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

For Department of State Use Only

Sequence Number: 07-09-22
Notice ID(s): 3513
File Date: 7/12/2022

Notice of Rulemaking Hearing

Hearings will be conducted in the manner prescribed by the Uniform Administrative Procedures Act, T.C.A. § 4-5-204. For questions and copies of the notice, contact the person listed below.

Agency/Board/Commission:	Tennessee Department of Commerce and Insurance
Division:	Tennessee Securities Division
Contact Person:	Jacob Strait
Address:	500 James Robertson Parkway, Nashville, TN 37243
Phone:	615-253-0646
Email:	Jacob.Strait@tn.gov

Any Individuals with disabilities who wish to participate in these proceedings (to review these filings) and may require aid to facilitate such participation should contact the following at least 10 days prior to the hearing:

ADA Contact:	Don Coleman
Address:	500 James Robertson Parkway, Nashville, TN 37243
Phone:	615-741-6500
Email:	Don.Coleman@tn.gov

Hearing Location(s) (for additional locations, copy and paste table)

Address 1:	500 James Robertson Parkway		
Address 2:	Room 1A		
City:	Nashville		
Zip:	37243		
Hearing Date:	09/01/2022		
Hearing Time:	11:00am	_X_CST/CDT ___EST/EDT	

Additional Hearing Information:

Revision Type (check all that apply):

__ Amendment
X New
__ 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 Please make sure that **ALL** new rule and repealed rule numbers are listed in the chart below.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.

(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 shall be provided in accordance with 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.

I certify that the information included in this filing is an accurate and complete representation of the intent and scope of rulemaking proposed by the agency.

Date: 07/12/2022

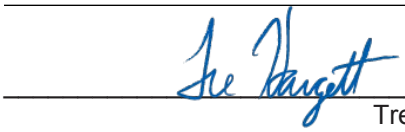
Signature: 

Name of Officer: Jacob Strait

Title of Officer: Associate General Counsel

Department of State Use Only

Filed with the Department of State on: 7/12/2022



Tre Hargett
Secretary of State

RECEIVED
JUL 12 2022
Secretary of State
Division of Publications

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 shall be provided in accordance with 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.