's information systems, including the SEC's compliance with FISMA.[34] For years, both the GAO and the SEC's OIG have highlighted concerns regarding the SEC's information security and have provided specific recommendations to address those concerns. As described above, recent reports from the GAO and the OIG note that the SEC has made improvements but has not implemented all their prior recommendations.

The SEC is to be commended for its increased focus on cyber concerns (including the recent appointment of the SEC's first Chief Risk Officer).[35] Hopefully, future GAO and OIG reviews will find that any remaining deficiencies have been corrected.

More generally, however, we would urge the SEC and this Committee to consider four basic principles as it considers the government's own information security practices. We outline them in the text below.

A. Recognize security risks and safeguard data on hand

While Chairman Clayton has described his commitment to continue to prioritize efforts to promote effective cybersecurity practices within the SEC, it is vital that all SEC staff be cognizant of the risk of the data they hold, including not just NPPI, but also nonpublic corporate information and information on markets and trading. All SEC staff must be held accountable for the protection of the data they hold.

B. Only collect necessary data

As Chairman Clayton recently explained last year to this Committee, the SEC acted to eliminate the collection of Social Security numbers and dates of birth on a number of EDGAR forms where the SEC concluded that the information was not necessary to its mission.[36] We applaud this action and encourage the SEC to apply this concept more broadly. For example, in OCIE's document requests, OCIE should consider whether it could carry out its mission with less data (e.g., request a sample

---

[34] In 2014, Congress enacted the Federal Information Security Modernization Act of 2014 (FISMA) (Public Law 113-283), which "provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets and a mechanism for oversight of Federal information security programs." FISMA also requires agencies to develop, document, and implement an agency-wide information security program to provide information security for the data and information systems that support the operations and assets of the agency. FISMA requires Inspectors General to annually assess the effectiveness of agency information security programs and practices and to report the results to OMB and DHS.

[35] On February 28, the SEC announced the appointment of its first Chief Risk Officer "to strengthen the agency's risk management and cybersecurity efforts." See SEC Press Release: https://www.sec.gov/news/press-release/2019-24.

[36] See Chairman Jay Clayton's December 11, 2018 testimony, *supra* at footnote 26.

rather than all available data). In addition to collecting only data that is absolutely necessary, SEC staff should consider whether there are circumstances in which information can be redacted or anonymized. Further, they should promptly destroy data and information once it is no longer needed.

C. Duty to report and notify public of breach

While we generally applauded the SEC's handling of the EDGAR breach, there is one aspect of the SEC's response that was of concern—the fact that the breach was not publicly acknowledged by the SEC until September 2017. This is almost a year after SEC IT staff detected the breach. In Chairman Clayton's September 2017 announcement, he explained that "[i]n August 2017, the Commission learned that an incident previously detected in 2016 may have provided the basis for illicit gain through trading." Private companies have been severely criticized for delays in reporting breaches to the public and we do not see any reason why government agencies like the SEC should not be held to the same standard. When a breach has occurred, whether the breach relates to a government agency or a private sector company, the public should be notified as promptly as possible so that markets, firms and individuals can take remedial steps.

D. SEC needs adequate resources

While additional funding alone will not solve the cybersecurity issues at the SEC, we acknowledge that attention to the SEC's cybersecurity and data protection absolutely requires enhanced investment—both in time and resources. ICI recently submitted letters to the Senate and House Committees on Appropriations (attached) to "support robust funding for the [SEC] for fiscal year 2020 and, in particular, increased funds to support the Commission's critical cybersecurity and data protection responsibilities." As we reference in our letter, the SEC recently appointed its first Chief Risk Officer (CRO), whose cybersecurity efforts deserve, indeed demand, adequate funding. Additional SEC efforts and resources will be needed to make further improvements to the agency's information security environment, including its EDGAR filing system.

* * * * *

Thank you for your consideration of our submission and for your attention to these vitally important issues. We look forward to working with you and the Committee as your examination moves forward.

With kindest regards.

Sincerely,

Paul Schott Stevens
President and CEO
Investment Company Institute

INVESTMENT COMPANY INSTITUTE®

Paul Schott Stevens, PRESIDENT AND CEO

1401 H Street, NW, Washington, DC 20005-2148, USA
202/326-5800 www.ici.org

202/326-5901 FAX: 202/326-5806
paul.stevens@ici.org

March 7, 2019

The Honorable Richard Shelby
Chairman
Committee on Appropriations
United States Senate
Washington, DC 20510

The Honorable Patrick Leahy
Vice Chairman
Committee on Appropriations
United States Senate
Washington, DC 20510

The Honorable John Kennedy
Chairman
Subcommittee on Financial Services
and General Government
United States Senate
Washington, DC 20510

The Honorable Christopher Coons
Ranking Member
Subcommittee on Financial Services
and General Government
United States Senate
Washington, DC 20510

Re: Importance of Robust FY2020 Funding for the Securities and Exchange Commission

Dear Chairman Shelby, Vice Chairman Leahy, Chairman Kennedy, and Ranking Member Coons:

On behalf of the Investment Company Institute,[1] I am writing to support robust funding for the Securities and Exchange Commission (SEC) for fiscal year 2020 and, in particular, increased funds to support the Commission's critical cybersecurity and data protection responsibilities. ICI represents the interests of regulated funds, which manage total assets of $21.9 trillion on behalf of more than 100 million Americans seeking to save for college, retirement, and other important financial goals. A well-funded and effective SEC is essential to the continued success of regulated funds and their investors.

Regulated funds play an important role not only in the lives of individual investors but in our nation's financial system. They are major participants in US capital markets, which are widely viewed as being the fairest, most efficient, and most competitive in the world. Regulated funds contribute to overall US economic growth by channeling and allocating investors' capital to businesses of all kinds,

[1] The Investment Company Institute (ICI) is the leading association representing regulated funds globally, including mutual funds, exchange-traded funds (ETFs), closed-end funds, and unit investment trusts (UITs) in the United States, and similar funds offered to investors in jurisdictions worldwide. ICI seeks to encourage adherence to high ethical standards, promote public understanding, and otherwise advance the interests of funds, their shareholders, directors, and advisers. ICI's members manage total assets of US$21.9 trillion in the United States, serving more than 100 million US shareholders, and US$6.6 trillion in assets in other jurisdictions. ICI carries out its international work through ICI Global, with offices in London, Hong Kong, and Washington, DC.

helping to finance their operations, research and development, innovation, and growth in employment.[2]

Our industry views regulation as a necessary component for building and sustaining the confidence of regulated fund investors. Regulated funds have prospered for close to 80 years under a robust framework of laws and regulations administered by the SEC under the Investment Company Act of 1940 and other federal securities laws.

Under the capable leadership of Chairman Jay Clayton, the SEC has put forth a strategic plan for 2018-2022 that outlines three goals intended to guide the agency's work: (1) attention to the interests of long-term "Main Street" investors; (2) a continual focus on changes in the securities markets and how the agency's regulation and oversight must adapt; and (3) a commitment to "elevating the agency's performance through technology, data analytics and human capital."[3] By holding itself to these goals, the SEC will be well positioned to utilize the resources it receives from Congress to maximum effect.

The SEC's current regulatory and policy agenda includes a range of initiatives that are of considerable import to the regulated fund industry, but of all the initiatives on the SEC's agenda, one stands out as a top priority for both the agency and the regulated fund industry: cybersecurity and data protection.[4] Indeed, this initiative reflects all three of the goals outlined in the SEC's strategic plan.

ICI and its members commend Chairman Clayton for his commitment to enhancing the SEC's practices relating to cybersecurity and data protection.[5] Under Chairman Clayton's leadership, the SEC has demonstrated that commitment, continuously evaluating its data security protocols in light of its regulatory program. A recent example is the SEC's action to allow mutual funds to report monthly portfolio holdings information at quarter's end, thereby reducing the sensitivity of the information collected by the Commission.[6] This was a much-needed step that ICI and its members strongly support.

Attention to the Commission's cybersecurity and data protection needs requires significant investment—both in time and resources. The SEC recently appointed its first Chief Risk Officer

---

[2] Statement of Paul Schott Stevens, President & CEO, ICI before the Committee on Financial Services, US House of Representatives, on Empowering a Pro-Growth Economy by Cutting Taxes and Regulatory Red Tape (June 20, 2018); *see also* Statement of Jay Clayton, Chairman, SEC before the Committee on Banking, Housing and Urban Affairs, US Senate, on Oversight of the US Securities and Exchange Commission (Dec. 11, 2018) ("Clayton Testimony").

[3] *See, e.g.,* Clayton Testimony.

[4] *Id.*

[5] *See, e.g.*, Jay Clayton, Chairman, SEC, Public Statement on Cybersecurity (Sept. 20, 2017), available at https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20.

[6] *See SEC Modifies Timing for Filing Non-Public Form N-PORT Data to Align With its Approach to Data Management and Cybersecurity* (press release, Feb. 27, 2019), available at https://www.sec.gov/news/press-release/2019-23.

(CRO), whose cybersecurity efforts will require, and deserve, increased funding. Additional SEC efforts and resources will be needed to make further improvements to the agency's information security environment, including its EDGAR filing system. A 2016 breach of that critical SEC system allowed the hackers to engage in illicit trading using the nonpublic information that was seized.[7] It is an unfortunate fact that some ICI members spend more on data security than the entire SEC budget, yet the SEC collects and must secure reams of sensitive market data, and in some cases, personally identifiable information.

In closing, I urge your support for robust funding for the SEC to fulfill its mission of protecting US investors, including the more than 100 million investors who own shares of regulated funds. These investors deserve the benefits of an SEC that can soundly and effectively regulate securities offerings, market participants, and the markets themselves.

With very best regards.

Sincerely,

Paul Schott Stevens
President and CEO
Investment Company Institute

cc: Members of the Subcommittee on Financial Services and General Government

[7] *See SEC Brings Charges in EDGAR Hacking Case* (press release, Jan. 15, 2019), available at https://www.sec.gov/news/press-release/2019-1.