

Technology Based Innovations for Regulatory Compliance (“RegTech”) in the Securities Industry¹

SEPTEMBER 2018

Contents

Executive Summary	1
I. Introduction	2
II. RegTech Applications in the Securities Industry	3
III. Implications of RegTech for the Securities Industry	6
IV. Request for Comments	11
Endnotes	12

A REPORT FROM THE FINANCIAL INDUSTRY REGULATORY AUTHORITY

Executive Summary

Regulation is a fundamental pillar supporting the success of the financial services industry, ensuring protection of investors and integrity of markets. Over the past century, regulatory requirements have evolved, both in the U.S. and globally, to keep pace with the growing complexity, speed and sophistication of the financial markets.

As financial services firms seek to keep pace with regulatory compliance requirements, they are turning to new and innovative regulatory technology (RegTech) tools to assist them in meeting their obligations in an effective and efficient manner.² These RegTech tools may facilitate the ability of firms to strengthen their compliance programs, which in turn has the potential to create safer markets and benefit investors. However, these tools may also raise new challenges and regulatory implications for firms to consider.

RegTech tools may facilitate the ability of firms to strengthen their compliance programs, which in turn has the potential to create safer markets and benefit investors. However, these tools may also raise new challenges and regulatory implications for firms to consider.

To better understand the implications of RegTech for the securities industry, FINRA undertook a focused review to learn more about the emergence and adoption of related tools within the securities industry.³ As part of these efforts, FINRA staff held discussions with over forty participants in the RegTech space, including broker-dealer firms, vendors, RegTech associations, academics and various other key players.⁴

This paper summarizes key findings from our review. Specifically, Section II of this paper provides a summary of how RegTech tools are being applied in the following five areas: (i) surveillance and monitoring, (ii) customer identification and anti-money laundering (AML) compliance, (iii) regulatory intelligence, (iv) reporting and risk management, and (v) investor risk assessment. Subsequently, Section III highlights key benefits and potential regulatory and implementation implications for broker-dealer firms to consider as they explore and adopt RegTech tools.

The discussion below is intended to be an initial contribution to an ongoing dialogue with market participants about the use of RegTech in the securities industry. Accordingly, FINRA is requesting comments on the areas covered by this paper.⁵ FINRA also requests comments on any related matters for which it would be appropriate to consider additional guidance, consistent with the principles of investor protection and market integrity, based on RegTech applications and their implications for FINRA rules.

I. Introduction

Role of RegTech

While the term RegTech does not have a commonly agreed upon definition, it is generally used to refer to new and innovative technologies designed to facilitate market participants' ability to meet their regulatory compliance obligations. The Institute of International Finance defines RegTech as "the use of new technologies to solve regulatory and compliance burdens more effectively and efficiently."⁶

Market participants are increasingly looking to use RegTech tools to help them develop more effective, efficient, and risk-based compliance programs. These RegTech tools have the potential to fundamentally transform how securities industry participants perform their compliance obligations. However, these tools may also raise new challenges and regulatory implications such as those associated with supervision, vendor management, data privacy and security.

Similarly, regulators are looking to enhance their regulatory efforts by using RegTech tools that leverage innovative technologies. For example, FINRA has deployed cloud storage and computing, big data analytics, machine learning and natural language processing to enhance its market surveillance and other regulatory functions.⁷

Rise of RegTech

A growing number of technology startups are leveraging a variety of innovative technologies to assist financial services firms with their regulatory compliance efforts. Additionally, many incumbent financial services firms have begun to develop a variety of RegTech tools in-house. According to a Thomson Reuters survey of over 500 compliance and risk professionals, "[r]egtech has begun to shape compliance. More than half (52 percent) of respondents considered that regtech solutions were affecting how they managed compliance in their firms with almost a fifth (17 percent) reporting they have already implemented one or more regtech solutions."⁸ A recent CB Insights study also notes that RegTech startups globally have raised nearly \$5 billion in funding across 585 deals between 2013 and 2017, with the bulk of startups in this space focused on compliance in the financial services sector.⁹ These past investment figures, however, only represent a small portion of the anticipated RegTech related expenditures in the coming years. One research report predicts that: "[t]he global demand for regulatory, compliance and governance software is expected to reach USD 118.7 billion by 2020."¹⁰

A growing number of technology startups are leveraging a variety of innovative technologies to assist financial services firms with their regulatory compliance efforts.

The recent rise of the RegTech industry has been shaped by both regulatory developments and technological innovations. While the use of technology to help meet regulatory requirements is not a new phenomenon, the confluence of significant regulatory and technological changes over the past few years has created incentives for firms to rethink how compliance functions operate.

The 2008 financial crisis resulted in the adoption of a number of new regulatory requirements on market participants both domestically and internationally, in an effort to strengthen the financial system and mitigate the potential for future crisis. In response, firms have been working to keep pace with the rapidly changing regulatory landscape as well as seeking better ways to comply with both new and existing mandates. As a result, many financial institutions have a greater need and desire to optimize the use of their limited resources by leveraging technology to develop compliance programs that are more effective, efficient, and risk-based.

The emergence and mainstream adoption of innovative technologies in recent years has also played a role in the rise of RegTech. Compliance functions now have the potential to be streamlined using a variety of technologies, such as artificial intelligence (AI)¹¹, natural language processing¹², big data and advanced analytics¹³, cloud-based computing¹⁴, robotics process automation¹⁵, distributed ledger technology¹⁶, application program interfaces (APIs)¹⁷ and biometrics¹⁸. These technologies present great opportunities for firms to develop and use applications that may enhance existing compliance at reduced costs. Moreover, the utilization of these technologies may also offer unique opportunities to enhance the integration of risk-management and compliance within the operations of an enterprise.¹⁹

II. RegTech Applications in the Securities Industry

Securities market participants are exploring and using a variety of RegTech tools to enhance their regulatory compliance efforts. This section examines the utilization of RegTech tools in five main areas: surveillance and monitoring, customer identification and AML compliance, regulatory intelligence, reporting and risk management, and investor risk assessment. As RegTech tools are used to bolster the effectiveness and efficiency of compliance programs in these areas, it is likely that market participants may encounter new operational challenges and regulatory considerations. In addressing these challenges, broker-dealers may wish to consider both the benefits and risks associated with any specific tool and consider steps to mitigate risks where applicable.

Surveillance and Monitoring

Based on discussions held by FINRA staff with various broker-dealers and other participants in RegTech, surveillance and monitoring is an area where RegTech is gaining substantial traction. For purposes of this paper, the area of surveillance and monitoring applies broadly to market surveillance and conduct monitoring, such as monitoring traders, registered representatives, employees, and customers for regulatory purposes.

Market participants have indicated that they are investing significant resources in this area, primarily in RegTech tools that seek to utilize cloud computing, big data analytics or AI/machine learning to obtain more accurate alerts and enhance compliance and supervisory staff efficiencies. Several market participants have noted significant reductions in false alerts generated by surveillance systems after utilizing RegTech tools.

Market participants have indicated that they are investing significant resources in this area, primarily in RegTech tools that seek to utilize cloud computing, big data analytics or AI/machine learning to obtain more accurate alerts and enhance compliance and supervisory staff efficiencies.

RegTech tools generally aim to move beyond traditional rule-based systems to a predictive risk-based surveillance model that identifies and exploits patterns in data to inform decision-making. For example, computer programs trained with historical data may be used to look for suspicious patterns and trends in current data, or identify future patterns and trends. These programs also generally learn from periodically or continuously incorporating new data through a feedback process that seeks to refine future alerts.

Certain RegTech tools also potentially allow a greater volume and variety of information to be readily reviewed and thereby may help to enhance the operation of a firm's regulatory compliance program. Specifically, vendors have started offering tools to record, monitor and analyze various forms of communications (*e.g.*, audio, video and digital). These tools offer firms the ability to move from sample-based reviews of communications to potentially surveil and review all relevant communications. In addition, market participants have indicated that RegTech tools afford them the opportunity to potentially move beyond a traditional lexicon-based review focused on specific terms and instead move towards a more risk-based review utilizing processes such as natural language processing and machine learning to help identify patterns or anomalies. Some tools also claim the ability to understand multiple languages and decipher slang, tone, code language, and "emotional words" denoting a strong reaction. As these tools are still in early stages of development and adoption, many firms are running newer RegTech surveillance tools in parallel with their traditional tools and supplementing these automations with human reviews to validate their effectiveness.

Some RegTech tools that seek to employ a more predictive risk-based surveillance model also focus on linking data streams previously viewed largely in isolation. For instance, the relationship between certain structured data (such as trade orders and cancels, market data, and customer portfolio) and unstructured data (such as emails, voice recordings, social media profiles and others communications) have historically been difficult to link together. However, RegTech tools are being developed that would help to integrate these disparate data forms and then identify and track related anomalies that merit attention.

Customer Identification and AML Compliance

Another compliance program area where there has been greater interest in the adoption of RegTech tools involves customer identification (also known as "know-your-customer" or KYC) and AML programs.²⁰

Customer identification and AML related rules and regulations are critical to legitimate and orderly conduct of financial markets. They allow market participants and regulators to identify and detect potential money laundering and terrorist financing activities, and other offences such as securities fraud and market manipulation. However, customer identification and AML compliance also come with associated costs.

Moreover, anecdotal statements by market participants suggest that traditional solutions and methods for customer identification and AML monitoring may, at times, have not been as effective as desired. The financial industry is exploring the use of RegTech tools as it looks for more effective solutions.

RegTech startups and various incumbent firms have started introducing solutions for customer identification and AML that are designed to employ technology to develop more effective, efficient, and risk-based systems. For example, some vendors are offering RegTech tools that incorporate the use of biometrics to more effectively identify and track customer activity. Other vendors are exploring the use of distributed ledger technology to reduce the burdens associated with individual financial institutions each separately identifying or monitoring the same customers.²¹ Some market participants are also seeking to combine data obtained directly from customers with data from external sources, and then processing this data using sophisticated data analytics to create a more holistic view of the customer. Some RegTech tools also offer the potential to conduct real-time transaction monitoring.

Beyond firm-specific approaches and tools, some vendors and financial institutions are also exploring the creation of central industry utilities as shared solutions for customer identification and AML compliance. Using certain RegTech tools (such as those employing distributed ledger technology), these types of utilities may have the potential to reduce the overall compliance burden on the industry. Shared solutions in this space (operating in compliance with any data privacy requirements) also may facilitate the pooling of data from various industry participants, thereby potentially enhancing the ability to trace the relationship of transactions across firms as well as the related movement of funds.

Regulatory Intelligence

Regulatory intelligence programs refer to areas of compliance that focus on the identification and interpretation of changes to applicable rules and regulations, frequently across multiple jurisdictions, in order to update a firm's compliance operations. Given the significant resources devoted to this area, market participants have been exploring the use of RegTech tools to help streamline this process.

In their basic form, RegTech tools assisting with regulatory intelligence typically provide a catalog of regulatory requirements in a user-friendly manner, that are updated on a real-time basis with timely reminders on forthcoming changes and new enforcement actions that may alert firms to review applicable supervision and compliance operations. Vendors operating in this space have also started to use natural language processing and machine learning to read and interpret new and existing regulatory requirements and then offer a gap analysis to their clients to help identify potential deficiencies within an organization's compliance program. These RegTech tools seek to help automate at least portions of what is otherwise an extremely manual and time-consuming process under which firms track relevant regulatory changes and then determine and implement appropriate changes to their compliance programs.²²

Some regulators are also exploring and adopting RegTech to facilitate dissemination of regulatory intelligence. For example, the UK Financial Conduct Authority (FCA) and the Bank of England (BoE) have launched an initiative to make their rulebooks "machine-readable," such that they can be easily processed and interpreted by machines and incorporated into firms' regulatory intelligence systems.²³

In addition, some RegTech tools seek to embed compliance functions into the normal operations of a firm by providing a platform whereby it is necessary to review for compliance with applicable regulations before an action is even taken. For example, in the context of derivatives trading, RegTech solutions are being offered to enable firms and their traders to ensure that their trades are compliant with applicable rules and regulations (such as those related to clearing and reporting) before they are executed.

Reporting and Risk Management

Reporting and risk management programs represent another compliance area where firms are seeking to utilize RegTech tools. Solutions in this space leverage technology to develop tools to facilitate or automate processes involved in risk-data aggregation, risk metrics creation and monitoring (for enterprise risk management as well as operational risk management), and regulatory reporting. For example, to assist with risk-data aggregation or regulatory reporting, a RegTech tool may be deployed to gather and analyze information on capital and liquidity for use in internal models or to report to regulators.

Investor Risk Assessment

In order to provide appropriate investment advice to clients, firms must seek information from their clients and apply reasonable policies and procedures to determine the investor's risk appetite and tolerance, subject to any periodic updates or refinements. The development of RegTech tools to assist with investor risk assessment is a relatively small but growing space within RegTech.

These types of RegTech tools seek to leverage technological innovations (such as data aggregation and machine learning) in combination with behavioral sciences to determine an investor's risk appetite and tolerance in a more scientific manner than existing tools. For example, some tools assess an investor's risk appetite and tolerance based on an investor's performance on "games" designed to provide insights into the investor's reactions to changes in market conditions and portfolio performance. This information could be used in conjunction with an investor's stated preferences to help develop a more holistic picture of an investor. In addition, some RegTech tools monitor investor portfolios in changing market conditions and produce recommendations to better align the portfolio with the investor's risk profile.

III. Implications of RegTech for the Securities Industry

The use of RegTech offers several potential benefits while also posing potential new challenges. This section provides a brief overview of the potential benefits RegTech innovations may offer, followed by a discussion of some of the potential issues and key regulatory implications for market participants to consider when adopting emerging technologies for their compliance programs.

Potential Impact on the Securities Industry

RegTech tools and services have the potential to provide several benefits to firms, such as enhanced risk management, increased effectiveness and efficiency, and opportunities for enhanced industry collaboration. This in turn may support firms' ability to further promote compliance, resulting in potential benefits to investors and the broader securities market. Accordingly, this section summarizes below some potential benefits associated with RegTech tools.²⁴

RegTech tools and services have the potential to provide several benefits to firms, such as enhanced risk management, increased effectiveness and efficiency, and opportunities for enhanced industry collaboration.

Risk Management

RegTech tools may strengthen a firm's ability to adopt a proactive risk-based approach to regulatory compliance. For example, instead of identifying violations after they occur, RegTech tools (based on AI and big-data analytics) are being used to proactively identify potential risks by creating alerts that facilitate the development of more forward-looking compliance programs. RegTech tools are also being used to facilitate the ability of firms to look at data across the organization to conduct enterprise-level reviews, thereby helping to break down silos and limiting potential compliance gaps.

Automation, Effectiveness and Efficiency

Increased automation of compliance processes is one of the most widely used forms of RegTech and offers many potential benefits. For example, use of robotics process automation (RPA) may allow firms to minimize the need to perform repetitive tasks (such as collecting data and analyzing information across systems), thereby reducing errors and speeding up processes, freeing up resources to perform higher level functions such as reviewing alerts and developing responses.

Moreover, certain RegTech tools can be embedded within a firm's operational and supervisory processes, thereby making rule compliance part of the business process (e.g., tools that review for compliance with certain specific rules before trades are submitted for execution). This offers the ability to potentially prevent non-compliant activities before they occur, as opposed to identifying them during a post-event compliance review.

The use of certain RegTech tools could also assist in reducing the number of false alerts, thereby freeing up staff time to focus on alerts that warrant escalation. For example, during our research, one firm noted that false alerts of its employee surveillance system were reduced by 80% after the adoption of a RegTech tool and that the escalation rate of its alerts went up significantly. Such tools have the potential to result in cost efficiencies, increase productivity and focus resources on heightened areas of risk. In addition, shared RegTech solutions such as industry utilities and shared use of cloud computing platforms offer opportunities for cost reductions.

Moreover, many emerging RegTech tools offer intuitive, user-friendly interfaces with advanced graphics and interactive tools, which empower end users with non-technology backgrounds (e.g., compliance and supervisory personnel) to tap into the benefits of these advanced technologies. The end-user interface of many RegTech tools offer synthesized visualizations of complex analytics and intuitive tools for end users to extrapolate different scenarios. These attributes make it easy to train personnel in the use of these tools as well as simplify the analysis for compliance functions.

Regulatory and Implementation Considerations

As broker-dealers explore RegTech tools and services to assist with their regulatory compliance efforts, they should be cognizant of potential challenges that the adoption of these tools may pose and their regulatory implications. This section discusses some of the key implications for broker-dealers to consider. While we highlight certain key thematic areas, this section is not meant to be an exhaustive list of all potential issues. Broker-dealers should conduct their own assessments of the implications of RegTech tools and services, based on their business models and compliance needs.

We invite market participants to engage in a dialogue with FINRA as they explore various RegTech tools and services and seek to understand and address any new regulatory implications that may arise during the process. We also invite market participants to provide feedback on areas where additional guidance, resources or modifications to FINRA rules may be desired to support adoption of these tools, while maintaining investor protection and market integrity.

Supervisory Control Systems

FINRA rules require firms to maintain reasonable supervisory policies and procedures related to supervisory control systems in accordance with applicable rules (See, e.g., [FINRA Rules 3110](#) and [3120](#)). This includes having reasonable procedures and control systems in place for supervision and governance of RegTech tools, including supervision of AI-based tools and systems.

Some of the RegTech applications discussed earlier in this report may use highly complex and sophisticated AI algorithms, which are designed to learn and evolve based on data patterns. Compliance and business professionals may not have the technical skills to understand in detail how these algorithms function. Auditing the methodology or logic used by an AI-algorithm to generate a specific output or decision can be challenging. Previously, FINRA has stated with respect to the use of technology-based trading tools: "[T]he use of algorithmic strategies has increased, the potential of such strategies to adversely impact market and firm stability has likewise grown. When assessing the risk the use of algorithmic strategies creates, firms should undertake a holistic review of their trading activity and consider implementing a cross-disciplinary committee to assess and react to the evolving risks associated with algorithmic strategies."²⁵ A similar analysis may be helpful in the context of AI-algorithms used for compliance tools. A firm's written supervisory

procedures (WSPs) may benefit from being appropriately updated and tested to reflect any required changes in supervisory procedures due to the integration or adoption of new RegTech tools, particularly with respect to those that employ emerging, complex technologies.

Some potential supervisory and governance areas that broker-dealers may want to consider when adopting RegTech tools are listed below.²⁶

- ▶ **Establishing a cross-functional technology governance structure.** It may be beneficial for a cross-disciplinary group to be involved in the development, testing and implementation of RegTech tools. Testing of various scenarios and outputs generated by the tools with input from a cross-functional group may also help limit potential issues.
- ▶ **Simplified summary of the RegTech tools.** Maintaining a simplified summary describing the underlying algorithms and related strategies may enable non-technical staff to understand the intended functions of the tools and algorithms so that they are better able to assess results that do not align with expectations.
- ▶ **Data quality risk-management.** Data integrity and control is of paramount importance for many RegTech tools, particularly those that employ AI to deliver desired results. Developing an appropriate data quality risk-management program is vital to helping ensure accuracy, completeness, and consistency of the data that is used to support the RegTech systems.
- ▶ **Process to identify and address errors or malfunctions.** Firms may benefit from having appropriate policies and procedures in place to identify, respond to, and mitigate material risks that may manifest in the event errors or malfunctions arise in association with the use of a RegTech tool. This may include establishing alternative processes that can be readily employed in the event the RegTech tool fails.
- ▶ **Training of personnel.** Firms may benefit from developing appropriate training for compliance, supervisory and operational staff on the use of RegTech tools adopted by the firm.

Outsourcing Structure and Vendor Management

Given the rapid development of RegTech tools and services, many broker-dealers are choosing to outsource discrete compliance and reporting functions (*e.g.*, customer identification, AML transaction monitoring, fraud surveillance, etc.) to RegTech vendors. The use of third party vendors enables firms, especially smaller ones, to leverage the use of advanced technologies and related efficiencies, without a significant capital investment.

Firms are reminded that outsourcing an activity or function to a third-party does not relieve them of their ultimate responsibility for compliance with all applicable securities laws and regulations and FINRA rules associated with the outsourced activity or function. As such, firms may desire to adjust or update their written supervisory procedures to ensure that they appropriately address outsourcing arrangements (*see, e.g., Notice to Members 05-48* (Outsourcing)).

The following are some potential areas for broker-dealers to consider when outsourcing to RegTech vendors:

- ▶ Whether an appropriate due-diligence analysis of the vendor was conducted including, where applicable, consideration of its technical, operational and financial soundness;
- ▶ Whether the vendor understands the regulatory requirements that it offers RegTech solutions for, and has a system in place to monitor for and incorporate any changes to such regulatory requirements;

- ▶ Whether the vendor’s cybersecurity policies and procedures are appropriate, particularly when the outsourcing arrangement involves sharing of sensitive firm and customer data;
- ▶ Whether there is a need for a continuity and transition plan, in the event the vendor is unable to fulfill its obligations and the required functions need to be abruptly moved back in-house;
- ▶ To the extent the use of outsourced RegTech services leads to the creation of new records, firms may wish to consider working with vendors to develop appropriate processes to meet the firm’s recordkeeping obligations such as those associated with Exchange Act Rules 17a-3 and 17a-4 and [FINRA Rule 4511](#) (Books and Records: General Requirements).

Customer Data Privacy

Some emerging RegTech tools and services involve the collection, analysis, and sharing of customer-related information, such as in the areas of surveillance and monitoring (*e.g.*, recording of customers’ communications with registered representatives), customer identification and AML compliance (*e.g.*, sharing customer onboarding data with a vendor), or investor risk assessment tools. While these tools and data-collection methods may strengthen a firm’s ability to leverage technology and conduct compliance functions in an efficient manner, they may also pose potential risks associated with customer data privacy, particularly where customer data is shared with a third-party vendor. Broker-dealers should consider the application of customer data privacy rules when exploring such RegTech applications.

Protection of financial and personal customer information is a key responsibility and obligation of FINRA member firms. As required by [SEC Regulation S-P](#) (Privacy of Consumer Financial Information and Safeguarding of Personal Information)²⁷, broker-dealers must have written policies and procedures in place to address the protection of customer information and records. In addition, as detailed in NASD [Notice to Members 05-49](#) (Safeguarding Confidential Customer Information), the policies and procedures should be reasonably designed to:

- ▶ Ensure the security and confidentiality of customer records and information;
- ▶ Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
- ▶ Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Firms also have obligations to provide initial and annual privacy notices to customers describing information sharing policies and informing customers of their rights. In addition, SEC [Regulation S-ID](#) (the Red Flags Rule) requires broker-dealer firms that offer or maintain covered accounts to develop and implement written “Identity Theft Prevention Programs.” Moreover, there are numerous international, federal and state regulations and statutes that set forth specific rules and requirements related to customer data privacy. Many of these laws are specific to the collection and use of personal information and firms should assess the applicability of these laws to both their business and their potential use of RegTech tools.

As firms adopt RegTech tools that involve changes in how they collect, store, analyze and share sensitive customer data, they may need to update their policies and procedures related to customer data privacy to reflect such changes. Accordingly, below are some issues that firms may want to consider:

- ▶ Whether appropriate consent from customers, as needed, has been obtained with respect to the collection of new or additional information (*e.g.*, recording of audio or video communications), use of such information for internal analysis and monitoring, and sharing of any customer data with third party vendors;

- ▶ Whether appropriate policies and procedures exist with respect to sharing such data with vendors, including how and what level of access is provided to vendors; any parameters for storing the data; any restrictions on vendors sharing data with other third parties, and any restrictions on aggregating customer information with data from other vendor clients;
- ▶ Whether related training is appropriate for relevant individuals and departments who collect or have access to customer data, including registered representatives, employees of the firm, and employees of vendors.

Security Risks

Cybersecurity and data-related risks continue to remain a top area of concern in the financial services industry. Some RegTech tools are being developed specifically to address security-related risks by leveraging advanced technologies, such as blockchain, biometrics and sophisticated cryptography.²⁸ However, the increased use and integration of RegTech into compliance and regulatory systems also has the potential to introduce new vulnerabilities related to security where segmented off-line processes are moved into a more automated computer-based system.

For instance, RegTech tools may involve linking to and pulling in data from multiple internal and external sources on an ongoing basis, which could potentially lead to new sources of security risks. Similarly, working with multiple new vendors and providing them with access to a firm's systems could also potentially create new sources of risk.

Security risk management should be an integral part of the evaluation and implementation of RegTech tools by firms. Specifically, firms should pay close attention to technology governance, system change management, risk assessments, technical controls, incident response, vendor management, data loss prevention, and staff training. For additional resources on this topic, including applicable rules, guidance and FINRA's report on Cybersecurity Practices, refer to [FINRA's webpage on cybersecurity](#).

Other Regulatory and Implementation Considerations

Interoperability

Firms may wish to consider whether new RegTech tools, particularly vendor tools, are compatible with other operational and compliance systems within the firm in order to limit the potential for system errors.

Communications with the Public

To the extent RegTech solutions generate or monitor communications with the public (*e.g.*, investor risk assessment tools that may generate reports to be shared with the end client, or surveillance tools that may purport to capture and analyze social media conversations), firms should pay attention to applicable FINRA rules and guidance, such as FINRA Rule 2210 (Communications with the Public), [FINRA Regulatory Notice 17-18](#) on Social Media and Digital Communications, and [FINRA Regulatory Notice 10-06](#) on Blogs and Social Networking Websites.

Talent and Training

Firms should consider whether they have the appropriate staff, functions, and training for processes that may change with the adoption of RegTech tools. According to a Thomson Reuters²⁹ survey, financial institutions are focused on revising skill sets "with more than half (56 percent) having widened the skill set within the risk and compliance functions to accommodate developments in fintech and regtech innovation and associated digital disruption, while 15 percent of respondents reported investing specifically in specialist skills."

IV. Request for Comments

FINRA continues its efforts to foster a dialogue with the industry, including with broker-dealers, other regulators and key stakeholders, to proactively identify any potential benefits or risks that new financial technologies may present to investors, broker-dealers and the securities market. Through this process, FINRA seeks to support innovation that contributes to investor protection and market integrity.

As the securities industry continues to expend time and resources in exploring and adopting RegTech solutions, we encourage stakeholders to actively engage with FINRA on areas where additional guidance or resources may be desired to support adoption of these solutions, consistent with the principles of investor protection and market integrity.

FINRA encourages comments on this paper, including areas where guidance or modifications to FINRA rules may be desired to support adoption of RegTech tools while maintaining investor protection and market integrity.

Comments are requested by November 30, 2018. Member firms and other interested parties can submit their comments using the following methods:

- ▶ Emailing comments to pubcom@finra.org; or
- ▶ Mailing comments in hard copy to: Marcia E. Asquith Office of the Corporate Secretary FINRA
1735 K Street, NW Washington, DC 20006-1506

To help FINRA process comments more efficiently, persons should use only one method to comment on the proposal.

Important Notes: All comments received in response to this paper will be made available to the public on the FINRA website. In general, FINRA will post comments as they are received.

Direct inquiries regarding this paper to Haimera Workie, Senior Director, Office of Emerging Regulatory Issues, at (202) 728-8097; or Kavita Jain, Director, Office of Emerging Regulatory Issues, at (202) 728-8128.

Endnotes

1. This paper is not intended to express any legal position, and does not create any new requirements or suggest any change in any existing regulatory obligations, nor does it provide relief from any regulatory obligations. While this paper summarizes key findings from FINRA's outreach and research on RegTech tools developed and adopted by the securities industry, it does not endorse or validate the use or effectiveness of any of these tools in fulfilling compliance obligations. Further, while the paper highlights certain regulatory and implementation areas that broker-dealers may wish to consider as they explore RegTech tools, the paper does not cover all applicable regulatory requirements or considerations. FINRA encourages firms to conduct a comprehensive review of all applicable securities laws, rules and regulations to determine potential implications of implementing RegTech tools.
2. This paper considers the use of RegTech to support compliance within the securities industry. In this context, RegTech can be thought of as a subset of financial technology (FinTech), given the focus is on the development of technology tools in the financial industry linked to promoting regulatory compliance.
3. In June 2017, FINRA launched the Innovation Outreach Initiative to foster an ongoing dialogue with the securities industry to help FINRA better understand FinTech innovations and to provide relevant information to our members, investors, and market participants. <http://www.finra.org/newsroom/2017/finra-launches-innovation-outreach-initiative>. The development of this paper was undertaken as part of the Innovation Outreach Initiative, and is designed to more broadly share insight gained from this outreach. More information on FINRA's FinTech efforts at <http://www.finra.org/industry/fintech>.
4. In addition, FINRA staff held roundtable discussions on the application of RegTech in the securities industry, at three separate FINRA FinTech Roundtables held in San Francisco, Dallas and New York City.
5. See Request for Comments section on page 11 of this paper.
6. RegTech, Institute of International Finance, <https://www.iif.com/topics/regtech>.
7. See FINRA Handles Record Volume of Market Activity through First Six Months of 2018, FINRA (July 12, 2018), <http://www.finra.org/newsroom/2018/finra-handles-record-volume-market-activity-through-first-six-months-2018>.
8. Susannah Hammond, FinTech, RegTech, and the Role of Compliance, Thomson Reuters (December 5, 2016), <https://blogs.thomsonreuters.com/answerson/fintech-regtech-compliance>.
9. The State of RegTech, CB Insights (Sept. 2017), <https://www.cbinsights.com/research/briefing/state-of-regulatory-technology-regtech/>.
10. Strategic Analysis of RegTech: A Hundred Billion-Dollar Opportunity, Medici (April 1, 2016), <https://medici.letstalkpayments.com/research-categories/strategic-analysis-of-regtech-a-billion-dollar-opportunity>.
11. Artificial intelligence generally refers to the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, pattern recognition, and decision-making.
12. Natural language processing generally refers to the processing of a sample of human language (spoken or written) by computer programs in order to categorize and classify its contents.
13. Big data analytics generally refers to a set of tools and processes required to work with large sets of diverse data that include different types such as structured/unstructured and streaming/batch. Because of the very large volume of data, big data analytics often require new tools and processes that are different from traditional data management and processing systems.
14. Cloud computing generally refers to the offering of computing capacity as a set of services that can be rapidly provisioned and scaled up or down based on need. Hosting of Cloud services can either be self-managed (Private Cloud) or by an external vendor via the Internet (Public Cloud).
15. Robotics process automation (RPA) generally refers to software that can be easily programmed to do basic tasks across applications just as human workers do. Robotics Process Automation, Investopedia, <https://www.investopedia.com/terms/r/robotic-process-automation-rpa.asp>.
16. "Distributed ledger technology involves a distributed database maintained over a network of computers connected on a peer-to-peer basis, such that network participants can share and retain identical, cryptographically secured records in a decentralized manner." FINRA, Distributed Ledger Technology: Implications of Blockchain for the Securities Industry (Jan. 2017), <http://www.finra.org/industry/blockchain-report>.
17. An application programming interface (API) is a technology protocol that allows entities to access and retrieve information from another entity's operating system services, software libraries, or other systems, in a pre-determined manner.
18. Biometrics generally refers to "[T]he measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity." Biometrics, Merriam-Webster Dictionary, <https://www.merriam-webster.com/dictionary/biometrics>.
19. These innovative technologies also have the potential to facilitate the development of compliance checks and reviews conducted concurrent to when the business activity is undertaken, which is sometimes referred to as "in-built compliance" or "compliance by design."
20. The Bank Secrecy Act of 1970 (BSA) requires all broker-dealers to, among other things, implement compliance programs to detect and prevent money laundering. In addition, FINRA Rule 3310 (Anti-Money Laundering Compliance Program) requires all broker-dealers to develop and maintain a written AML program to comply with the requirements of the BSA. FINRA Rule 2090 (Know Your Customer (KYC)) requires broker-dealers to "use reasonable diligence, in regard to the opening and maintenance of every account, to know (and retain) the essential facts concerning every customer and concerning the authority of each person acting on behalf of such customer."

21. "A report from Quinlan & Associates estimates that blockchain technology could deliver the industry \$4.6 billion in annual AML cost savings – representing 32% of current annual costs – in the form of reduced compliance headcount, lower technology spend and fewer regulatory penalties." Building RegTech into your FinTech Strategy: Innovating to Stay Competitive in the Digital Age, FinExtra and Pegasystems (March 2017), https://www.finextra.com/finextra-downloads/surveys/documents/c015120b-5e94-4f77-b523-be59591ad72d/pega_researchpaper_v4.pdf.
22. In most cases any automation is also supplemented with human review by small teams of subject matter and technical experts.
23. UK Financial Conduct Authority, Model Driven Machine Executable Regulatory Reporting (Nov. 1, 2017), <https://www.fca.org.uk/firms/our-work-programme/model-driven-machine-executable-regulatory-reporting>.
24. Please note that FINRA does not endorse or validate the use or effectiveness of any specific tools in fulfilling compliance obligations. FINRA encourages broker-dealers to conduct a comprehensive assessment of any RegTech tools they wish to adopt to determine their benefits, implications and ability to meet their compliance needs.
25. Guidance on Effective Supervision and Control Practices for Firms Engaging in Algorithmic Trading Strategies, FINRA Regulatory Notice 15-09 (March 2015). FINRA also requires registration of associated persons involved in the design, development, or significant modification of algorithmic trading strategies. See [Regulatory Notice 16-21](#) (June 2016).
26. These are some of many possible areas that broker-dealers may wish to consider as they explore adjusting their supervisory processes. This does not express any legal position, and does not create any new requirements or suggest any change in any existing regulatory obligations, nor does it provide relief from any regulatory obligations. It is not intended to cover all applicable regulatory requirements or considerations. FINRA encourages firms to conduct a comprehensive review of all applicable securities laws, rules and regulations to determine potential implications of implementing RegTech tools.
27. [17 C.F.R. Part 248](#)
28. Cryptography refers to the security process of converting data from its ordinary form into unintelligible text such that it can be read and processed by only those it is intended for.
29. Susannah Hammond, FinTech, RegTech, and the Role of Compliance, Thomson Reuters (December 5, 2016), <https://blogs.thomsonreuters.com/answeron/fintech-regtech-compliance>.

Investor protection. Market integrity.
 1735 K Street, NW
 Washington, DC 20006-1506
www.finra.org
 © 2018 FINRA. All rights reserved.
 18_0201.1 –09/18