

## Core Cybersecurity Threats and Effective Controls for Small Firms

Sound cybersecurity practices are a key focus of member firms and FINRA, especially given the evolving nature, increasing frequency and mounting sophistication of cybersecurity attacks —as well as the potential for harm to investors, member firms, and the markets. Cybersecurity is one of the principal operational risks facing broker-dealers, and FINRA expects member firms to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations.

The following list updates and expands on the Core Cybersecurity Controls for Small Firms provided in the [Report on Selected Cybersecurity Practices – 2018](#) (2018 Report) by identifying key cybersecurity risks currently faced by small firms and helping them enhance their customer information protection, and cybersecurity written supervisory programs (WSPs) and related controls, including:

- Highlighting the most common and recent categories of cybersecurity threats faced by small firms, including questions to assist firms with addressing such threats;
- Providing a summary of effective core controls small firms should consider, as well as relevant questions for consideration to evaluate their current cybersecurity programs; and
- Including appendices with a glossary of relevant terms and additional resources.

### Contact Us

Questions related to this tool or other Cybersecurity topics can be sent to Member Supervision’s CyberTech team at [CAU@finra.org](mailto:CAU@finra.org).

### Regulatory Obligations

Rule 30 of the U.S. Securities and Exchange Commission’s (SEC) Regulation S-P requires firms to have written policies and procedures that are reasonably designed to safeguard customer records and information. FINRA Rule [4370](#) (Business Continuity Plans and Emergency Contact Information) also applies to denials of service and other interruptions to members’ operations. Cybersecurity remains one of the principal operational risks facing broker-dealers and FINRA expects firms to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations.

Technology-related problems, such as problems in firms’ change- and problem-management practices, or issues related to an increase in trading volumes, can expose firms to operational failures that may compromise their ability to comply with a range of rules and regulations, including FINRA Rules [4370](#), [3110](#) (Supervision) and [4511](#) (General Requirements), as well as Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3 and 17a-4.

## COMMON CYBERSECURITY THREATS FOR SMALL FIRMS

### 1

#### IMPOSTER WEBSITES



Reviewed



Small firms frequently report to FINRA cybersecurity risks related to imposter websites,<sup>1</sup> where fraudsters use registered representatives' names, firm information or both to establish websites that market investment services and products. These sites attempt to steal both personal information and investor funds by leading site visitors to believe that they are investing in a legitimate business or legitimate products. Firms may want to consider asking the following questions, where applicable, with respect to how they monitor for, and address, imposter websites:

- How does your firm monitor for imposter websites that may be impersonating your firm or your registered representatives?
  - Has your firm registered website name variations, including common misspellings or visually similar character substitutions?
  - Does your firm use social media or website monitoring services to watch for imposter websites?
- How does your firm address imposter websites once they are identified? If your firm becomes aware of an imposter website, has it addressed the concern with the hosting provider and domain name registrar, sought assistance from specialists and informed regulators and customers?<sup>2</sup>

### 2

#### PHISHING



Reviewed



Phishing is one of the most common cybersecurity threats affecting firms<sup>3</sup> – it may take a variety of forms, but all phishing attempts try to convince the recipient to provide information or take action. The fraudsters typically try to disguise themselves as a trustworthy entity or individual via email, instant message, phone call or other communication, where they request personally identifiable information (PII) (such as Social Security numbers, usernames, or passwords), direct the recipient to click on a malicious link, open an infected attachment or application, or attempt to initiate a fraudulent wire transfer or transaction. Firms may want to consider asking the following questions, where applicable, with respect to how they identify, prevent and mitigate phishing attempts:

- Do your firm's policies and procedures address phishing by, for example:
  - identifying phishing emails;

<sup>1</sup> See FINRA Information Notice - [4/29/19 \(Imposter Websites Impacting Member Firms\)](#) and Regulatory Notice [20-30](#) (Fraudsters Using Registered Representatives Names to Establish Imposter Websites).

<sup>2</sup> See Information Notice - [4/29/19 \(Imposter Websites Impacting Member Firms\)](#).

<sup>3</sup> See, e.g., Regulatory Notice [12-05](#) (Verification of Emailed Instructions to Transmit or Withdraw Assets From Customer Accounts); Regulatory Notice [21-30](#) (FINRA Alerts Firms to a Phishing Email Campaign Using Multiple Imposter FINRA Domain Names); Regulatory Notice [21-22](#) (FINRA Alerts Firms to Phishing Email From "FINRA Support" From the Domain Name "westour.org"); Regulatory Notice [21-20](#) (FINRA Alerts Firms to Phishing Email Using "gateway-finra.org" Domain Name); Regulatory Notice [20-27](#) (FINRA Alerts Firms to Use of Fake FINRA Domain Name); Regulatory Notice [21-08](#) (FINRA Alerts Firms to Phishing Email Using "finra-online.com" Domain Name); and Regulatory Notice [20-12](#) (FINRA Warns of Fraudulent Phishing Emails Purporting to be from FINRA)..

- clarifying that staff should not click on any links or open any attachments in phishing emails;
- requiring deletion of phishing emails;
- developing a process to securely notify Information Technology (IT) administrators or compliance staff of phishing attempts;
- confirming requests for wire transfers of a certain type, or above a certain threshold, with the customer via telephone or in person; and
- ensuring proper resolution and remediation after phishing attacks?
- Has your firm implemented email scanning and filtering to monitor and block phishing and spam communication?
- Does your firm regularly conduct phishing email campaign simulations to evaluate employee understanding and compliance of its phishing policies and procedures?

### 3

#### CUSTOMER AND FIRM EMPLOYEE ACCOUNT TAKEOVERS (ATOs)



Reviewed



Customer and firm employee email ATOs have become an increasingly problematic area for firms. ATOs can occur either at customer or firm personnel accounts and usually begin with their email account being compromised. Fraudsters can gain unauthorized access to customer and firm employee email accounts through data breaches, phishing emails or websites that trick users into clicking on malicious links allowing them to execute unauthorized transactions in financial accounts, firm systems, bank accounts and credit cards. Fraudsters can also monitor those email accounts, view or download the information contained within messages and even add new email rules to hide legitimate correspondence. In addition, some fraudsters use synthetic identities to establish accounts to divert specific types of payments, such as congressional stimulus funds or unemployment payments, or to engage in automated clearing house (ACH) or wire fraud. Firms may want to consider asking the following questions, where applicable, with respect to how they identify, prevent and mitigate ATOs impacting broker-dealers or affiliates, as well as those impacting customer accounts:

For ATOs impacting broker-dealers or affiliates:

- Does your firm require multi-factor authentication (MFA) for external access to email systems, vendor portals or other systems that may contain confidential information?
- Does your firm have automated monitoring, alerting or both for suspicious logins?
- For high-risk transactions (*e.g.*, third-party money movements) does your firm have a process to validate these requests?

For ATOs impacting customer accounts:

- What documentary identification (*e.g.*, drivers' licenses, passports) and non-documentary methods (*e.g.*, contacting the customer, obtaining a customer's financial statement) does your firm use to verify customers' identities when establishing online accounts?
- What approaches does your firm take to verify customer identities when they access their online accounts (*e.g.*, MFA, adaptive authentication) and initiate transfer requests (*e.g.*, reviewing the Internet Protocol (IP) address of requests made online or through a mobile device for consistency with past legitimate transactions)?
- How does your firm proactively address potential or reported customer ATOs? What practices has your firm implemented to restore customer account access in a secure and timely manner?
- Do your firm's Suspicious Activity Reporting (SAR) procedures address ACH or wire fraud? Does your firm collaborate with its clearing firm to allocate responsibilities for handling ACH or wire transactions?

- Does your firm educate its customers on account security? Does your firm provide resources to its customers to help them identify potential security threats (e.g., email or SMS text messages for certain types of account activity)?

## 4

### MALWARE



Reviewed



Malware is a catch-all term for multiple types of malicious software (e.g., viruses, spyware, worms) designed to cause damage to a stand-alone or networked computer. Malware most often originates from phishing emails where a user clicked on a link or opened an attachment. Once activated, it can mine a firm's system for PII and sensitive data; erase data; steal credentials; alter, corrupt or delete a firm's files and data; take over an email account; and even hijack device operations or computer-controlled hardware. Firms may want to consider asking the following questions, where applicable, with respect to how they identify, prevent and respond to malware attacks:

- How does your firm train employees to recognize and report cyberattacks involving malware?
- What preventative measures does your firm take (e.g., endpoint malware protection) to defend against malware?
- How does your firm monitor for indications of malware on your firm's systems?
- How does your firm's incident response plan address malware infections?
- How does your firm incorporate threat intelligence regarding newly-identified instances of viruses or other types of malware into its IT infrastructure?

## 5

### RANSOMWARE



Reviewed



Ransomware attacks are an increasingly common threat for small firms, and can quickly cripple their business operations, as well as expose firms to risks of data exfiltration and publication. This type of highly sophisticated malware commonly encrypts a firm's files, databases, or applications to prevent firm employees from accessing them until a ransom demand is paid to the fraudster. Firms may want to consider asking the following questions, where applicable, with respect to how they identify, prevent and respond to ransomware attacks:

- Has the firm evaluated capabilities to detect and block sophisticated attacks, using tools such as endpoint detection and response (EDR), a host-based intrusion detection system (HIDS) and a host-based intrusion prevention system (HIPS)?
- Does your firm keep offline backups of systems and data? Are recovery capabilities tested on a regular basis?
- Does your firm's incident response plan include a scenario for potential ransomware attacks? If so, does your plan address factors such as:
  - making cybersecurity insurance claims;
  - engaging cybersecurity experts to conduct forensics investigations and to assist in recovery efforts;
  - assessing and mitigating the impact of these attacks; and

- notifying affected parties (*e.g.*, customers, employees, regulators) as required by data breach notification laws applicable to your firm?

## 6

### DATA BREACHES



Reviewed



Data breaches are another serious threat to small firms that can expose sensitive customer or firm information to an unauthorized party and may result in customer harm, reputational damage to a firm, or both. If a data breach has been identified, firms must determine whether sensitive data is impacted and the various data privacy concerns, including the required notifications to regulators and customers because of the breach. Firms may want to consider asking the following questions, where applicable, with respect to how they investigate, monitor for, prevent and respond to data breaches:

- How does your firm investigate data breaches?
- Do your firm’s contracts with vendors define “breach” – in the context of data and systems the vendor is involved with – as well as address the manner and timing of the vendor’s notification to the data owner of a security breach, and the requirements as to who is responsible for notifying customers along with any related costs?
- Has your firm established a formal data loss prevention (DLP) program and applicable WSPs to monitor and prevent data breaches?
- Does your firm regularly train employees on effective practices for preventing data breaches (*e.g.*, appropriately handling customer requests for username and password changes; identifying social engineering activities from fraudsters)?
- Does your firm have a process to notify regulators and customers about data breaches?

## EFFECTIVE CORE CYBERSECURITY CONTROLS FOR SMALL FIRMS

The following are some of the effective cybersecurity controls observed at small firms they should consider, as well as relevant questions for consideration they could use to evaluate their current cybersecurity programs. In addition to the following controls, FINRA has provided a number of cybersecurity resources for small firms that provide additional information on these and other controls, including the [Cybersecurity and Technology Governance](#) section of the [2022 Report on FINRA’s Examination and Risk Monitoring Program](#), the [2015 FINRA Report on Cybersecurity Practices](#), the [2018 Report](#), [FINRA’s Small Firm Cybersecurity Checklist](#) and the [Cybersecurity Topic Page](#).

## 1

### GOVERNANCE AND RISK MANAGEMENT



Reviewed



A firm’s governance framework should enable it to become aware of relevant cybersecurity risks, estimate their severity and decide how to manage (*i.e.*, to accept, mitigate, transfer or avoid) each risk. Because there is no one-size-fits-all approach to cybersecurity, any governance framework should also include defined risk management policies, processes and structures coupled with relevant controls tailored to the nature of the cybersecurity risks the firm faces and the resources the firm has available. Firms may want to consider asking the following questions, where applicable, with respect to how they implement and maintain their cybersecurity-related governance framework and risk management policies:

- Does your firm use well-established, relevant industry frameworks<sup>4</sup> and standards to implement and maintain its cybersecurity program, including policies that are appropriate for the firm’s size, business model and cybersecurity threat environment, particularly in areas such as:
  - data protection;
  - vendor management;
  - asset management;
  - risk management;
  - incident management and responses; and
  - branch controls?
- Has your firm conducted program risk assessments that include prioritization, tracking, and follow up for all required implementation items for your cybersecurity program (*e.g.*, leveraging FINRA’s Small Firm Cybersecurity Checklist)?
- Does your firm have a Chief Information Security Officer (CISO) or otherwise designate a single staff person to lead the firm’s overall cybersecurity program, such as your firm’s Chief Compliance Officer (CCO), IT leader or another member of senior management with sufficient knowledge of cybersecurity risks and controls?
- Has your firm established conducted documented meetings or assigned accountability for action items discussed in meetings?
- Does your firm’s cybersecurity leadership engage your firm’s executive management in all risk-based decisions aligned to the overall organization’s goals and corresponding risks?

## 2

### VENDOR MANAGEMENT



Reviewed  
✓

Member firms – including small firms – have increasingly leveraged vendors to implement systems and perform key functions (*e.g.*, customer relationship management systems, clearing arrangements, account statement generation) and often contract with Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs), respectively, to oversee their IT infrastructure and cybersecurity programs. Relying on vendors may help small firms reduce operating costs, improve efficiency and concentrate on core broker-dealer operations. However, due to the recent increase in the number and sophistication of cyberattacks during the COVID-19 pandemic, FINRA reminds firms of their obligations to oversee, monitor and supervise cybersecurity programs and controls provided by third-party vendors.<sup>5</sup> Firms may want to consider asking the following questions, where applicable, with respect to how they select, conduct due diligence on and document relationships with cybersecurity vendors:

- Does your firm have a process for its decision-making on outsourcing, including the selection of cybersecurity vendors? Does this process engage key internal stakeholders and consider the impact of such outsourcing on its ability to comply with federal securities laws and regulations, and FINRA rules?

<sup>4</sup> Examples of these relevant frameworks include the [National Institute of Standards and Technology \(NIST\) Cybersecurity Framework](#), [Center For Internet Security \(CIS\): Critical Security Controls](#) and [Federal Trade Commission \(FTC\): Cybersecurity for Small Business](#).

<sup>5</sup> Firms can find relevant guidance in [Regulatory Notice 21-29](#) (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors) and the Cybersecurity and Infrastructure Security Agency’s (CISA) [Risk Considerations for Managed Service Provider Customers](#).

- Does your firm implement risk-based due diligence on vendors' cybersecurity practices critical to managing risks present in a firm's environment, including the ability to protect sensitive firm and customer non-public information?<sup>6</sup>
- Does your firm document relationships with vendors in written contracts that clearly define all parties' roles and responsibilities related to cybersecurity, such as evidencing compliance with federal and state securities laws and regulations, and FINRA rules; protection of sensitive firm and customer information; and notifications to your firm of cybersecurity events, and the vendor's efforts to remediate those events?
- Does your firm conduct independent, risk-based reviews to determine if vendors have experienced any cybersecurity events, data breaches or other security incidents? If so, does your firm evaluate the vendors' response to such events?

### 3

#### ACCESS CONTROLS



Reviewed  
✓

Small firms may face a unique set of challenges related to access controls due to their reliance on third party providers such as clearing firms, client management systems and IT services, including cloud-based providers. Third party providers may be especially appealing to small firms with fewer internal resources. However, this may result in vendor employees wearing multiple hats and having more access to systems and data than needed to fulfill their functions. Firms may want to consider asking the following questions, where applicable, with respect to how they grant access to firm and customer data, establish and enforce access and authentication controls, and detect and resolve anomalies within privileged accounts:

- Does your firm maintain WSPs in crucial areas, such as identity governance, onboarding, offboarding and periodic access reviews?
- Does your firm follow the Principle of Least Privilege when granting entitlements?
- Has your firm established identity and access management protocols for registered representatives and other staff, including managing the granting, maintenance and termination of access to firm and customer data?
- Does your firm enforce complex password standards and authentication controls (*e.g.*, MFA, password reuse, password change intervals, minimum length, character types and length, change frequency)?
- Has your firm implemented enhanced procedures (*e.g.*, monitoring, alerts) to detect anomalies in privileged accounts, such as a privileged user assigning herself or himself extra access rights, performing unauthorized work during off-hours or logging in from different geographic locations concurrently? Do your firm's procedures also account for logging the occurrence of anomalies, and how firms resolve them?
- Has your firm established physical access controls across office locations or access controls for remote work?

<sup>6</sup> See *id.*, at Section II for steps small firms can take when performing due diligence (*e.g.*, talking to industry peers; collecting and reviewing American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 reports, if available).

## 4

### DATA PROTECTION



Reviewed  
✓

Data protection is one of the most important facets of a small firm's cybersecurity program. Small firms have information assets (e.g., employee and customer information, firm sensitive data) that, if inadequately protected, could result in harm to the customers, individuals or the firm's reputation. DLP controls typically identify sensitive customer and firm data based on rules and then block or quarantine the transmission of the data whether by email, data upload or download, file transfer or other method; they can also prevent the inadvertent or malicious transmission of sensitive customer or firm information to unauthorized recipients. Firms may want to consider asking the following questions, where applicable, with respect to how they establish a formal DLP program, and applicable WSPs and controls, to protect sensitive customer and firm data:

- Has your firm identified where sensitive information is stored and transmitted?
- Has your firm established a formal DLP program and applicable WSPs to monitor and prevent data breaches?
- Does your firm regularly train employees on effective practices for preventing data breaches (e.g., appropriately handling customer requests for username and password changes; identifying social engineering activities from fraudsters)?
- How does your firm implement encryption for confidential data at rest or in transit?
- Does your firm prohibit the storage of sensitive customer or firm data in unapproved or prohibited locations (e.g., a file server, cloud provider or thumb drive transmitted without encryption)?
- What is your firm's policy regarding storing sensitive data on removable media or personal devices, as well its retention and secure disposal?
- How does the firm ensure that third parties involved in maintaining or storing sensitive information have reasonable data protection safeguards and cybersecurity controls? Are third parties' data protection responsibilities mutually agreed upon?

## 5

### TECHNICAL CONTROLS



Reviewed  
✓

Technical controls perform many critical functions, such as keeping unauthorized individuals from gaining access to a system and detecting when a security violation has occurred. However, small firms may not have sufficient resources to ensure adequate safeguards around all possible attack surfaces, especially in today's hyperconnected world and ever-changing risk landscape. Small firms can use a cybersecurity risk assessment to determine which threats are most significant for each branch and then identify and implement appropriate technical and other controls to mitigate those threats. Firms may want to consider asking the following questions, where applicable, with respect to how they assess the cybersecurity risks at each of their branches, and implement appropriate controls to mitigate those risks:

- Does your firm understand where its cybersecurity risks lie, including its technology hardware and software asset inventories?
- Do your firm's staff in cybersecurity positions have the technical skillsets to properly configure tools and applications?
- How does your firm verify that its critical and sensitive systems have adequate protection and detection controls?



- What cyber hygiene controls (*e.g.*, endpoint, MFA, email encryption, DLP) does your firm implement?
- Does your firm enable automatic patching and updating features of operating systems and other software to help maintain the latest security controls?
- Does your firm prohibit the sharing of passwords among firm staff?

## 6

### BRANCH CONTROLS



Reviewed



Overseeing IT and cybersecurity controls across a branch network can be especially challenging for small firms, including firms with independent contractor models. A branch network may present challenges for a firm' seeking to implement a consistent firm-wide cybersecurity program. Some firms may experience increased challenges if their branches may, for example, purchase their own assets, allow Bring Your Own Devices (BYOD), use nonapproved vendors, or not follow their firm's software patching and upgrade protocols. As a result, firms should evaluate whether they need to enhance their branch-focused cybersecurity measures to maintain robust cybersecurity controls and protect customer information across their organizations. Firms may want to consider asking the following questions, where applicable, with respect to how they supervise their branch network:

- What policies and procedures regarding cybersecurity and annual attestations of compliance have been established for each of your firm's branch offices?
- What cybersecurity training required when onboarding new branch locations or new staff?
- How does your firm confirm each of its branches meet firm cybersecurity standards, use firm-recommended vendors or other vendors meeting firm standards? What consequences does the firm impose (such as fines, sanctions, or termination) on branches and registered representatives engaging in repeat violations of firm standards?
- What compliance and technology support does your firm provide its branches and registered representatives implementing firm cybersecurity protocols?
- What are your firm's configuration requirements for physical security and technical controls at each branch (*e.g.*, hard drive encryption, virus protection, MFA, patching and removable storage media)? How does your firm monitor these controls? Are these controls reviewed during branch inspections or monitored through the use of automated tools?
- How does your firm confirm that each of its branches use only secure, encrypted wireless settings for office and home networks?
- If a review of one of your firm's branches identifies material deficiencies or reported material cybersecurity incidents, how does it confirm that the branch has implemented corrective action?

## 7

### INCIDENT MANAGEMENT AND RESPONSE



Reviewed



Incident response plans can help small firms address cybersecurity threats from bad actors. Developing and implementing an incident response plan may require contracting with an outside specialist but doing so may aid firms in responding to threats rapidly and effectively. Cybersecurity-related incidents may also require firms to [file a SAR with the Financial Crimes Enforcement Network \(FinCEN\)](#), as well as notify [the FBI through their Internet Crime and Complaint Center \(IC3\)](#) and the [Federal Trade Commission \(FTC\)](#). Firms may want to consider asking the following questions, where applicable, with respect to how they develop and implement their incident response plans:

- Does your firm maintain an incident response plan to identify and escalate incidents in a timely manner?
- Does your firm have the data inventory, assets inventory, and controls to assess the impact of incidents?
- Does your firm have capabilities for incident detection, containment, mitigation, and recovery either from internal resources or with help from a third party? If from a third party, have you established the relationship with defined service level agreements (SLAs)?
- What communication plans does your firm prepare for outreach to relevant stakeholders (*e.g.*, customers, regulators, law enforcement, intelligence agencies, industry information-sharing bodies) if an incident occurs?
- Do your firm's post incident reviews aim for improvements, including evaluating the incident management process, policy updates and control effectiveness?
- Have you tested the incident response plan within the past year?<sup>7</sup>
- Has the firm investigated or considered cybersecurity insurance?

## 8

### TRAINING



Reviewed  
✓

A well-trained staff is an important defense against cyberattacks. Even well-intentioned staff can become inadvertent vectors for successful cyberattacks, so effective training helps reduce the likelihood that such attacks will be successful. Firms may want to consider asking the following questions, where applicable, with respect to how they design internal cybersecurity training, what personnel they require to take the training, and how frequently they conduct and evaluate the training:

- How frequently and consistently does your firm conduct cybersecurity training? Are all individuals or third parties at the firm included in cybersecurity training? How often does your firm conduct training?
- Is your firm's training tailored to the cybersecurity risks applicable to its business? Does the training encompass a variety of methods (*e.g.*, reminder emails, online formal training, discussions of actual events)?
- Does your firm's training include simulated phishing exercises to validate employee understanding and track participation metrics? What consequences do employees face if they don't pass (*e.g.*, mandatory retraining)?
- How does your firm ensure that IT personnel are trained and kept abreast of the cybersecurity threat landscape to continuously assess the effectiveness of technical controls?
- Has your firm considered incorporating a formal or informal evaluation of the staff's understanding of and compliance with firm cybersecurity requirements into its training program?

<sup>7</sup> For additional guidance, see the [NIST Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities](#).

## Appendix 1 – Glossary

*Account Takeover (ATO)* – a form of identity theft where a fraudster uses stolen login credentials to gain unauthorized access to another individual’s online account.

*Bring Your Own Device (BYOD)* – a policy that allows firm employees to use their personal devices (e.g., computers, smartphones, tablets) to access the firm’s network.

*Data Loss Prevention (DLP)* – a set of technologies, products, and techniques that prevent end users from moving key information outside the firm’s network.

*Endpoint Detection and Response (EDR) Tools* – integrated endpoint security solutions that combine real-time continuous monitoring and collection of endpoint data with rules-based automated responses and analysis capabilities.

*Host-Based Intrusion Detection System (HIDS) and Host-Based Intrusion Prevention System (HIPS)* – software that protects computer systems from malware and other unwanted, negative activity utilizing advanced behavioral analysis and the detection capabilities of network filtering to monitor running processes, files, and registry keys within an operation system.

*Multi-Factor Authentication (MFA)* – an authentication method that requires a user to provide two or more verification factors to gain access. Verification factors include something you know (password), something you have (token), something you are (biometrics), or somewhere you are (Geolocation).

*Managed Service Providers (MSP)* – third-party companies that remotely manage a customer’s information technology (IT) infrastructure and end-user systems.

*Managed Security Service Providers (MSSP)* – providers of outsourced monitoring and management of security devices and systems, which may include security hardening, security monitoring, incident response and forensics services.

*Personally Identifiable Information (PII)* – data or information that allows the identity of an individual to be directly or indirectly inferred.

*Principle of Least Privilege* – the information security practice that any user, program or process should have the bare minimum privileges necessary to perform a function.

*Service Level Agreement (SLA)* – a contract between a service provider and a customer that identifies the types of provided services, and the standards the customer expects the service provider to meet.

## Appendix 2 – Additional Resources

### FINRA

#### Guidance

- *Regulatory Notice [21-29](#)* (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors)
- *Regulatory Notice [21-18](#)* (FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts)
- *Regulatory Notice [20-30](#)* (Fraudsters Using Registered Representatives Names to Establish Imposter Websites)
- *Regulatory Notice [20-13](#)* (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic)
- *Regulatory Notice [12-05](#)* (Verification of Emailed Instructions to Transmit or Withdraw Assets From Customer Accounts)

#### Reports

- [2022](#) Report on FINRA’s Examination and Risk Monitoring Program – [Cybersecurity and Technology Governance](#)
- [Report on Selected Cybersecurity Practices – 2018](#)
- [Report on Cybersecurity Practices – 2015](#)

#### Compliance Tools and Other Resources

- [Compliance Vendor Directory](#)
- [Cybersecurity Topic Page](#)
- [Firm Checklist for Compromised Accounts](#)
- [Small Firm Cybersecurity Checklist](#)

#### **Non-FINRA Resources**

- [CIS: Critical Security Controls](#)
- [FBI: Internet Crime and Complaint Center \(IC3\)](#)
- [FinCEN: SAR Filing Instructions](#)
- [FTC: Cybersecurity for Small Business](#)
- [FTC: ReportFraud.ftc.gov](#)
- [NIST: Cybersecurity Framework](#)
- [NIST: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities](#)

## FINRA Compliance Tool Disclaimer

This optional tool is provided to assist member firms in fulfilling their regulatory obligations. This tool is provided as a starting point, and you must tailor this tool to reflect the size and needs of your firm. Using this tool does not guarantee compliance with or create any safe harbor with respect to FINRA rules, the federal securities laws or state laws, or other applicable federal or state regulatory requirements. This tool does not create any new legal or regulatory obligations for firms or other entities.

**Updates** – This tool was last reviewed and updated, as needed, on February 21, 2024. This tool does not reflect any regulatory changes since that date. FINRA periodically reviews and update these tools. FINRA reminds member firms to stay apprised of new or amended laws, rules and regulations, and update their WSPs and compliance programs on an ongoing basis.

Member firms seeking additional guidance on certain regulatory obligations should review the relevant FINRA [Topic Pages](#), including the [Cybersecurity Topic Page](#).

**Staff Contact(s)** – FINRA's Office of General Counsel (OGC) staff provides broker-dealers, attorneys, registered representatives, investors and other interested parties with interpretative guidance relating to FINRA's rules. Please see [Interpreting the Rules](#) for more information.

OGC staff contacts:

[Phil Shaikun](#)

[Carrie Jordan](#)

FINRA, OGC

1700 K Street, NW

Washington, DC 20006

(202) 728-8000