October 18, 2018

Jennifer Piorko Mitchell
Office of the Corporate Secretary
FINRA
1735 K Street, NW
Washington, DC 20006-1506

Re: *Special Notice: Financial Technology Innovation* (July 30, 2018)

Dear Sir/Madam:

SIFMA[1] appreciates the opportunity to comment on FINRA's Special Notice on Financial Technology Innovation. The financial services industry uses technology to better serve and protect customers, improve security, and compete globally with other financial services providers. SIFMA appreciates FINRA's continued attention and support of fintech innovation while also seeking to educate investors about potential risks. SIFMA also appreciates FINRA's efforts to improve the technological expertise of its staff by engaging with the industry both formally through its Fintech Advisory Committee and informally through the examination process and meetings with industry groups including SIFMA. We welcome the opportunity to provide additional information and expertise on any of these topics or other related issues.

As you know, SIFMA has taken an active role in many fintech issues including recently issuing Data Aggregation Principles[2] and submitting an extensive white paper on financial technology innovation to the

[1] SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

[2] *See* SIFMA Data Aggregation Principles (April 2018) (available at https://www.sifma.org/explore-issues/personal-data-aggregation/).

U.S. Department of the Treasury ("Innovation White Paper"),[3] as well as an extensive sandbox proposal.[4] SIFMA continues to examine the role of technology in the financial services industry as a means of providing a better customer experience but also improving compliance with laws and regulations.

As previously stated in our Innovation White Paper, SIFMA believes that the following general principles should guide all regulators in their efforts to promote financial services innovation:

- Innovation in the financial industry is essential to its success and must be encouraged. Regulators should therefore ensure flexibility of the regulatory framework to encourage and support innovation without compromising consumer protection or the safety and soundness of the financial system.
- Regulations and supervisory practices should be principles-based and technology-agnostic to accommodate future innovation without requiring regulatory reforms each time a new technology is created. New regulations are not necessary in many cases.
- Innovation and customer protection are optimized when regulation is based on function or activity (rather than the type of entity or regulated status) and applied in a consistent manner. This requires a rethinking of our current entity-based regulatory framework in addition to coordination and commitment among regulators with different jurisdictional interests at both the federal and state levels.
- Regulatory policy should encourage collaboration among federal and state regulators, financial institutions, and technology companies—in each case both domestically and internationally—to maximize knowledge-sharing.
- Regulators should have advanced technological expertise to evaluate changing technologies.

SIFMA urges FINRA to use these principles as a guiding force in any future rulemaking and guidance intended to address financial technology issues.

1. Rules or process that could be modified to better support fintech innovation

SIFMA agrees that rules that inhibit innovation in financial services without harm to customers should be reconsidered and potentially amended and removed. To that end, FINRA should do a formal rulebook review which may be technologically outdated regardless of whether they directly or indirectly support fintech innovation. Further, any time a new rule is implemented, FINRA should consider whether the rule

[3] *See* SIFMA Promoting Innovation in Financial Services (April 6, 2018) (available at https://www.sifma.org/resources/submissions/promoting-innovation-in-financial-services/).

[4] *See* SIFMA Fintech Regulatory Sandbox Proposal (May 14, 2018) (available at *https://www.sifma.org/resources/submissions/sifma-fintech-regulatory-sandbox-proposal/*) ("Sandbox Proposal").

supports a particular technology or standard which may become outdated in the future or which may inhibit technology innovation.

FINRA should also consider using a joint regulatory sandbox program, which would allow broker-dealers to test new technologies in a live environment at the same time allowing regulators to identify barriers in regulation, such as existing FINRA or SEC rules. This would allow firms to test new technology, including artificial intelligence applications, in the earlier stages of development in a more robust manner than would otherwise be possible. To be most effective, a sandbox should be a cooperative effort between regulatory agencies, established and supervised as a collaborative effort. The broadest range of financial regulatory authorities should be included to prevent fragmentation, including at a minimum the Securities and Exchange Commission ("SEC") and the Commodity Futures Trading Commission ("CFTC") for markets activities. Such a collaboration would educate all regulatory staff about the potential use of the technology while also providing member firms with feedback from FINRA staff.

Below are a few examples of rules and policies that may and will affect member firms' use of evolving technologies.

a. Communications Rules

FINRA's rules governing communications and advertising may inhibit member firms' ability to test innovative communications concepts which may or may not be viable for their intended use or the firms' business. Requiring member firms to follow each level of approval, retention and supervision imposes a significant burden on a firm's ability to test a new product, application, process, or tool. Firms should have the ability to use a sandbox approach for such new products to safely alleviate the burden of certain rules during the testing stage.

b. SEC Recordkeeping Rules

Further, although not a FINRA rule, SIFMA would like to once again highlight the challenges of the SEC's requirement for broker-dealers' digital books and records to be stored in a non-rewritable, non-erasable system such as the "write once, read many" ("WORM") format under Exchange Act Rule 17a-4(f).[5] Because neither the banking regulators nor the CFTC require that records be stored in WORM format, the disparity between recordkeeping standards put in place by the SEC and those of other regulators makes implementing new technology unnecessarily challenging.

[5] 17 C.F.R. § 240.17a-4(f).

SIFMA with other trade associations has submitted a petition to amend Rule 17a-4 to make it less burdensome and outdated.[6] SIFMA is petitioning the SEC to remove WORM storage requirements and implement electronic recordkeeping standards that employ principles-based and technology-agnostic requirements such as those applicable to investment advisers, investment companies, transfer agents, and now swap dealers and futures commission merchants.[7] The CFTC recently eliminated the WORM requirement from its rules, choosing to modernize its recordkeeping requirement by introducing a principles-based approach, rather than prescriptively requiring that digital books and records be stored in WORM format. FINRA should consider publicly supporting this petition.

2. Data Aggregation

SIFMA believes that the financial services industry should be allowed to reach solutions for data aggregation without the imposition of new regulations. Stakeholder collaboration in the industry is central to the current fast pace of innovation in the industry, including the adoption of new standards and data handling protocols to facilitate customer access, control, and enhance data security. At this time, FINRA should refrain from rulemaking that may disrupt the industry's progress toward the adoption of uniform access, security and data handling standards. SIFMA believes that regulators should be limited to articulating general principles and guidelines to help industry as it works to address issues and develop solutions, as FINRA has done, rather than engaging in direct regulation of data aggregation practices. SIFMA is working with financial institutions, financial technology companies, and other industry groups to develop common technology standards and protocols that will help our members to better protect customer data. On October 18th the industry launched the Financial Data Exchange, a new organization dedicated to setting common technology solutions that would allow financial institutions, aggregators, and intermediaries to more securely transfer authorized customer data.

The minimum standards include:

- Because of the extensive damage that could result from data being compromised, participants in the fintech chain are partnering with the industry to develop and implement a means to access consumer financial data that does not require sharing their confidential financial account credentials (e.g., personal IDs and passwords). Instead, all participants should work to maximize the availability and use of modern, safe and hygienic methods (e.g., OAuth), which triangulate authentication with the bank and protects consumers from having to share this sensitive information with third parties.

[6] *See* SIFMA Petition for Rulemaking to Amend Rule 17a-4(f) (Nov. 14, 2017).
[7] *See* id. at 9 for proposed rule text that our membership has suggested previously.

- Because data aggregators are often retained by third parties, such as fintech service providers, these aggregators are often invisible to consumers. Clear disclosure and explanation of this relationship, including the name and contact information of the aggregator, should also be included as part of the required notice and consent. Any aggregator that has a direct consumer relationship should already be clearly subject to Gramm-Leach-Bliley Act ("GLBA") and required to provide a privacy notice in connection with establishing the consumer relationship.

- Third parties that do not have direct consumer relationships and only facilitate access to data:
    - Should only access the customer financial account data necessary to provide the product or service they are offering and should not be permitted to access or use other non-public and confidential personal information;
    - Must ensure that clear and conspicuous explanations of how they will access and handle consumers' financial account data, including whether they will pass or sell that data on to other parties, are provided to consumers. For such disclosures to be effective, consumers must be able to readily and easily control that access both before it begins and on an ongoing basis.

- Consumers should be able to withdraw their consent easily and at any time with confidence that data aggregators with whom they have relationships, or behind-the-scenes third parties, will stop collecting their personal information and delete any access credentials or tokens within a reasonable time of withdrawal of their consent.

- Consumers deserve assurances that anyone accessing their personal information will keep it safe and secure, adopt the same data and security standards followed by regulated financial institutions, and share full responsibility for any personal information that they receive and provide to others while such data is in their custody or control. In addition, consistent standards should be applied across the aggregator community regarding notifying consumers and federal banking regulators about any personal data breach.

- Third party data aggregators should be responsible for the risks they create and bear financial responsibility for customer losses incurred.

SIFMA applauds FINRA's efforts to provide clarity on these issues, as well as educate consumers in the recent *Investor Alert* on the risks of using data aggregation products, particularly when required to share

log-in credentials.[8] SIFMA believes that customers may not always take these risks into consideration when using data aggregation services and FINRA's materials are an important resource to improve customer awareness.

3. Artificial Intelligence and Robotic Process Automation

a. Supervision in the Context of Artificial Intelligence

Artificial intelligence ("AI") uses in the financial services industry are in the early stages of production but the possibilities are expanding rapidly. Given the potential for AI to provide major societal and economic benefits in the future, stakeholders must foster its innovation and development. As with any developing technologies, it is important that the risks are considered and actively managed. AI is intended to enhance existing processes and procedures such that they are more efficient and accurate and not replace human intelligence as is sometimes inferred. The ultimate decision-making is generally still done by humans, not computers.

Under the current regulatory framework, regulation should not be directed at the technologies used by firms, but at the activities in which firms engage. This approach will allow technology to develop to the maximum benefit of all market participants, while safeguarding clients and market stability. FINRA, together with other regulators, should observe where risks are accumulating due to changing business models or market pressures, and encourage continued dialogues with the industry in this regard.

We welcome FINRA's efforts to further engage with members in better understanding the use of AI. AI technology has been evolving over several decades, but now thanks to the increasing availability of data, advancements in computing power, and better algorithms, the use of AI to facilitate product and process innovations is more practical and scalable. Given the massive advancements in AI research over the past few years, understandably the media has been dominated by stories relating to the huge problem-solving potential of AI on the one hand, and similarly outsized fears around its risks and impacts on the other. In reality, the financial industry is generally focused on using AI in narrowly-defined tasks where there is greater certainty of reliability in outcomes.

AI comprises a large variety of techniques, so it is important to ensure that there is clarity between stakeholders when engaging in discussions on AI. There is no single definition of AI and opinions are mixed especially as it comes to approaches that have characteristics of both AI and traditional statistical methods, with techniques that have long been a part of econometric modelling toolkits generally not

[8] *See FINRA Investor Alert: Know Before You Share* (March 2018) (available at http://www.finra.org/investors/alerts/know-you-share-be-mindful-data-aggregation-risks).

considered AI. However, most relevant approaches share certain common attributes, such as the use of cross-validation and a degree of automation in the model development (feature engineering) process. Furthermore, the subset of AI known as machine learning, which broadly sorts techniques into the groups of supervised learning, unsupervised learning, and reinforcement learning, is commonly used today across the financial industry and other sectors. In that respect, innovations such as the majority of robotic process automation ("RPA") do not use AI, but nevertheless equally deserve to be considered with regards to matters of supervision.[9]

There are a multitude of potential benefits depending on the AI use case, but generally the use of AI results in the more efficient processing of information which can result in lower costs, improved regulatory compliance, better customer experience, better risk management, and more optimal decision making. There are currently several use cases for AI for broker-dealer businesses in various stages of maturity, including:

- Enhanced fraud protection
- KYC/AML
- Trade surveillance/market abuse
- Development of investing strategies
- Order execution
- Evaluation of market risk
- Aggregation of written communications or extraction of themes from documents
- Enhanced client service capabilities

Although not necessarily yet identified, future use cases are likely to include areas where consolidated, high quality big data is available and can be used to augment or make existing manual processes more efficient. These innovations would conceivably allow businesses to make better informed decisions, and free up human resources to perform higher value tasks. For example, machine learning may be applied in jobs such as trading, investing and credit decisions. However, today there are natural challenges that will be overcome as technologies continue to develop and evolve. For example, machine learning still faces challenges in consistently solving complex problems with many different variables or outcomes.

The use of AI does not always result in novel risks, but in some cases may amplify existing risks or manifest new sources of existing risks. Potential risks and the way in which firms manage or mitigate those risks has been well documented, and include, for example, the use of data that contains errors or biases could result in incorrect or sub-optimal outcomes or decisions. This is clearly not a new risk but

[9] See Attachment.

given that it could result in increased reputational or financial risks is taken very seriously and addressed through various controls such as extensive testing.

The complexity of AI is often cited as a key concern, but complexity varies depending on the specific techniques required to solve a given problem. In some instances, AI solutions are less complex than certain commonly used statistical methods. The challenge faced by other methods, deep learning in particular, is that they can be highly complex and are seen as “black boxes” whereby there is no intuitive way for the user to understand why or how an algorithm has made a decision. To be sure, the need to have explainability of an algorithm depends entirely on the use case. For example, where an algorithm has a greater bearing on a decision or its outcome has a material impact on individual persons, the need for explainability arises. Firms realize the importance of explainability, especially when considering the use of AI in regulated activities and are rapidly developing techniques to “open up the black box” and interpret more complex algorithms.

Additionally, the risks and challenges associated with AI are not unique to financial services and are widely acknowledged by the tech and academic communities. As with data aggregation, there are industry efforts underway to address the challenges associated with AI, for example, including the development of explainable artificial intelligence (“XAI”). These efforts should be encouraged as this is the most practical and flexible approach. FINRA may wish to communicate its concerns with members to engage in a productive dialog and provide valuable input around regulatory expectations which will guide industry efforts as it tackles these challenges.

Uncertainty around regulatory expectations may inhibit or slow innovation. Financial institutions will require more clarity on FINRA’s expectations on explainability, transparency, model governance and testing. Further FINRA should assess existing rules to ensure they are flexible enough to accommodate the use of new technologies to carry out existing activities. For example, sandboxes or waivers may be used to test and validate AI models in real-world environments instead of test environments.

Broker-dealers are driving responsible innovation and, like any new technology, implementing AI requires controls to ensure compliance with existing laws and regulations. In terms of accountability, firms typically pursue the use of AI with appropriate control in order to generate business results and this is driven by a “head of data analytics” or similar senior office that is responsible for driving AI strategy in partnership with technology and business teams. Models that use AI are subject to model governance processes, which ensures the appropriate model controls are taken and that the models do what they’re intended to do. These governance processes are based on the process for standard models to ensure a unified approach that meets regulatory requirements. Firms carefully supervise and thoroughly test new systems, which often initially run alongside systems they are designed to improve, before they go into full production.

As explained above, FINRA should not consider regulations targeted at AI. AI is a technological method of carrying out a function and not an activity in and of itself that needs to be regulated. One of the key takeaways from the recent White House summit on AI[10] was that overly burdensome regulations could force innovation to take place outside of the U.S. SIFMA supports the administration's leadership in removing regulatory barriers to the deployment of AI-powered technologies. Similarly, SIFMA supports the U.S. Department of the Treasury's recommendation that regulators should not impose unnecessary burdens or obstacles to the use of AI and machine learning and should provide greater regulatory clarity that would enable further testing and responsible deployment of these technologies by regulated financial institutions as the technologies develop.

FINRA should, however, explore ways to continue ensuring that supervisory staff at all levels are adequately informed about AI and machine learning technology, including how it is used and its benefits and risks, and monitor the impact of AI on various aspects of the financial services industry. FINRA has demonstrated its willingness to engage with the industry, commitment to promoting safe innovation, and educate itself on technological developments. FINRA already engages with member firms through the ongoing supervisory process, including requests for documentation and more detailed information, which promotes a dialog relating to firms' initiatives. By virtue of this interaction, there should be greater confidence that firms are not developing uses of AI in isolation or without oversight.

b. Robotic Process Automation

The Special Notice included RPA in a list of technologies including AI, machine learning, chatbots, and other more "cognitive" emerging technologies. It is important to clearly define what RPA is as a rule-based technology, and equally importantly, how it differs from cognitive technologies. Defining the purpose and functions of RPA and the specific differences from AI and machine learning is critical for understanding how securities firms apply them, and the oversight and control frameworks that are used to supervise each of these technologies. Attachment A to this letter includes more information on RPA which may be helpful to FINRA as these technologies evolve and become more prevalent in the securities industry.

FINRA should further explore the differences between RPA and cognitive technologies, as well as the distinctions among the various other cognitive technologies. Understanding these nuances is critical for regulators as member firms adopt new processes and procedures using these technologies.

[10] *See Summary of the 2018 White House Summit on Artificial Intelligence for American Industry* (May 2018) (available at https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf)

4. Development of a Taxonomy-Based Machine-Readable Rulebook

SIFMA believes that there are opportunities for FINRA to develop a machine-readable rulebook which would allow the integration of advanced technologies into firms' existing compliance structures. The adoption of such a system would encourage the fintech industry to continue to build out compliance solutions that take advantage of machine-readable formatted regulations.

Firms will be more likely to take advantage of a machine-readable rulebook if the format interacts well with existing systems. FINRA should consider surveying member firms about their current systems and practices to ensure that the new format complements systems without requiring firms to build-out new systems.

Further, FINRA should issue routine supervisory reports on numerical regulatory outcomes and data sets. Other, less prescriptive regulation would require more work to transpose into machine-readable code and could start to be tackled once more simple reporting has successfully been automated.

* * *

SIFMA would appreciate any opportunity to discuss these and other fintech issues with FINRA staff. If you have any questions or would like to set up a meeting please contact me at 202-962-7300.

Sincerely,

/Melissa MacGregor/

Melissa MacGregor
Managing Director & Associate General Counsel

cc: Charles DeSimone, Managing Director, SIFMA
Christopher Killian, Managing Director, SIFMA

Attachment
Robotic Process Automation (RPA)

1. RPA vs Cognitive Technologies

According to the IEEE Standards Association (IEEE SA), robotic process automation is defined as the use of "preconfigured software instance that uses business rules and predefined activity choreography to complete the autonomous execution of a combination of processes, activities, transactions, and tasks in one or more unrelated software systems to deliver a result or service with human exception management."[11] In other words, RPA software is a means to increase processing efficiency in repetitive, rules-based processes by using software to simulate the sequential "robotic" actions performed by a human on a computer.

The fundamental difference between RPA and cognitive technologies or automation strategies is that RPA does not have intelligent decision-making ability based on learning or other cognitive abilities. Beyond carrying out a pre-programmed sequence of actions to the exact parameters (or "instruction set") laid out in its implementation. RPA does not have the ability of cognitive technologies such as learning, reasoning, or generating and testing hypotheses of its own. This distinction is critical in understanding RPA applications and oversight. An RPA may run on top of existing applications and may have a unique profile and access rights mimicking the actions of a human.

The use of the term "robot" in the discussion of RPA software does not imply any use of judgment, evolution of the program rules, or decision making based on learning by the software as is done in AI, that has not been specifically built, and tested by, the implementation team. Some users characterize RPA applications as being "events based," in that, as with any traditional process automation software, they are driven by defined if/then conditions for the start and stop of their activities based on the parameters defined by their users.

Similarly, unlike in machine learning applications, in RPA, the software "robots" are not autonomously learning or getting better over time at identifying issues or options – unless humans update the instruction set of the RPA programs.

Machine learning, on the other hand, is a specific application of artificial intelligence that empowers machines to learn and improve without being explicitly programmed. Using statistical techniques, a

[11] https://standards.ieee.org/standard/2755-2017.html

computer system can be trained (or train itself) to find relationships in a dataset, create predictive models based on those relationships, and update its model to improve the accuracy of its predictions.

Finally, artificial intelligence is "the combination of cognitive automation, machine learning ("ML"), reasoning, hypothesis generation and analysis, natural language processing and intentional algorithm mutation producing insights and analytics at or above human capability."[12]

In summary, RPA replicates human *actions* while machine learning and artificial intelligence seek to imitate human *cognition.*

2. Benefits of RPA

Applications of RPA offer a range of benefits to firms, and ultimately to their clients as well. At the highest level, RPA allows repetitive tasks to be done more accurately and efficiently. Using RPA reduces or eliminates the introduction of human error and ensures that these tasks are done repetitively well - more efficiently, and accurately, at scale. Increasing the accuracy of processes and reducing error rates drives improvements in data quality, throughput, and the overall control environment. RPA applications allow managers to know exactly what is being done and by who. This transparency of process and the reduction of error translates directly into improvements in KPIs such as cycle time, quality, and accuracy.

Creating efficient and less error-prone processes directly translates into substantial client benefits. Client experience improves when RPA allows work to be done more quickly and accurately – greater speed of processing provides high-quality information and results to clients faster, while greater accuracy reduces the amount of time that clients need to spend interacting with broker-dealer staff to resolve any errors that arise during processing. Automating routine processing frees up staff time to focus on enhanced client service, handling of exceptions and other complicated issues, where the expertise of human staff is needed to help clients resolve issues.

While RPA is an extension of the longstanding trend towards process automation, it does offer certain advantages over prior approaches to automation. For example, RPA can be leveraged within, and around, a firm's core infrastructure technology and operations flows. Examples of this include bridging the gap between IT staff availability and timeframe required to enhance discrete manual core infrastructure workflows, systems or platforms, managing information produced by different systems, etc. – tasks humans have performed in the past but can be automated.

[12] IEEE Standards Association, "IEEE 2755-2017 - IEEE Guide for Terms and Concepts in Intelligent Process Automation", https://standards.ieee.org/standard/2755-2017.html

Handling functions through RPA also generates substantial amounts of data on the processes involved. This data can be used for more effective risk management, oversight, analysis, detailed client reporting and further data driven process improvement. SIFMA members have pointed to improving data quality and its associated benefits for reducing risk as a major motivation for using RPA.

While reducing costs by replacing human capital with machine resources is often perceived as the primary driver for augmenting manual processes with RPA, SIFMA members have cited in benchmarking surveys that improving the quality of work done by their staff and their work experience is their most important motivation for adopting RPA. Rather than just being a rationale for replacing people with machines, effective use of RPA allows for the redeployment of staff to higher value tasks like risk management, more frequent and customized client facing interactions, and other tasks which require human judgement and expertise. In addition, the cost, accuracy, and efficiency benefits of RPA also allow firms to repatriate process which had been moved off shore back to within the US.

For example, RPA applications can process most high-volume, manual, and routine transactions while human staff devote their efforts to investigating and resolving exceptions that are identified by RPA software. This model allows for a tremendous improvement in overall efficiency, more effective risk management, enhanced oversight, and employee job satisfaction. The reduction in manual processing time afforded by RPA directly increases opportunities for staff to offer bespoke support, service, and analysis to clients and counterparties.

RPA also improves basic automation within applications that have been handled in the past by non-IT user-created software macros and offers advantages in risk management compared with ad hoc approaches. In contrast with software macros, which are often created outside the standard IT governance development and oversight protocols, RPA offers discrete software that can be created and managed within a structured IT governance framework while providing tech-savvy users with greater control and enhanced ability to deliver solutions that can interact with a range of different programs and systems. These actions can be tracked automatically by the RPA program, which provides readily accessible monitoring and auditing benefits not often available when using software macros. As firms apply RPA to their current activities, the implementation process is also an opportunity to rework processes to bring them closer in line with best industry practices.

RPA can also be combined with other emerging technologies to further improve processes. According to the SIFMA survey, firms find optical character recognition (“OCR”) and natural language processing to be the most common technological pairings with RPA. Firms are also exploring how RPA can be connected to artificial intelligence applications such as chatbots to improve client experience.
Connecting RPA with OCR is a natural extension of its capabilities to extract, process, and update information. As an example, one workflow could be: OCR is used to extract information from printed

forms or other documents, then natural language processing is applied to analyze and understand this information in its digital form, and finally it can be processed using rules-based RPA software to flag exceptions. The benefits of this multi-tool technology solution are clear – allowing firms to easily unlock information from a range of documents, and then track and manage it offers greater accountability, oversight, and efficiency.

There are also challenges for firms that apply RPA. In addition to the issues of control and supervision discussed below, it is important to develop plans to keep the knowledge base intact with the organization as processes are automated. In addition, firms need to consider how business resiliency and business continuity planning intersect with RPA, such as whether human staff would replace RPA in a disaster recovery environment that does not support RPA.

3. Common Applications of RPA

Use of RPA in the securities industry varies widely depending on system configurations, business models, technology infrastructure, and general strategy. Effective RPA deployment needs to be built on top of processes that are not optimized, because it cannot overcome the shortcomings of those that are poorly structured, bloated, or otherwise ineffectual. RPA is not a substitute for a flawed process, so naturally there is variation in where firms chose to incorporate RPA within their broader strategies for ongoing automation and process improvement.

There are, however some key areas where firms have deployed RPA to date, including transaction processing, data extraction, data entry, data aggregation, data transformation, and reporting. The industry is also in the early stages of using RPA for static data entry and maintenance, client servicing, compliance, and surveillance.

RPA also has potential to assist firms in reconciliations. For example, by applying RPA to the process of comparing data between systems, firms would be able to handle most easily resolvable mismatches, thus leaving human staff to resolve more complex cases. In addition, RPA can be layered with existing third-party technology which cannot efficiently interact or connect with other systems or technologies.
Firms will continue to identify areas where RPA will improve systems and processes, but will focus primarily on rules-based, repetitive tasks that can leverage the strengths of RPA. Some firms have created frameworks for identifying and implementing RPA including legal and compliance reviews, risk reduction, efficiency, and broader business strategy considerations.

4. Oversight and Control of RPA

The oversight and control requirements firms are using to manage RPA deployments are shaped by markedly different considerations than some other forms of emerging technologies or cognitive applications. As SIFMA members implement RPA, they are working to situate it within existing well-defined and clearly structured oversight models. These models draw on firms' prior experience with automation, as well as extending the supervision and control frameworks used for human employees to encompass digital labor. Applications of RPA do not eliminate any supervisory responsibilities, and firms still need the same supervision, risk management, and control frameworks for processes that incorporate RPA. Firms recognize these requirements and have worked to develop programs which extend and apply the supervision requirements for human labor to RPA as well. The expectations for control around RPA are also more closely aligned to those for human labor than they are to existing standards for cognitive technologies, such as the use of algorithms on the trading side, for example.

Firms working with RPA draw on their existing governance and control experience working with new software and technology through the structured software development lifecycle and best practices. Industry management of RPA deployments draws on extensive experience for technology change management procedures and best practices. Similarly, firms draw on their existing programs to manage vendors and third parties, as well as FINRA's outsourcing guidance.

Some firms have found it valuable to develop a Digital Labor Center of Excellence for RPA, or equivalent function, which provides central governance to manage and oversee the use of RPA. Other firms integrate RPA within their existing business or operations control framework (depending on the firm and the applications where RPA is used) or connect it with their technology control and risk management processes. These programs also include structures and guidelines for supervision of the maintenance of RPA, testing, and ongoing reviews.

Firms have also focused on ensuring that the deployment of RPA is consistent with requirements for segregation of duties. Approaches used by firms include: provisioning unique user IDs for associated systems and application permissions, just as human employees would have; functional isolation; entitlement management programs; and other supervision models.

Firms suggest that as RPA becomes more widespread within the industry, policies to supervise and control it will continue to evolve. Potential future considerations could include standard IT post-implementation reviews, onboarding processes for RPA similar to those for workers, and developing oversight frameworks that recognize the differences between early applications of RPA and "seasoned" digital labor.

SIFMA and its members would be happy to further discuss and share experiences with FINRA regarding how they have been approaching these important supervision and risk management responsibilities.

5. Regulatory Context for RPA

SIFMA members do not currently see major regulatory obstacles to the continued development and implementation of RPA in securities markets processes. FINRA should further explore the differences between RPA and cognitive technologies, and the difference between the various cognitive technologies themselves. The differences between the technological and operating models of each of these technologies, and each firm's unique use of them within their business, create a variety of different contexts within the broader regulatory framework. Understanding these nuances is critical for regulators as the industry adopts new operating models and approaches to processing using these technologies.