April 25, 2018

Craig S. Phillips
Counselor to the Secretary
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220

Re: Treasury Report on Regulations Impacting Nonbank Financial Institutions, Technology, and Innovation

Dear Mr. Phillips:

The Investment Adviser Association[1] (IAA) appreciates the opportunities for our members and staff to meet with members of the Department of Treasury (Treasury) staff on January 8, 2018 and again on April 11, 2018.[2] We are pleased to provide comments following those meetings to help inform Treasury's upcoming report on regulations affecting Nonbank Financial Institutions, Technology, and Innovation (FinTech Report), pursuant to the President's "Core Principles" Executive Order (Executive Order).[3] Treasury's FinTech Report will serve as a foundation for regulatory policy in the quickly evolving world of financial technology (fintech) and we are hopeful that the report will help promote innovation and competition in financial services while continuing to protect investors and the markets. We would be pleased to provide any additional information that may be helpful.

General Principles

All IAA members are investment advisers registered with the Securities and Exchange Commission (SEC), and subject to principles-based regulation under the Investment Advisers Act of 1940 (Advisers Act) and related rules. As such, all of our members are subject to a fiduciary duty that obligates them to act in the best interest of their clients. Everything they do as advisers and asset managers, therefore, including their development and use of technology, is informed by this overarching duty. In order to both enhance the client relationship and

[1] The IAA is a not-for-profit association that represents the interests of investment adviser firms registered with the U.S. Securities and Exchange Commission (SEC). Founded in 1937, the IAA's membership consists of over 640 firms that collectively manage more than $20 trillion in assets for a wide variety of individual and institutional investors, including pension plans, trusts, registered investment companies (RICs or mutual funds), private funds, endowments, foundations, and corporations. For more information, please visit www.investmentadviser.org.

[2] Our first meeting with Treasury staff addressed issues relating to the provision of investment advice through a digital platform (Digital Advice Meeting). The second meeting addressed how advisers are exploring technology more broadly in order to enhance the client experience and relationship, streamline back-office functions, and provide other business efficiencies (FinTech Meeting).

[3] Executive Order 13772, Presidential Executive Order on Core Principles for Regulating the United States Financial System (Feb. 3, 2017).

experience as well as streamline back-office and other business functions, advisers are exploring the potential benefits offered by new technology, looking at new ways to streamline client onboarding, provide quality investment management and advisory services, process, store, and deliver information, and meet regulatory requirements.

Investment advisers approach technology from a highly regulated perspective, respectful of the protections inherent in the regulatory framework of the Advisers Act. Advisers seeking new technological solutions do not seek to eliminate regulation, but recognize that a modernized and measured approach to regulation will allow investors, the markets, and their businesses to thrive.

As Treasury considers the use of technology in financial services and whether to make recommendations regarding regulation in this area, we ask that you consider the following general principles:

- Regulatory focus should continue to be on investor protection and market integrity and efficiency while supporting and facilitating exploration of financial innovation.

- To allow for the industry to keep up with and harness changing technology, regulation must be principles-based. Prescriptive rules become quickly obsolete and, because they often fail to anticipate novel uses of technology, they invariably act as a roadblock to innovation. In the area of quickly developing financial innovation and technology, broad uniform standards are likely to be more effective than rules.

- Regulation and standards should be technology-neutral and not based on the presence, absence, or type of technology.

- Regulators should expressly support financial institutions taking a reasonable, risk-based approach when assessing, implementing, and applying technology to their businesses. For example, regulators should recognize that not all types of data are equally sensitive.

- Federal regulators should collaborate and coordinate with one another and with state regulators wherever possible to reach solutions so that regulated persons understand what is expected of them and to mitigate regulatory overlap and inconsistency.

- Both firms and technology are global in nature. U.S. regulators should seek international cooperation to facilitate global standards and solutions where appropriate, while guarding against needlessly burdensome international regulations that might hamper U.S. companies' progress and efficiencies.

- Regulators should continue to work with regulated industries, such as the investment adviser community, to further understand both the potential and the risks of new and emerging technology. Both the SEC and the Commodity Futures Trading Commission

(CFTC) recognize the need to foster responsible fintech innovation.[4] Treasury should play an active role in facilitating further and coordinated engagement.

Below we discuss the use of technology by investment advisers, including **digital advice**, **distributed ledger technology**, **cloud services**, the **use of third parties**, and **data aggregation**. We then identify areas of existing regulations that we believe would benefit from a **retrospective review** in light of current and developing technologies.

Digital Advice

Broadly speaking, the term "digital advice" is used to describe the way investment advisers use digital investment tools and algorithms to give investors, many of whom may not typically invest or save for retirement, a straightforward and low entry-point path for investment. Digital advisers thus provide important benefits to investors, especially as individuals are increasingly responsible for their own savings in retirement.

In our Digital Advice Meeting, several of our members described their business models, explaining how, notwithstanding their vastly different businesses, they all continue to operate effectively as fiduciaries within the flexible, principles-based regulatory structure of the Advisers Act. Thus, their services are an important component in empowering Americans to make independent financial decisions and informed choices in the marketplace, save for retirement, and build individual wealth.

It is important to underscore that the use of technology by digital advisers to offer investment services does not change the regulatory environment in which they operate, nor does it change the types of investments (*e.g.*, asset classes and investment strategies) that they offer their clients. As we explained in the Digital Advice Meeting, while each digital adviser adopts its own strategies and protocols, their investment approaches follow generally accepted investment protocols, including asset allocation, diversification, risk assessment, and prudent investment strategies. Our digital adviser members are not high frequency traders and they generally do not use highly leveraged or risky strategies. Rather, they simply offer a modernized and accessible portfolio approach to traditional investing. Regulations should not hinder the ability of advisory firms to develop and innovate in this area, including developing new ways of communicating with and onboarding investors.

The SEC in early 2017 issued helpful guidance to digital advisers, together with an investor bulletin on digital advice.[5] The SEC's guidance included suggestions for digital advisers on how

[4] *See, e.g.*, comments at *SEC FinTech Forum*, Nov. 14, 2016, details available at https://www.sec.gov/spotlight/fintech; and CFTC's efforts to promote responsible financial innovation through *LabCFTC*, details available at https://www.cftc.gov/LabCFTC/Overview/index.htm.

[5] *See SEC Staff Issues Guidance Update and Investor Bulletin on Robo-Advisers*, available at https://www.sec.gov/news/pressrelease/2017-52.html.

to meet their disclosure, suitability, and compliance obligations under the Advisers Act. At the time, then Acting Chairman Michael Piwowar observed that: "As technology continues to improve and make profound changes to the financial services industry, it's important for regulators to assess its impact on U.S. markets and give thoughtful guidance to market participants." He noted that the SEC's guidance and investor bulletin are "designed to help investors tap into the opportunities that fintech innovation can provide while ensuring fairness and investor protection." Importantly, the SEC's guidance reaffirmed that digital advice can be and is subject to the Advisers Act fiduciary duty.

Should Treasury consider any recommendations relating to the use of technology to provide investment advice, we ask that those recommendations support the approach set out in the SEC's guidance and underscore the importance of a principles-based flexible framework that applies uniformly to all advisers. Most importantly, regulators, including the SEC, should not adopt requirements that apply exclusively to digital advisers. This will allow for continued innovation that benefits investors and ensures that the Advisers Act and its fiduciary duty apply consistently to all advisers, regardless of how advice is delivered.

Distributed Ledger Technology

Distributed ledger technology (DLT), including, of course, blockchain, is frequently discussed by regulators in connection with cryptocurrencies and initial coin offerings. The focus of those discussions is often from the perspective of securities, commodities, or other financial investments rather than from the perspective of the potential of the underlying technology itself. We fully support regulatory efforts to protect investors and the markets generally and to shut down fraud and malfeasance in particular. That said, cryptoassets are only a small part of this burgeoning and potentially infrastructure-changing technology. We urge Treasury to encourage regulators to adopt a measured approach by also focusing on the promise of this technology, which, we believe, could revolutionize financial services.

As we discussed in our FinTech Meeting, DLT allows data to be stored securely and accurately in a decentralized format. The potential business applications are myriad. DLT can streamline and simplify workflows, increase immediate transparency for all parties, as well as for regulators, and provide enhanced data security. Through secure record of ownership and self-executing smart contract functionality, among other things, DLT could facilitate clearing and settlement across asset classes, proxy voting, data quality, securities lending, internal controls, and recordkeeping, to name just a few potential uses.

However, existing regulatory requirements either would impede the use of DLT in certain cases or there is a great deal of uncertainty around how these requirements would apply. This provides an obvious disincentive to explore potential operational applications of this new technology. We believe that DLT has enormous potential to create operational efficiencies in a number of different areas, including, for example, in areas of recordkeeping and in the trading and settlement of investments. Treasury should encourage these developments and work with the financial industry to map out a regulatory approach that will facilitate exploration and

innovation.

Cloud Services

In recent years, financial institutions of all sizes and fintech companies alike have championed the benefits of cloud computing,[6] including "public cloud" solutions offered by third parties such as Microsoft, Google, and Amazon Web Services. Indeed, cloud services may represent the most significant near-term potential growth area in technology use by financial service providers. These services not only offer significant operational efficiencies through economies of scale and lowered costs, but they also allow financial institutions to leverage technology to make financial services more accessible, affordable, and secure.[7] In many instances third-party cloud storage can be a more secure solution than managing private infrastructure, since it can offer large and world-class security teams and protective technology. Thus, even if every financial services firm could build its own infrastructure, it is doubtful they could all develop a similarly robust security program.

Regulatory uncertainty hinders financial institutions from making significant capital investments to deploy technology solutions or otherwise support these innovations. The uncertainty arises either because existing rules are unclear as to their applicability to cloud services or because dated regulatory guidance has not kept pace with the rapid and transformative impact of technology innovation in this space. Companies offering services that rely on public cloud solutions frequently encounter reluctance on the part of potential commercial partners, including investment advisers, because those partners are unsure whether their regulator will deem an innovative application compliant under third-party risk management and due diligence principles.

Given the prohibitive costs of building out and maintaining a private cloud infrastructure, it would be helpful for regulators—including the FFIEC, SEC, and CFTC—to clarify that financial services firms, including investment advisers, may leverage public cloud solutions provided that they exercise meaningful oversight and security diligence. We ask that Treasury encourage financial regulators to issue updated guidance[8] to make it clear that no law or regulation prohibits

[6] The Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook defines "cloud computing" as "Generally a migration from owned resources to shared resources in which client users receive information technology services on demand from third-party service providers via the Internet 'cloud.' In cloud environments, a client or customer relocates its resources – such as data, applications, and services – to computing facilities outside the corporate firewall, which the end user then accesses via the Internet."

[7] *See* Financial Services Roundtable, *Data Security, Integrity and Accessibility in the Cloud: Shared Responsibility Principles for Financial Services Institutions & Cloud Service Providers*, available at http://www.fsroundtable.org/wp-content/uploads/2017/05/FSR-Tech-Collaboration_Cloud-b.pdf.

[8] The most recent FFIEC guidance on cloud computing was issued in July 2012. The nearly six-year-old guidance classifies cloud computing as a "relatively new term" and offers little comfort that examiners will view the use of public cloud infrastructure as a reasonable risk decision. *See* FFIEC Information Technology Subcommittee,

the use of the public cloud. They also should make it clear that regulated entities may employ cloud services—directly or through their service providers—provided they develop effective oversight mechanisms designed to ensure that customer data and critical operations are protected. Importantly, we note that meaningful oversight does not mean perfect oversight. As we discuss below in connection with oversight of third parties, the standard for due diligence should be risk-based and not strict liability.

Use of Third Party Service Providers

Investment advisers have generally used third parties to provide or assist them with services. In recent years, their reliance on third-party vendors has increased substantially, especially with respect to technology. Some vendors are regulated entities, such as banks or transfer agents, but others are not subject to requirements relating to data collection, protection, transparency, or security. In addition, because of the pace of technological evolution, third-party contracts have not kept up with new developments—including new risks. This results in significant challenges for the adviser industry, which does not always have the expertise, or the leverage in these commercial relationships, to ensure optimal vendor safeguards.

Investment advisers are required to conduct due diligence of third parties as part of their compliance programs.[9] As emphasized above, advisers are also subject to a fiduciary duty to their clients, which imposes a high duty of care on them to oversee their vendors. However, these standards do not and should not be construed to impose strict liability on advisers for breaches or other failures of a third party. Regulatory expectations and principles should explicitly recognize that the standard of care for advisers is based on reasonableness under the circumstances.

Treasury should encourage a principles-based approach that focuses on process, not outcome. The approach should explicitly permit advisers to assess vendor risk and implement appropriate processes for due diligence, monitoring, incident response, and other controls commensurate with the risk. No matter how diligent an adviser's oversight has been, some vendor failures and data breaches can be expected. Regulators should focus on how the adviser evaluates and monitors the risk, assesses the exposure from a breach, and responds to the incident (including notifications and remediation). Determining the appropriate action following a breach will depend on the facts and circumstances and not on compliance with check-the-box rules, such as the time frame for notification of a breach or the specific method of providing notice. We discuss data breach notification regulation in more detail below.

We believe that commercial forces have and will continue to press third parties to have improved information security and be more responsive to diligence requests from financial institutions. But in parallel, regulators should acknowledge that the standard for advisers using third-party

---

Outsourced Cloud Computing (July 10, 2012), available at https://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf.

[9] *See Compliance Programs of Investment Companies and Investment Advisers*, Advisers Act Release No. 2204 (Dec. 17, 2003), available at https://www.sec.gov/rules/final/ia-2204.htm.

services should not be one of strict liability.

Data Aggregation

For purposes of this letter, we refer to "data aggregation" as services offered by third parties to aggregate a client's personal financial data from multiple providers onto a single platform. Consumers and the financial services industry generally all recognize the value of data aggregation. As stakeholders continue to work towards solutions acceptable to all market participants, we believe it is important to highlight certain principles, including **transparency**, **access**, and **security**.

Transparency. Consumers have a right to clearly understand and approve of how their data will be accessed and for what purposes it will be used. Likewise, consumers should have the ability to easily withdraw their consent to the collection, aggregation and use of their data.

Access. Consumers have a right to access their personal data, including to support the services their investment advisers and others provide to them. In a world where most individuals hold accounts at multiple institutions, access to aggregated data is critical to allowing consumers to understand their financial situation.

Security. Consumers have a right to expect that the data collected by aggregators will be kept safe and secure.

Treasury is well-positioned to help facilitate discussions among market participants and regulators as they develop and implement solutions that provide consumers access to their financial account information in a transparent, safe and secure manner.

Regulators Should Also Invest in Technology Solutions

The principles discussed in this letter apply not only to the financial services industry but also to regulators themselves. We believe it is critical that they invest in technology and technological know-how to enhance their understanding of evolving fintech, and to ensure greater protection and security for the data they collect from the industry.

Regulators should also be encouraged to help streamline regulatory compliance where they can. For example, they could put certain regulatory requirements into machine-readable format so that regulated entities can conduct automated reviews. Regulators should also consider forming internal working groups and industry advisory groups on key emerging areas such as machine learning and artificial intelligence and DLT. These areas in particular offer great promise for investment firms and are areas of continued focus by investment firms.

Modernization of Existing Regulations

Rules under the Advisers Act. Several rules under the Advisers Act require modernizing in light of new technology, including rules regarding books and records, custody, delivery of

information, and advertising. We addressed the need to modernize these and other rules in our earlier letter to Treasury in connection with its reports on asset management and capital markets issues.[10] However, these rules should also be revisited because of their negative impact on financial innovation.

Books and Records: Rule 204-2 under the Advisers Act requires investment advisers to maintain certain books and records. The SEC should make it clear that DLT and cloud services may be used to store records, as discussed above. In addition, to reduce uncertainty, the SEC's rules should clearly permit the use of electronic signatures when DLT is used. This includes extending the Electronic Signatures in Global and National Commerce (ESIGN) Act and the Uniform Electronic Transactions Act (UETA) to explicitly allow digital signatures executed on DLT technology as electronic signatures. DLT leverages the same public/private key encryption mechanisms that are fundamental to securing transactions and communications occurring throughout the Internet today. At the time the ESIGN Act and the UETA were enacted – 18 and 19 years ago respectively – such authentication practices were neither as pervasive nor as "tried-and-true" in securing the world's technological infrastructure as they are today.

Custody: SEC Rule 206(4)-2 under the Advisers Act addresses custody of assets by investment advisers. Regulators will need to understand new and evolving structures for custody and cryptoassets. This rule also raises a number of challenges for investment advisers with respect to whether and how asset ownership could be recorded or maintained using new technology such as DLT.

Delivery of Information: The SEC should promote the use of electronic delivery for required disclosures to advisory clients. Under guidance that goes back to releases issued in 1995 and 2000, an investment adviser may satisfy its ongoing disclosure delivery obligations by providing notice that the information is available electronically, ensuring effective access to such information, and by either evidencing actual delivery or obtaining informed consent from clients. Many advisers have been reluctant to use e-delivery due to the costs, implementation issues, and lack of clarity regarding the current consent requirements. We recommend that the SEC shift its approach from the "delivery with consent" model to a "notice and access" approach. Under a notice and access approach, an adviser would satisfy its delivery obligation by posting required disclosures on its website and providing clients a paper or electronic notice that includes a link to the location of the disclosures on the adviser's website page. Clients would not have to affirmatively choose this approach, but clients would still have the option of opting out to receive paper copies of disclosures at any time. The SEC has adopted a notice and access approach with respect to the delivery of other documents, including proxy materials. Encouraging the use of the electronic delivery as the default option for delivery would improve disclosures for investors, significantly reduce costs, and provide environmental benefits.

[10] Letter from the IAA to Secretary Mnuchin Re: Review of Regulations; Executive Orders 13771 and 13777 (July 28, 2017), available at: https://higherlogicdownload.s3.amazonaws.com/INVESTMENTADVISER/aa03843e-7981-46b2-aa49-c572f2ddb7e8/UploadedImages/publications/Treasury-RFI-Comment-Letter.pdf.

Advertising: Rule 206(4)-1 under the Advisers Act governs advertising by investment advisers. This rule has not been materially amended since its adoption in 1961, and includes certain *per se* prohibitions on advertisements by advisers that refer to either testimonials or past specific recommendations. Such restrictions no longer make sense in today's advertising and investing environment. Investors today are accustomed to conducting research on the Internet, creating and evaluating user reviews, and sharing views publicly. The ban on testimonials, in effect, thwarts common uses of social media. It is questionable, based on staff interpretations, for example, whether members of the public can "like" an adviser's online posts without running afoul of the rule. The rule materially impedes advisers' marketing activities, unnecessarily restricts potential investors' access to important information, and does not reflect investor expectations. We are encouraged that the rule is included in the SEC's regulatory agenda and we believe the agency should consider how investors seek information today and how they are likely to do so in the future about advisers and about their peers' experience with advisers.

Other Regulations in Need of Review. We discuss below other areas of concern for investment advisers, particularly in the areas of state regulations and regulations related to personally identifiable information.

Data Breach and Cybersecurity Regulations: A concerning area of regulation regards cybersecurity and the reporting of data breaches. Multiple federal agencies have issued regulations or statements regarding data security. To add to the complexity, many states also have requirements regarding reporting of data breaches. The various data breach notification laws and regulations create a difficult patchwork of regulatory burdens that is difficult for advisers to navigate. State laws differ from one another and from federal regulation in several respects, including timing of notice to individuals and regulators, as well as thresholds for reporting to a state attorney. We request that Treasury recommend, and encourage federal regulators and the states to adopt, a uniform standard regarding data breach notification that is risk-based and based on the facts and circumstances surrounding the breach.

In addition to data breach notification requirements, several states are considering or have issued cybersecurity regulations. For example, New York cybersecurity regulations, which do not expressly apply to investment advisers but may apply to many of our members that are also registered in other capacities,[11] represent first-in-the-nation regulatory requirements that impose significant obligations on covered entities, as defined in the regulations. The Colorado Division of Securities also recently adopted new cybersecurity requirements that apply to state-registered investment advisers.[12] Other states are now considering their own cybersecurity regulations. At least 28 states enacted cybersecurity legislation in 2017, while 42 states introduced some

[11] 23 NYCRR Part 500.01 (c) (2017) (A "covered entity" is defined as "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law").

[12] 3 CCR 704-1, Section 51-4.14 (IA).

resolution or bill related to cybersecurity.[13] Our concern is that states will not address these issues in a consistent manner, potentially causing a complicated maze of regulations for financial service firms.

Personally Identifiable Information. Another area of regulation in need of modernization regards the definition of personally identifiable information (PII). While we strongly believe that PII must be protected, we also believe that financial regulators should agree that not every piece of data is equally sensitive, and that regulated entities should focus on applying the highest protections to the most sensitive data. For example, an email address should not need to be treated precisely the same as a social security number. The theft of a social security number or checking account details can be significantly more damaging to an individual than the compromise of his or her mailing or email address. Fundamental risk management principles suggest that while each information category should be protected, financial services firms should focus most closely on protecting that information that would cause the most harm if compromised.

Existing regulatory guidance, at a very general level, acknowledges risk-based approaches to data protection. But, as discussed above in connection with third-party oversight, we think that regulators should make explicit through additional guidance that the practical application of these principles can reasonably lead to regulated entities applying their highest levels of protection to the most sensitive categories of PII, while applying lesser but still meaningful and appropriate levels of protection to less sensitive information. Innovation can be encouraged if security resources are focused on the areas with the most impact and sensitivity.

As an example, the FFIEC Interagency Guidelines Establishing Standards for Safeguarding Customer Information ("Interagency Standards") require financial institutions to design "information security programs to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of activities."[14] The Interagency Standards also "allow latitude to determine the sensitivity of customer information in the course of assessing the likelihood of and potential damage from the identified threats."[15] Although the Interagency Standards provide these high-level principles on classifying sensitive financial data, many financial institutions still labor under a concern that financial regulators will expect that they protect all types of customer information to the same extent and in a uniform secure manner. Additional guidance may alleviate some of this concern.

We ask that Treasury recommend that regulators encourage and permit financial institutions to

---

[13] *See* National Conference of State Legislatures, *Cybersecurity Legislation 2017,* available at http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2017.aspx.

[14] *Appendix B to Part 570–Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, 66 FR 8640 (Feb. 1, 2001).

[15] *Id*.

take reasonable, risk-based approaches to protect consumer privacy in a manner that includes data classification of PII commensurate with risk and remediation commensurate with potential harm. Financial regulators should clarify that while all PII must be safeguarded appropriately, depending on the circumstances, companies may reasonably decide to apply different levels of protection and remediation to different categories of PII based on sensitivity and potential harm to consumers. This principles-based approach would allow firms to tailor data protection to their clients and business models.

* * *

We applaud Treasury for its comprehensive approach to studying fintech, its related benefits and challenges, and the need to review whether and how regulations need to be updated to encourage exploration of technology that promises to benefit investors and financial services firms. We appreciate the opportunity to meet with you and provide comments and insights on these important issues. Please contact the undersigned at (202) 293-4222 if we can be of further assistance during the preparation of your report.

Respectfully Submitted,

Gail C. Bernstein
General Counsel

Paul D. Glenn
Special Counsel

cc: The Hon. Jay Clayton, Chairman, SEC
The Hon. Kara M. Stein, Commissioner, SEC
The Hon. Michael S. Piwowar, Commissioner, SEC
The Hon. Robert J. Jackson, Jr., Commissioner, SEC
The Hon. Hester M. Peirce, Commissioner, SEC
The Hon. J. Christopher Giancarlo, Chairman, CFTC
The Hon. Brian D. Quintenz, Commissioner, CFTC
The Hon. Rostin Behnam, Commissioner, CFTC