Title 7. Banking and Securities
Part 2. Texas Department of Banking
Chapter 17. Trust Company Regulation
Subchapter A. General
7 TAC §17.5

The Finance Commission of Texas (the commission), on behalf of the Texas Department of Banking (the department), adopts new 7 TAC §17.5, concerning required notice of cybersecurity incidents. The section is being adopted with clarifying, nonsubstantive changes to the proposed text as published in the July 5, 2019 issue of the *Texas Register* (44 Tex. Reg. 3384). The new rule will be republished in the *Texas Register*.

Millions of Americans, throughout the country, have been victims of identity theft. Identity thieves misuse personal information they obtain from a number of sources, including financial institutions, to perpetrate identity theft. Federal law strongly encourages financial institutions to take preventative measures to safeguard customer information against attempts to gain unauthorized access to the information, and further directs financial institutions to develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems that occur despite preventative measures, see 15 U.S.C. 6801; also see 16 C.F.R. §314.4. Revisions proposed by the Federal Trade Commission (FTC) in 2019 will explicitly require covered financial institutions, including trust companies, to develop an incident response plan as part of their information security programs in proposed 16 C.F.R. §314.4(h), see the April 4, 2019 edition of the *Federal Register* (84 Fed. Reg. 13158, at 13169). In connection with the proposal, the FTC stated that, for many financial institutions, satisfying the current requirement to have a reasonable information security program (16 C.F.R. §314.4(b)) would necessarily require development of an incident response plan, see 84 Fed. Reg. at 13169.

Further, organizations across all industries are facing a surge of ransomware attacks launched by cybercriminals. New types of ransomware principally causing this surge have the potential to cause significantly more business disruption and difficulty restoring computer data and networks. Attackers are also often demanding steeper amounts and are targeting small and medium-sized companies in addition to the larger organizations that often make headlines. Confidential business information, trade secrets, organizational strategies and financial information are all vulnerable to loss, either directly or through compromise of a cloud-based service provider.

New §17.5 will require a state trust company to notify the banking commissioner promptly if it experiences a material cybersecurity incident in its information systems, whether maintained by the trust company or by an affiliate or third party service provider at the direction of the trust company. Regulatory oversight of a state trust company's remediation and compliance efforts in response to a material cybersecurity incident can better inform the examination process applicable to all state trust companies, resulting in stronger and more secure protection of sensitive customer information and other confidential information.

Subsection (a) provides definitions. "Cybersecurity incident" is defined by

§17.5(a)(1) in a manner consistent with current federal guidance as essentially an observed irregularity that must be investigated to determine if information has been accessed, damaged and/or stolen. Most cybersecurity incidents will not result in a notice to the commissioner. Materiality is determined with reference to the circumstances under which a notice is required by subsection (b). Finally, the definition is designed to encompass incidents regarding an information system maintained by a service provider on behalf of the state trust company.

Section 17.5(a)(2) defines "information system" more broadly than current federal guidance, which is limited to systems that handle sensitive customer information. Beyond sensitive customer information, there are other types of sensitive data that can have a detrimental impact on a trust company if breached, including confidential business information, trade secrets, organizational strategies and financial information. Further, a breach of specialized systems such as telephone switching or exchange systems and environmental control systems can have a material adverse effect on a trust company's operations and financial performance.

Subsection (b) requires a state trust company to notify the banking commissioner as soon as practicable but prior to client notification, and no later than 15 days following the trust company's determination that an investigated cybersecurity incident will likely (1) require notice or a report to a regulatory or law enforcement agency other than the department, (2) a data breach notification to clients of the trust company under applicable law, or (3) adversely impact, at least temporarily, the ability of the state trust company to effect transactions on behalf of its clients or beneficiaries of trusts and custodial arrangements handled by the trust company, accurately report transactions to clients and beneficiaries, or otherwise conduct trust company business.

Subsection (c) specifies the information required to be submitted in the notice, to the extent known at the time of submission. The purpose of the notice is not to provide comprehensive information regarding the incident, but rather to provide a confidential early warning to (1) ensure the commissioner is informed of the basic circumstances before receiving related consumer complaints and calls from elected officials, and (2) enable the department to monitor the trust company's incident response and provide guidance if appropriate. While examiners with the department have sophisticated expertise and can assist if warranted, the section does not authorize the department to directly conduct or interfere with the trust company's incident response. The required notice is confidential pursuant to Finance Code §181.301.

Subsection (d) acknowledges that the filing of a suspicious activity report (SAR) may be required under federal law. While a SAR filing can be a triggering event to required notice under §17.5(b)(1), subsection (d) cautions that the trust company should not mention or discuss any SAR filing in the submitted notice.

New subsection (e), not part of the original proposal, advises a state trust company that the notice requirement imposed by new §17.5 must be incorporated into the written incident response plan it maintains as part of the information security program required by 16 C.F.R. §314.4.

Subsection (f), originally proposed as subsection (e), provides an exemption from the notification requirement for a family trust company that is exempt under Finance Code, §182.011.

The commission received comments from the Texas Bankers Association (TBA). TBA was supportive of the intent of the proposal but requested consideration of certain changes and clarifications. In addition, the commission received comments on a similar proposed rule affecting state banks, and those comments influenced several improvements to this rule.

TBA believes the proposed definition of "cybersecurity incident" is overly broad given the number of daily attacks attempted on financial institutions, sometimes in the thousands each day, because many of these attempts have the potential to "jeopardize the cybersecurity of the information system or the information the system processes," as stated in the proposal. Under this definition, the commissioner could be inundated by cybersecurity incident reports because compliance officers would rather overreport than underreport. TBA suggests that the definition could be improved if made more specific and consequence-focused.

The department disagrees but acknowledges that additional explanation is appropriate. In the information security literature, the thousands of daily, attempted attacks on an information system are called "events." An event is elevated to an "incident" if the observed irregularity must be further investigated to determine if information has been accessed, damaged and/or stolen. The existence of an incident, as defined by §17.5(a)(1), triggers an investigation, and an incident is reportable only if the trust company concludes, based on its investigation, that a consequence listed in §17.5(b)(1) through (3) is likely. Thus, only a few cybersecurity incidents are actually reportable.

TBA argues that the 15-day cybersecurity incident notification window is too short to permit a reasonable investigation and should be changed to at least 30 days. The department disagrees and suggests that this objection is based on a misreading of the proposed text. The 15-day cybersecurity incident notification window provided in §17.5(b) does not commence upon detection of the incident, as the comments would imply, but rather begins when the institution determines, after investigation, that the incident is material, based on the circumstances or consequences detailed in §17.5(b)(1) through (3). Minor wording changes were made to clarify this aspect of the rule.

Based on concerns expressed by another commenter, the department determined that proposed §17.5(b)(3), which required a notice if the incident would have a material adverse effect on the financial performance of the trust company or on clients or beneficiaries, was too subjective and uncertain to ensure compliance. As adopted, revised §17.5(b)(3) requires a notice if the trust company concludes the incident has an adverse impact on its ability to effect transactions on behalf of clients or beneficiaries of trusts or custodial arrangements handled by the trust company, to accurately report transactions to clients and beneficiaries, or to otherwise conduct trust company business, even if temporary.

This articulation should be more readily ascertainable than the version as proposed.

Finally, TBA expressed concern with the interplay of the proposed rule and the filing of a SAR, arguing that the language in proposed subsection (d) seems to direct a trust company to walk straight to the edge of disclosing the SAR filing but not actually disclosing the filing. The department disagrees. The notice content specified by §17.5(c) is relatively brief and simple to accomplish, and does not include a disclosure of the existence of related SAR filings, if any. Section 17.5(d) is merely precautionary because acknowledging the existence of a SAR is potentially a criminal offense under federal law.

Texas law provides that, to be considered nonsubstantive, changes made in the adopted version of a rule must not adversely affect the rights of affected parties as compared to the proposal or affect persons who would not have been impacted by the rule as proposed. While numerous changes are made to the proposed text of §17.5, the scope of the rule has not changed, the revisions more precisely tailor the section in response to comments noting unintended results of the proposed language or requesting additional clarification regarding specific attributes of the rule, thus enhancing the rights of affected parties as compared to the proposal. The commission thus concludes the changes to §15.5 are nonsubstantive and do not require re-proposal.

The new rule is adopted under Finance Code, §181.003(a)(2), which authorizes the commission to adopt rules necessary or reasonable to preserve or protect the safety and soundness of state trust companies.

§17.5. Notice of Cybersecurity Incident.

(a) Definitions. The following words and terms, when used in this section, shall have the following meanings, unless the context clearly indicates otherwise.

(1) "Cybersecurity incident" means any observed occurrence in an information system, whether maintained by the trust company or by an affiliate or third party service provider at the direction of the trust company, that:

(A) jeopardizes the cybersecurity of the information system or the information the system processes, stores or transmits; or

(B) violates the security policies, security procedures or acceptable use policies of the information system owner to the extent such occurrence results from unauthorized or malicious activity.

(2) "Information system" means a set of applications, services, information technology assets or other information-handling components organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, including the operating environment as well as any specialized system such as telephone switching or exchange systems and environmental control systems.

(b) Notice required. A state trust company shall notify the banking commissioner and submit the information required by subsection (c) of this section as soon as practicable but prior to customer notification, and not later than 15 days following the trust company's [~~a~~]

determination that a cybersecurity incident [~~has occurred~~] regarding the trust company's information system [~~, whether maintained by the trust company or by an affiliate or third party service provider at the direction of the trust company, that~~] will likely:

(1) require submission of a notice or report to another state or federal regulatory agency or to a self-regulatory body other than the notice required by this section;

(2) require sending a data breach notification to trust company clients [~~of~~] or beneficiaries of trusts and custodial arrangements handled by the trust company under applicable state or federal law, including Business and Commerce Code, §521.053, or a similar law of another state; or

(3) adversely impact, at least temporarily, the ability of the state trust company to effect transactions on behalf of its clients or beneficiaries of trusts and custodial arrangements handled by the trust company, accurately report transactions to clients and beneficiaries, or otherwise conduct trust company business [~~cause a material adverse effect on:~~

[~~(A) the financial performance of the trust company; or~~

[~~(B) clients or beneficiaries of trusts and custodial arrangements handled by the trust company~~].

(c) Content of notice. The confidential notice required by subsection (b) of this section must include, to the extent known at the time of submission:

(1) a brief description of the cybersecurity incident, including the approximate date of the incident, the date the incident was discovered, and the nature of any data that may have been illegally obtained or accessed;

(2) subject to subsection (d) of this section, a list of the state and federal regulatory agencies, self-regulatory bodies, and foreign regulatory agencies to whom notice has been or will be provided; and

(3) the name, address, telephone number, and email address of the employee or agent of the trust company from whom additional information may be obtained regarding the incident.

(d) Omission of certain information. The filing of a suspicious activity report (SAR) related to the cybersecurity incident under applicable federal law constitutes a notice described by subsection (b)(1) of this section. However, the trust company should not reference or mention the filing of a SAR in the notice filed with the commissioner.

(e) Incident response plan. The notice requirement imposed by this section must be incorporated into the trust company's written incident response plan, maintained as part of the trust company's information security program.

(f) Exemptions. This section does not apply to a state trust company that is exempt under Finance Code, §182.011.