

**Department of State****Division of Publications**

312 Rosa L. Parks Ave., 8th Floor, Snodgrass/TN Tower

Nashville, TN 37243

Phone: 615-741-2650

Email: [publications.information@tn.gov](mailto:publications.information@tn.gov)**For Department of State Use Only**

Sequence Number: 04-04-23

Rule ID(s): 9864

File Date: 4/6/2023

Effective Date: 7/5/2023

## Rulemaking Hearing Rule(s) Filing Form

Rulemaking Hearing Rules are rules filed after and as a result of a rulemaking hearing (Tenn. Code Ann. § 4-5-205).

Pursuant to Tenn. Code Ann. § 4-5-229, any new fee or fee increase promulgated by state agency rule shall take effect on July 1, following the expiration of the ninety (90) day period as provided in § 4-5-207. This section shall not apply to rules that implement new fees or fee increases that are promulgated as emergency rules pursuant to § 4-5-208(a) and to subsequent rules that make permanent such emergency rules, as amended during the rulemaking process. In addition, this section shall not apply to state agencies that did not, during the preceding two (2) fiscal years, collect fees in an amount sufficient to pay the cost of operating the board, commission or entity in accordance with § 4-29-121(b).

<b>Agency/Board/Commission:</b>	Tennessee Department of Commerce and Insurance
<b>Division:</b>	Securities Division
<b>Contact Person:</b>	Anthony Glandorf
<b>Address:</b>	500 James Robertson Parkway, Nashville, TN
<b>Zip:</b>	37243
<b>Phone:</b>	615-253-3703
<b>Email:</b>	<a href="mailto:Anthony.glandorf@tn.gov">Anthony.glandorf@tn.gov</a>

**Revision Type (check all that apply):**☐ Amendment☐ Content based on previous emergency rule filed on \_\_\_\_\_☒ New☐ Content is identical to the emergency rule☐ Repeal

**Rule(s)** (ALL chapters and rules contained in filing must be listed here. If needed, copy and paste additional tables to accommodate multiple chapters. Please make sure that **ALL** new rule and repealed rule numbers are listed in the chart below. Please enter only **ONE** Rule Number/Rule Title per row)

Chapter Number	Chapter Title
0780-04-03	Industry Regulation
Rule Number	Rule Title
0780-04-03-.16	Cybersecurity

Chapter 0780-04-03  
Industry Regulation  
New

Rule 0780-04-03-.16 Cybersecurity is a new rule. All subsequent rules, and references thereto, are renumbered accordingly.

0780-04-03-.16 CYBERSECURITY.

(1) When used in this Rule:

- (a) "Consumer" means an individual who is a Tennessee resident and whose nonpublic information is in a registrant's possession, custody, or control.
- (b) "Cybersecurity event" means an event resulting in unauthorized access to, disruption, or misuse of an information system or any nonpublic information stored on such information system. The term "cybersecurity event" does not include:
  - 1. The unauthorized acquisition of encrypted nonpublic information if the encryption, protective process, or key is not also acquired, released, or used without authorization; or
  - 2. An event regarding which the registrant has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.
- (c) "Encrypted" means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.
- (d) "Information system" means any information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic information, as well as any specialized system such as industrial and process controls systems, telephone switching and private branch exchange systems, and environmental control systems.
- (e) "Nonpublic information" means information that is not publicly available information and is:
  - 1. Business-related information of a registrant the tampering with which, or unauthorized disclosure, access, or use of which, would cause a material adverse impact to the business, operations, or security of the registrant;
  - 2. Any information concerning a consumer which, because of name, number, personal mark, or other identifier, can be used to identify such consumer, in combination with any one or more of the following data elements:
    - (i) Social security number;
    - (ii) Driver's license number or non-driver identification card number;
    - (iii) Account, credit card, or debit card number;
    - (iv) Any security code, access code, or password that would permit access to a consumer's financial account; or
    - (v) Biometric records that would permit access to a consumer's financial account.
- (f) "Publicly available information" means any information that a registrant has a reasonable basis to believe is lawfully made available to the general public from federal, state, or local government records, widely distributed media, or disclosures to the general public that are required to be made by federal, state, or local law. There is a presumption that a registrant has a reasonable basis to believe that information is lawfully made available to the general public if the registrant has taken steps to determine:

1. That the information is of the type that is available to the general public; and
2. Whether a consumer can direct that the information not be made available to the general public and, if so, that such consumer has not done so.

(g) "Registrant" means any broker-dealer, issuer-dealer, or investment adviser registered or required to be registered pursuant to the Tennessee Securities Act of 1980 (the "Act").

(h) "Third-party service provider" means a person or business that contracts with a registrant to maintain, process, or store nonpublic information, or otherwise is permitted to access that information, through its provision of services to the registrant.

(2) Information Security Program.

(a) Implementation. Commensurate with the size and complexity of the registrant, the nature and scope of the registrant's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the registrant or in the registrant's possession, custody, or control, each registrant shall develop, implement, and maintain a comprehensive written information-security program based on the registrant's risk assessment, which shall include written policies and procedures. These written policies and procedures shall contain administrative, technical, physical safeguards, and training for the protection of the registrant's information system, all nonpublic information in its possession, custody, or control, and all nonpublic information provided to any third-party service provider by the registrant.

(b) Objectives. A registrant's information-security program shall be designed to:

1. Protect the confidentiality, integrity, and availability of nonpublic information and the security of the information system;
2. Protect against any threats or hazards to the confidentiality, integrity, or availability of nonpublic information and the information system;
3. Protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to consumers;
4. Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed for legitimate business purposes of the registrant; and
5. Manage risk through the implementation of security measures, such as:
  - (i) The placement of access controls on information systems, including controls, like multi-factor authentication, to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of nonpublic information;
  - (ii) Identification and management of data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with its relative importance to business objectives and the organization's risk strategy;
  - (iii) Restriction of access at physical locations containing nonpublic information to only authorized individuals;
  - (iv) Encryption or other appropriate means of protection of all nonpublic information during transmission over a network, and all nonpublic information stored on mobile computing or storage devices or media;
  - (v) Adoption of secure development practices for in-house developed applications utilized by the registrant and procedures for evaluating, assessing, or testing the security of the externally developed application utilized by the registrant;

- (vi) Regular testing and monitoring of systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;
  - (vii) Incorporation of audit trails within the information security program designed to detect and respond to cybersecurity events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the registrant;
  - (viii) Implementation of measures to protect against loss, destruction, or damage of nonpublic information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures;
  - (ix) Development, implementation, and maintenance of procedures for the secure disposal of nonpublic information;
  - (x) Providing personnel with regular cybersecurity awareness training;
  - (xi) Reviewing data policies of third-party vendors; or
  - (xii) Any other such measure as may be appropriate for the protection of nonpublic information.
- (c) Maintenance. The registrant must review, no less frequently than annually, and modify, as needed, its cybersecurity policies and procedures to ensure the adequacy of the security measures and the effectiveness of their implementation.

(3) Investigation of a Cybersecurity Event.

- (a) If the registrant learns or has reason to believe that a cybersecurity event has or may have occurred, the registrant, or an outside service provider designated to act on behalf of the registrant, shall conduct a prompt investigation.
- (b) The registrant or outside service provider designated to act on behalf of the registrant shall, at a minimum, determine to the fullest extent possible:
  - 1. Whether a cybersecurity event has occurred;
  - 2. The nature and scope of the cybersecurity event; and
  - 3. Any nonpublic information that may have been involved in the cybersecurity event.
- (c) If the registrant determines that a cybersecurity event has occurred, the registrant shall perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event in order to prevent further unauthorized acquisition, release, or use of nonpublic information in the registrant's possession, custody, or control.
- (d) If the registrant learns that a cybersecurity event has or may have occurred involving its third-party service provider, the registrant shall complete the requirements of this Paragraph (3) or confirm and document in writing that the third-party service provider has completed such requirements.
- (e) The registrant shall maintain records concerning all cybersecurity events for a period of at least three (3) years from the date of the cybersecurity event and shall produce those records upon request by the Division.

(4) Notification of a Cybersecurity Event.

- (a) Notification to the Division.
  - 1. Each registrant shall provide the Division with initial notice as promptly as possible, but in no event later than three (3) business days from a determination that a cybersecurity event has

occurred, if:

- (i) The registrant maintains its principal office and place of business in this state;
  - (ii) The cybersecurity event affected, or the registrant has reason to believe the cybersecurity event affected, nonpublic information possessed, maintained, or controlled by the registrant; or
  - (iii) The registrant is required to provide notice to any government agency, self-regulatory organization, or any other supervisory body pursuant to any state or federal law.
2. The initial notice to the Division shall include, in general terms:
- (i) The date of the cybersecurity event; and
  - (ii) The name and contact information of a person who is both familiar with the cybersecurity event and authorized to act on behalf of the registrant.
3. Based on the initial notice provided to the Division pursuant to Part 1. above, the Division may commence a private investigation into the cybersecurity event pursuant to T.C.A. § 48-1-118. If a private investigation is initiated, then the Division may request the following information:
- (i) A description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if applicable;
  - (ii) How the cybersecurity event was discovered;
  - (iii) Communication logs for the period beginning with the occurrence of the cybersecurity event, discovery of the cybersecurity event, and the registrant's response;
  - (iv) Whether any lost, stolen, or breached information has been recovered, and if so, how the recovery was achieved;
  - (v) The identity of the source of the cybersecurity event;
  - (vi) Whether the registrant has filed a police report or notified any regulatory, government, or law enforcement agencies, and if so, when such notification was provided;
  - (vii) A description of the specific types of information acquired without authorization;
  - (viii) The date(s) that the registrant acquired, and thereafter maintained, possession, custody, or control of the nonpublic information affected by the cybersecurity event;
  - (ix) The period during which the information system was compromised by the cybersecurity event;
  - (x) The aggregate number of consumers affected by the cybersecurity event;
  - (xi) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;
  - (xii) A description of efforts being undertaken to remediate the situation which allowed the cybersecurity event to occur;
  - (xiii) A copy of the registrant's privacy policy and a statement outlining the steps the registrant will take to investigate and notify consumers affected by the cybersecurity event; and
  - (xiv) Any other such information as the Division may request.



(b) Notification to Consumers.

1. Notification to Consumers of a cybersecurity event shall be provided in accordance with the methods and timeframes set forth in T.C.A. § 47-18-2107 and any other applicable laws.

(c) Notification Regarding Cybersecurity Events of Third-Party Service Providers.

1. In the case of a cybersecurity event involving a registrant's third-party service provider of which the registrant has become aware, the registrant shall treat such event as it would under Subparagraph (4)(a).
2. The computation of time shall begin on the first business day following the third-party service provider's notification to the registrant that a cybersecurity event has occurred, or the registrant otherwise acquires actual knowledge of the cybersecurity event.
3. Nothing in this Rule shall prevent or abrogate an agreement between a registrant and another registrant, a third-party service provider, or any other party to fulfill any of the investigation requirements imposed under Paragraph (2) or notice requirements imposed under Paragraph (3).

(5) Record Keeping. Every registrant shall maintain the following records and information:

- (a) A copy of each version of the written information security program implemented by the registrant pursuant to this Rule;
- (b) All records documenting the registrant's compliance with this Rule, including, but not limited to, documentation of the registrant's compliance with the notification requirements of Paragraph (4) of this Rule and its annual review of its information security program required by Subparagraph (c) of Paragraph (2) of this Rule; and
- (c) These records must be maintained for a period of no less than three (3) years and shall be provided to the Department upon request.

(6) Noncompliance with this Rule. Any failure by a registrant to comply with the requirements of this Rule shall constitute a dishonest and unethical practice in the securities business in violation of T.C.A. § 48-1-112(a)(2)(G).

Authority: T.C.A. §§ 48-1-102, 48-1-107, 48-1-109, 48-1-111, 48-1-112(a)(2)(G), 48-1-116, and 48-1-118.

\* If a roll-call vote was necessary, the vote by the Agency on these rulemaking hearing rules was as follows:

Board Member	Aye	No	Abstain	Absent	Signature (if required)
N/A					

I certify that this is an accurate and complete copy of rulemaking hearing rules, lawfully promulgated and adopted by the Commissioner of Commerce and Insurance on 09/01/2022, and is in compliance with the provisions of T.C.A. § 4-5-222.

I further certify the following:

Notice of Rulemaking Hearing filed with the Department of State on: 07/12/2022

Rulemaking Hearing(s) Conducted on: (add more dates). 09/01/2022

Date: Mar 17, 2023

Signature:   
Carter Lawrence (Mar 17, 2023 13:42:00)


Name of Officer: Carter Lawrence

Title of Officer: Commissioner

Agency/Board/Commission: Tennessee Department of Commerce and Insurance

Rule Chapter Number(s): 0780-04-03

All rulemaking hearing rules provided for herein have been examined by the Attorney General and Reporter of the State of Tennessee and are approved as to legality pursuant to the provisions of the Administrative Procedures Act, Tennessee Code Annotated, Title 4, Chapter 5.

  
Jonathan Skrmetti  
Attorney General and Reporter

March 28, 2023  
Date

**Department of State Use Only**

Filed with the Department of State on: 4/6/2023

Effective on: 7/5/2023

**RECEIVED**

Apr 06 2023, 2:17 pm

Secretary of State  
Division of Publications

  
Tre Hargett  
Secretary of State

### **Public Hearing Comments**

One copy of a document that satisfies T.C.A. § 4-5-222 must accompany the filing.

No public comments were received for this rulemaking.



## Regulatory Flexibility Addendum

Pursuant to T.C.A. §§ 4-5-401 through 4-5-404, prior to initiating the rule making process, all agencies shall conduct a review of whether a proposed rule or rule affects small business.

The analysis set forth by T.C.A. § 4-5-402(b) is as follows:

1. The type or types of small business and an identification and estimate of the number of small businesses subject to the rule being proposed that would bear the cost of, or directly benefit from the rule being proposed;

This rule affects state registered broker-dealers and investment advisers. The effect of the rule will be different on different sized firms. The complexity of the cybersecurity program will vary based on the size and complexity of the operations of the firm. The rule is estimated to impact two to three hundred small businesses.

2. The projected reporting, recordkeeping and other administrative costs required for compliance with the rule being proposed, including the type of professional skills necessary for preparation of the report or record;

This rule requires state registered broker-dealers and investment advisers to develop and implement risk management procedures surrounding cybersecurity. The firms are required to annually review their program and make adjustments when necessary. The rule also requires firms to report any cybersecurity attacks or intrusions to the Division.

3. A statement of the probable effect on impacted small businesses and consumers;

Small businesses may be affected according to the size and complexity of the cybersecurity program initiative. Consumers whose nonpublic information is in the possession of broker-dealers and investment advisers would also benefit from added protections for their nonpublic information.

4. A description of any less burdensome, less intrusive or less costly alternative methods of achieving the purpose and objectives of the rule being proposed that may exist, and to what extent the alternative means might be less burdensome to small business;

As a cybersecurity program will be developed by each firm, any less burdensome or costly alternative will be borne by the firm. As the complexity needed for each program will vary with the size and complexity of the firm operations, there is no less intrusive or burdensome method way to implement this rule.

5. A comparison of the rule being proposed with any federal or state counterparts; and

The Securities and Exchange Commission's ("SEC") Regulation S-P Rule 30 requires firms to have written policies and procedures that are reasonably designed to safeguard customer records and information. The Financial Industry Regulatory Authority ("FINRA") Rule 4370 also applies to denials of service and other interruptions to members' operations. The North American Securities Administrators Association ("NASAA") has written a cybersecurity model rule and has encouraged states to adopt it. The model rule has been adopted by six states, Arkansas, Montana, Nebraska, Oklahoma, South Carolina, and Virginia. Washington, D.C. has also adopted the rule, and another eight states have adopted substantially similar requirements. This rule includes provisions and standards that are substantially similar to those found in the NASAA model rule and also establishes investigation and reporting requirements for broker-dealers and investment advisers following cybersecurity incidents.

6. Analysis of the effect of the possible exemption of small businesses from all or any part of the requirements contained in the rule being proposed.

An exemption from the rules may benefit small businesses that require a complex cybersecurity program. However, any exemption from the rule that may benefit the small firm may also be to the detriment of client privacy financial privacy interests and confidential treatment of nonpublic information. Moreover, any perceived benefit an exemption might have for a small business would be overridden by the financial risks associated with compromised confidential client information.

### **Impact on Local Governments**

Pursuant to T.C.A. §§ 4-5-220 and 4-5-228, "On any rule and regulation proposed to be promulgated, the proposing agency shall state in a simple declarative sentence, without additional comments on the merits or the policy of the rule or regulation, whether the rule or regulation may have a projected financial impact on local governments. The statement shall describe the financial impact in terms of increase in expenditures or decrease in revenues."

The proposed rule will not have an impact on local governments.

## Additional Information Required by Joint Government Operations Committee

All agencies, upon filing a rule, must also submit the following pursuant to T.C.A. § 4-5-226(i)(1).

A brief summary of the rule and a description of all relevant changes in previous regulations effectuated by such rule;

This new rule addresses the cybersecurity practices by state registered broker-dealers and investment advisers. This rule will require broker-dealers and investment advisers to implement policies and procedures as it relates information security. The purpose of this rule is to protect the confidentiality, integrity, and availability of nonpublic information in possession of broker-dealers and investment advisers and the security of their computer information systems.

As fiduciaries, broker-dealers and advisers are required to act in the best interest of their clients at all times. These firms owe their clients a duty of care and a duty of loyalty. The fiduciary obligation to the clients includes the obligation to take steps to protect client interests from being placed at risk because of the firm's inability to provide advisory services. These include steps to minimize operational and other risks that could lead to significant business disruptions or a loss or misuse of client information. Under this framework, broker-dealers and advisers today consider a number of rules and regulations, which indirectly address cybersecurity. As discussed above, cybersecurity incidents can lead to significant business disruptions, including lapses in communication or the inability to place trades orders. In addition, these disruptions can lead to the loss of access to accounts or investments, potentially resulting in the loss or theft of data or assets. Thus, broker-dealers and advisers should take steps to minimize cybersecurity risks in accordance with their fiduciary obligations.

Broker-dealers and advisers play critical roles in our financial markets and increasingly depend on technology for key business operations. The businesses are exposed to, and rely on, a broad array of interconnected systems and networks, both directly and through service providers such as custodians, pricing services, and other technology vendors. Advisers also increasingly use digital engagement tools and other technology to engage with clients and develop and provide investment advice. As a result, they face numerous cybersecurity risks and may experience cybersecurity incidents that can cause, or be exacerbated by, critical system or process failures. (see Note 1) At the same time, cyber threat actors have grown more sophisticated and may target broker-dealers and advisers, putting them at risk of suffering significant financial, operational, legal, and reputational harm. (see Note 2) Cybersecurity incidents affecting these businesses also can cause substantial harm to their clients. For example, cybersecurity incidents caused by malicious software (also known as malware) can cause the loss of adviser or client data. Cybersecurity incidents can prevent an adviser from executing its investment strategy or an adviser or client from accessing an account, which can lead to financial losses for clients. In addition, cybersecurity incidents can lead to the theft of intellectual property, confidential or proprietary information, or client assets.

Note 1: See, e.g., Financial Services Information Sharing and Analysis Center, Navigating Cyber 2021 (Mar. 2021), available at <https://www.fsisac.com/navigatingcyber2021-report> (detailing cyber threats that emerged in 2020 and predictions for 2021).

Note 2: See, e.g., Federal Bureau of Investigation, 2020 Internet Crime Report (Mar. 17, 2021), at 5, available at [https://www.ic3.gov/Media/PDF/AnnualReport/2020\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf) ("FBI 2020 Internet Crime Report") (noting the FBI's Internet Crime Complaint Center received more than 791,790 complaints in 2020)

A citation to and brief description of any federal law or regulation or any state law or regulation mandating promulgation of such rule or establishing guidelines relevant thereto;

There is no federal law or regulation or any state law or regulation mandating promulgation of such rule or establishing guidelines relevant thereto. However, the Securities and Exchange Commission's ("SEC") Regulation S-P Rule 30 requires firms to have written policies and procedures that are reasonably designed to safeguard customer records and information. Further, T.C.A. § 48-1-112(a)(2)(G) authorizes the Commissioner to deny, suspend, or revoke the registration of any state registered broker-dealer or investment adviser who has engaged in any dishonest or unethical practice in the securities business, and T.C.A. § 48-1-116 empowers the Commissioner to promulgate rules, such as the present Rule, to carry out the purposes of the Tennessee Securities Act. Consequently, the Commissioner has determined that the failure of any registered broker-dealer or investment adviser to maintain reasonable policies and procedures to protect customer records and information constitutes a dishonest and unethical practice in the securities business in violation of T.C.A. § 48-1-112.

In addition, T.C.A. § 48-1-115 authorizes the Commissioner to participate in the North American Securities

Administration Association (NASAA) to the extent the Commissioner deems participation as being in the public interest and necessary for the protection of investors. Tennessee is currently a state member of NASAA. On May 19, 2019, NASAA members adopted a model rule for cybersecurity stating that the rule "seeks to highlight the importance of data privacy and security in our financial markets along with the related need for investment advisers to have information security policies and procedures." Further, NASAA indicated that the [rulemaking] package also provides a basic structure for how state-registered investment advisers may design their information security policies and procedures, which we expect to create uniformity in both state regulation and state-registered investment adviser practices." This rule includes provisions and standards that are substantially similar to those found in the NASAA model rule and also establishes investigation and reporting requirements for broker-dealers and investment advisers following cybersecurity incidents.

Identification of persons, organizations, corporations or governmental entities most directly affected by this rule, and whether those persons, organizations, corporations or governmental entities urge adoption or rejection of this rule;

This rule directly affects all broker-dealers and investment advisers registered or required to be registered pursuant to the Tennessee Securities Act of 1980. This rule will also affect any Tennessee consumer who utilizes the services of a broker-dealer or investment adviser registered or required to be registered under the Act by way of being afforded the cybersecurity protections mandated.

Identification of any opinions of the attorney general and reporter or any judicial ruling that directly relates to the rule or the necessity to promulgate the rule;

The Department is not aware of any opinions of the attorney general and reporter or any judicial ruling that directly relates to the rule or the necessity to promulgate the rule.

An estimate of the probable increase or decrease in state and local government revenues and expenditures, if any, resulting from the promulgation of this rule, and assumptions and reasoning upon which the estimate is based. An agency shall not state that the fiscal impact is minimal if the fiscal impact is more than two percent (2%) of the agency's annual budget or five hundred thousand dollars (\$500,000), whichever is less;

This proposed rule will have a minimal fiscal impact on state revenues and expenditures; local government revenues and expenditures would not be impacted.

Identification of the appropriate agency representative or representatives, possessing substantial knowledge and understanding of the rule;

Elizabeth Bowling, Assistant Commissioner  
Anthony Glandorf, Chief Counsel for Securities and FSIU Litigation

Identification of the appropriate agency representative or representatives who will explain the rule at scheduled meeting of the committees;

Elizabeth Bowling, Assistant Commissioner  
Anthony Glandorf, Chief Counsel for Securities and FSIU Litigation

Office address, telephone number, and email address of the agency representative or representatives who will explain the rule at a scheduled meeting of the committees; and

500 James Robertson Parkway, Nashville, TN 37243; Elizabeth Bowling: 615-770-0088; Anthony Glandorf: 615-253-3703; [Elizabeth.Bowling@tn.gov](mailto:Elizabeth.Bowling@tn.gov); [Anthony.Glandorf@tn.gov](mailto:Anthony.Glandorf@tn.gov)

Any additional information relevant to the rule proposed for continuation that the committee requests;

None Known.



**COMMERCE AND INSURANCE**  
**DIVISION OF SECURITIES**  
**INDUSTRY REGULATION**

0780-04-03-.16 CYBERSECURITY

(1) When used in this Rule:

- (a) "Consumer" means an individual who is a Tennessee resident and whose nonpublic information is in a registrant's possession, custody, or control.
- (b) "Cybersecurity event" means an event resulting in unauthorized access to, disruption, or misuse of an information system or any nonpublic information stored on such information system. The term "cybersecurity event" does not include:
  - 1. The unauthorized acquisition of encrypted nonpublic information if the encryption, protective process, or key is not also acquired, released, or used without authorization; or
  - 2. An event regarding which the registrant has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.
- (c) "Encrypted" means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.
- (d) "Information system" means any information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic information, as well as any specialized system such as industrial and process controls systems, telephone switching and private branch exchange systems, and environmental control systems.
- (e) "Nonpublic information" means information that is not publicly available information and is:
  - 1. Business-related information of a registrant the tampering with which, or unauthorized disclosure, access, or use of which, would cause a material adverse impact to the business, operations, or security of the registrant;
  - 2. Any information concerning a consumer which, because of name, number, personal mark, or other identifier, can be used to identify such consumer, in combination with any one or more of the following data elements:
    - (i) Social security number;
    - (ii) Driver's license number or non-driver identification card number;
    - (iii) Account, credit card, or debit card number;
    - (iv) Any security code, access code, or password that would permit access to a consumer's financial account; or

(v) Biometric records that would permit access to a consumer's financial account.

(f) "Publicly available information" means any information that a registrant has a reasonable basis to believe is lawfully made available to the general public from federal, state, or local government records, widely distributed media, or disclosures to the general public that are required to be made by federal, state, or local law. There is a presumption that a registrant has a reasonable basis to believe that information is lawfully made available to the general public if the registrant has taken steps to determine:

1. That the information is of the type that is available to the general public; and
2. Whether a consumer can direct that the information not be made available to the general public and, if so, that such consumer has not done so.

(g) "Registrant" means any broker-dealer, issuer-dealer, or investment adviser registered or required to be registered pursuant to the Tennessee Securities Act of 1980 (the "Act").

(h) "Third-party service provider" means a person or business that contracts with a registrant to maintain, process, or store nonpublic information, or otherwise is permitted to access that information, through its provision of services to the registrant.

(2) Information Security Program.

(a) Implementation. Commensurate with the size and complexity of the registrant, the nature and scope of the registrant's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the registrant or in the registrant's possession, custody, or control, each registrant shall develop, implement, and maintain a comprehensive written information-security program based on the registrant's risk assessment, which shall include written policies and procedures. These written policies and procedures shall contain administrative, technical, physical safeguards, and training for the protection of the registrant's information system, all nonpublic information in its possession, custody, or control, and all nonpublic information provided to any third-party service provider by the registrant.

(b) Objectives. A registrant's information-security program shall be designed to:

1. Protect the confidentiality, integrity, and availability of nonpublic information and the security of the information system;
2. Protect against any threats or hazards to the confidentiality, integrity, or availability of nonpublic information and the information system;
3. Protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to consumers;
4. Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed for legitimate business purposes of the registrant; and
5. Manage risk through the implementation of security measures, such as:

(i) The placement of access controls on information systems, including controls, like multi-factor authentication, to authenticate and permit



access only to authorized individuals to protect against the unauthorized acquisition of nonpublic information;

- (ii) Identification and management of data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with its relative importance to business objectives and the organization's risk strategy;
- (iii) Restriction of access at physical locations containing nonpublic information to only authorized individuals;
- (iv) Encryption or other appropriate means of protection of all nonpublic information during transmission over a network, and all nonpublic information stored on mobile computing or storage devices or media;
- (v) Adoption of secure development practices for in-house developed applications utilized by the registrant and procedures for evaluating, assessing, or testing the security of the externally developed application utilized by the registrant;
- (vi) Regular testing and monitoring of systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;
- (vii) Incorporation of audit trails within the information security program designed to detect and respond to cybersecurity events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the registrant;
- (viii) Implementation of measures to protect against loss, destruction, or damage of nonpublic information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures;
- (ix) Development, implementation, and maintenance of procedures for the secure disposal of nonpublic information;
- (x) Providing personnel with regular cybersecurity awareness training;
- (xi) Reviewing data policies of third-party vendors; or
- (xii) Any other such measure as may be appropriate for the protection of nonpublic information.

- (c) Maintenance. The registrant must review, no less frequently than annually, and modify, as needed, its cybersecurity policies and procedures to ensure the adequacy of the security measures and the effectiveness of their implementation.

### (3) Investigation of a Cybersecurity Event.

- (a) If the registrant learns or has reason to believe that a cybersecurity event has or may have occurred, the registrant, or an outside service provider designated to act on behalf of the registrant, shall conduct a prompt investigation.
- (b) The registrant or outside service provider designated to act on behalf of the registrant shall, at a minimum, determine to the fullest extent possible:

1. Whether a cybersecurity event has occurred;
2. The nature and scope of the cybersecurity event; and
3. Any nonpublic information that may have been involved in the cybersecurity event.

- (c) If the registrant determines that a cybersecurity event has occurred, the registrant shall perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event in order to prevent further unauthorized acquisition, release, or use of nonpublic information in the registrant's possession, custody, or control.
- (d) If the registrant learns that a cybersecurity event has or may have occurred involving its third-party service provider, the registrant shall complete the requirements of this Paragraph (3) or confirm and document in writing that the third-party service provider has completed such requirements.
- (e) The registrant shall maintain records concerning all cybersecurity events for a period of at least three (3) years from the date of the cybersecurity event and shall produce those records upon request by the Division.

#### (4) Notification of a Cybersecurity Event.

##### (a) Notification to the Division.

1. Each registrant shall provide the Division with initial notice as promptly as possible, but in no event later than three (3) business days from a determination that a cybersecurity event has occurred, if:
  - (i) The registrant maintains its principal office and place of business in this state;
  - (ii) The cybersecurity event affected, or the registrant has reason to believe the cybersecurity event affected, nonpublic information possessed, maintained, or controlled by the registrant; or
  - (iii) The registrant is required to provide notice to any government agency, self-regulatory organization, or any other supervisory body pursuant to any state or federal law.
2. The initial notice to the Division shall include, in general terms:
  - (i) The date of the cybersecurity event; and
  - (ii) The name and contact information of a person who is both familiar with the cybersecurity event and authorized to act on behalf of the registrant.
3. Based on the initial notice provided to the Division pursuant to Part 1. above, the Division may commence a private investigation into the cybersecurity event pursuant to T.C.A. § 48-1-118. If a private investigation is initiated, then the Division may request the following information:

- (i) A description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if applicable;
- (ii) How the cybersecurity event was discovered;
- (iii) Communication logs for the period beginning with the occurrence of the cybersecurity event, discovery of the cybersecurity event, and the registrant's response;
- (iv) Whether any lost, stolen, or breached information has been recovered, and if so, how the recovery was achieved;
- (v) The identity of the source of the cybersecurity event;
- (vi) Whether the registrant has filed a police report or notified any regulatory, government, or law enforcement agencies, and if so, when such notification was provided;
- (vii) A description of the specific types of information acquired without authorization;
- (viii) The date(s) that the registrant acquired, and thereafter maintained, possession, custody, or control of the nonpublic information affected by the cybersecurity event;
- (ix) The period during which the information system was compromised by the cybersecurity event;
- (x) The aggregate number of consumers affected by the cybersecurity event;
- (xi) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;
- (xii) A description of efforts being undertaken to remediate the situation which allowed the cybersecurity event to occur;
- (xiii) A copy of the registrant's privacy policy and a statement outlining the steps the registrant will take to investigate and notify consumers affected by the cybersecurity event; and
- (xiv) Any other such information as the Division may request.

(b) Notification to Consumers.

1. Notification to Consumers of a cybersecurity event shall be provided in accordance with the methods and timeframes set forth in T.C.A. § 47-18-2107 and any other applicable laws.

(c) Notification Regarding Cybersecurity Events of Third-Party Service Providers.

1. In the case of a cybersecurity event involving a registrant's third-party service provider of which the registrant has become aware, the registrant shall treat such event as it would under Subparagraph (4)(a).
2. The computation of time shall begin on the first business day following the third-party service provider's notification to the registrant that a cybersecurity event has occurred, or the registrant otherwise acquires actual knowledge of the cybersecurity event.
3. Nothing in this Rule shall prevent or abrogate an agreement between a registrant and another registrant, a third-party service provider, or any other party to fulfill any of the investigation requirements imposed under Paragraph (2) or notice requirements imposed under Paragraph (3).

(5) Record Keeping. Every registrant shall maintain the following records and information:

- (a) A copy of each version of the written information security program implemented by the registrant pursuant to this Rule;
- (b) All records documenting the registrant's compliance with this Rule, including, but not limited to, documentation of the registrant's compliance with the notification requirements of Paragraph (4) of this Rule and its annual review of its information security program required by Subparagraph (c) of Paragraph (2) of this Rule; and
- (c) These records must be maintained for a period of no less than three (3) years and shall be provided to the Department upon request.

(6) Noncompliance with this Rule. Any failure by a registrant to comply with the requirements of this Rule shall constitute a dishonest and unethical practice in the securities business in violation of T.C.A. § 48-1-112(a)(2)(G).

Authority: T.C.A. §§ 48-1-102, 48-1-107, 48-1-109, 48-1-111, 48-1-112(a)(2)(G), 48-1-116, and 48-1-118.