Title 7. Banking and Securities
Part 2. Texas Department of Banking
Chapter 33. Money Services Businesses
7 TAC §33.30

The Finance Commission of Texas (the commission), on behalf of the Texas Department of Banking (the department), adopts new 7 TAC §33.30, 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. 3391). 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 money services businesses, 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 §33.30 will require a money services licensee under Texas Finance Code, Chapter 151, to notify the banking commissioner promptly if it experiences a material cybersecurity incident in its information systems, whether maintained by the licensee or by an affiliate or third party service provider at the direction of the licensee. This notice requirement should be incorporated into the licensee's written incident response plan. Regulatory oversight of a licensee's remediation and compliance efforts in response to a material cybersecurity incident can better inform the examination process applicable to all licensees, resulting in stronger and more secure protection of sensitive customer information and other confidential information.

Subsection (a) provides definitions of "cybersecurity incident" and "information system." The term "you" is also defined to mean a holder of a license issued under Texas Finance Code, Chapter 151.

"Cybersecurity incident" is defined by §33.30(a)(1) in a manner consistent with currently applicable federal guidance as essentially an observed irregularity that must be investigated to determine if information has been damaged 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 licensee.

Section 33.30(a)(2) defines "information system" more broadly than current federal guidance, which is limited to systems that handle sensitive customer information.

Subsection (b) requires a licensee to notify the banking commissioner as soon as practicable but prior to customer notification, and no later than 15 days following the licensee'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 customers under applicable law, or (3) adversely impact, at least temporarily, the ability of the licensee to effect transactions on behalf of its customers, accurately report transactions to customers, or otherwise conduct licensee 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 licensee'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 licensee's incident response. The required notice is confidential pursuant to Finance Code §151.606.

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 §33.30(b)(1), subsection (d) cautions that the licensee should not mention or discuss any SAR filing in the submitted notice.

New subsection (e), not part of the original proposal, advises a licensee that the notice requirement imposed by new §33.30 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.

The commission received no comments for or against adoption of proposed §33.30. However, the department circulated the proposal for pre-comment before the commission authorized publication of the proposal in the *Texas Register* for comment.

A current licensee suggested that the information to be protected should be limited to personally identifiable information of consumers to be consistent with federal law and guidance. The department disagreed with this comment. In addition to personally identifiable information of consumers, there are other types of sensitive data that can have a detrimental impact on a licensee if stolen or compromised, 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 licensee's operations and financial performance.

Although no comments were received regarding proposed §33.30, the department received comments on similar rules proposed for state banks and trust companies that noted possible issues regarding how to determine the materiality of an incident. Commenters also requested additional clarification regarding specific attributes of the rule text. The department agreed with some of these concerns and revised the proposals to better define a materiality standard and to provide greater clarity. Because those concerns could validly be raised regarding this proposal, the department made similar revisions to §33.30 as described in the succeeding paragraphs.

One commenter believed the proposed definition of "cybersecurity incident" was 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. The commenter suggested that this definition would cause the commissioner to be inundated by cybersecurity incident reports because compliance officers would rather overreport than underreport. The department disagreed 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 §33.30(a)(1), triggers an investigation, and an incident is reportable only if the licensee concludes, based on its investigation, that a consequence listed in §33.30(b)(1) through (3) is likely. Thus, only a few cybersecurity incidents are actually reportable.

Commenters also argued 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 §33.30(b) does not commence upon detection of the incident, as the comments would imply, but rather begins when the licensee determines, after investigation, that the incident is material, based on the circumstances or consequences detailed in §33.30(b)(1) through (3). Minor wording changes were made to clarify this aspect of the rule.

Based on other concerns expressed by commenters, the department determined that

proposed §33.30(b)(3), which required a notice if the incident would have a material adverse effect on the financial performance of the licensee or on its customers, was too subjective and uncertain to ensure compliance. As adopted, revised §33.30(b)(3) requires a notice if the licensee concludes the incident has an adverse impact on its ability to effect transactions on behalf of its customers, to accurately report transactions to customers, or to otherwise conduct licensee business, even if temporary. This articulation should be more readily ascertainable than the version as proposed.

Finally, one commenter 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 licensee to walk straight to the edge of disclosing the SAR filing but without actually disclosing the filing. The department disagrees. The notice content specified by §33.30(c) is relatively brief and simple to accomplish, and does not include a disclosure of the existence of related SAR filings, if any. Section 33.30(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 §33.30, the scope of the rule has not changed. The revisions more precisely tailor the section and provide additional explanation and 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 §33.30 are nonsubstantive and do not require re-proposal.

The new rule is adopted under Finance Code, §151.102(a), which authorizes the commission to adopt rules necessary or appropriate to preserve and protect the safety and soundness of money services businesses and protect the interests of purchasers of money services and the public.

§33.30. 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 you or by an affiliate or third party service provider at your direction, 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 electronic payment systems, industrial/process control systems, telephone switching and[~~,~~] private branch exchange systems and environmental control systems.

(3) "You" means a holder of a money transmission or currency exchange license issued under Finance Code, Chapter 151.

(b) Notice required. You must 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 [~~within~~] 15 days following your [~~a~~] determination that a cybersecurity incident [~~has occurred~~] regarding your information system [~~, whether maintained by you or by your affiliate or a third party service provider at your direction, that~~] will likely:

(1) require you to submit a notice or report [~~of the incident~~] to another state or federal regulatory or law enforcement agency or to a self-regulatory body[~~,~~] other than the notice required by this section;

(2) require you to provide a data breach notification to any of your customers 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, your ability to effect transactions on behalf of your customers, accurately report transactions to [~~cause a material adverse effect on your financial performance or on any of~~] your customers, or otherwise conduct your business.

(c) The 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 you have provided or will provide notice of the incident; and

(3) the name, address, telephone number, and email address of your employee or agent 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, you [~~the licensee~~] 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 written incident response plan that you maintain as part of your information security program.