Appendix 1—Ransomware Controls

Firms have implemented the following technical controls to address ransomware risks relevant for their operations, customer base and technology infrastructure. FINRA expects firms to develop and maintain reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations; however, there should be no inference that FINRA requires firms to implement any specific practices described in this *Notice*.

Control	Description
Adaptive Monitoring and Tagging	Ongoing monitoring and adaptive technology include active tagging of workloads, threat hunting, virus assessments and consistent evaluation of traffic for mission-critical applications, data or services.
Advertisement Blocks	Blocking advertisement pop-ups on all devices and browsers via extensions to address risks relating to malicious advertisements.
Anti-Ransomware Software Updates	Consistent updating of network software to address emerging ransomware risks, including updating existing intrusion detection and prevention system (IDPS), antivirus and anti-malware.
Anti-Spam Filter	Effective spam filters block malicious emails sent to firm employees. Content based dynamic spam filters offer protection against new and emerging spam techniques.
Bring-Your-Own-Device (BYOD) Policy	A BYOD policy allows firm employees to use their personal devices (*e.g.,* computers, smartphones, tablets) to access the firm's network, such as enterprise mobility management.
Cloud Access Security Broker (CASB)	CASBs help manage policy enforcement for firms' cloud infrastructure and provide added visibility, compliance, data security and threat protection in securing firms' data.
Data Loss Prevention (DLP)	A set of technologies, products, and techniques that prevent end users from moving key information outside the firm's network.
Desktop Extensions	Blocking extensions protects firms' authentication of usernames and passwords, prevents web browsing activity trackers and limits malicious messages that may be added into frequently visited web pages. Extensions may include third-party applications hosted in the cloud that are "watching" trade activities and may conduct identity theft and, as a result, induce trade transactions that may appear as insider trading. Displaying extensions and training staff not to open executable files with a ".exe" extension may also mitigate this threat.

Email Gateway	Updating secure web gateway helps firms monitor email attachments, websites and files for malware and provides visibility into potential attacks.
Endpoint Detection and Response Tools	Integrated endpoint security solutions that combine real-time continuous monitoring and collection of endpoint data with rules-based automated responses and analysis capabilities.
Executable File Blocks	Preventing all ".exe" files from launching until they have been quarantined and deemed safe helps address risks relating to executable files on the internet, which may include malicious executable code, trojans and viruses that can lock down firms' networks.
Forensic Analysis	After any detection of ransomware, investigations include its entry point and time in the environment, as well as confirming that it has been fully removed from all network devices.
Host-Based Intrusion Detection System and Host-Based Intrusion Prevention System	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.
Inventory Tools	Inventory tools help firms identify their most valuable assets or network segments, understand how bad actors could infiltrate firm networks, provide visibility into traffic flows and identify what segments need added protection or restrictions.
JavaScript File Blocks	Disabling Windows Script Host and reviewing all readme.txt., .exe and .zip files on a regular basis prevents ransomware from infecting all internal brokerage and third-party order entry and clearing systems.
Managed Service Providers	Third-party companies that remotely manage a customer's IT infrastructure and end-user systems.
Multi-factor Authentication (MFA)	An authentication method that requires a user to provide two or more verification factors to gain access, such as something you know (*e.g.,* password), something you have (*e.g.,* token), something you are (*e.g.,* biometrics) or somewhere you are (*e.g.,* geolocation).

Microsegmentation	Strict policies at the application level, segmentation gateways and next generation firewalls (NGFWs) can prevent ransomware from reaching firms' most sensitive systems or data.
Patching	Regular software updates with the latest security patches help prevent ransomware and other cybersecurity attacks because they address the latest threats.
Ransomware as a Service (RaaS)	A service provided by experienced ransomware bad actors to other ransomware users, where the experienced actors receive compensation for developing or launching ransomware attacks developed by the operators.
Rapid Response Testing	Preparing to restore systems and data recovery quickly by pre-assigning roles and ensuring a plan is in place.
Restricted Privilege	Periodic user access reviews limit the scope of any successful ransomware attacks to the compromised user's scope of access.
Sandbox Testing	Testing new or unrecognized files using sandboxes, which provide a safe environment that is disconnected from firms' networks.
Service Level Agreement	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.
Zero Trust Approach	Zero trust architecture provides visibility and control over your network, including stopping ransomware, by helping firms prioritize assets and evaluate traffic, microsegment their users and conduct adaptive monitoring.