Title 7. Banking and Securities
Part 1. Finance Commission of Texas
Chapter 3. State Bank Regulation
Subchapter B. General
7 TAC §3.24

The Finance Commission of Texas (the commission), on behalf of the Texas Department of Banking (the department), adopts new 7 TAC §3.24, concerning required notice of cybersecurity incident. 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. 3381). 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, e.g., 12 C.F.R. part 208, Appendix D–2 (Federal Reserve System), and 12 CFR part 364, Appendix B (Federal Deposit Insurance Corporation).

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

Subsection (a) provides definitions. "Cybersecurity incident" is defined by §3.24(a)(1) without regard to materiality and 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 bank.

Section 3.24(a)(2) defines "information system" more broadly than current federal guidance, which is limited to systems that handle sensitive customer information. However, there are other types of sensitive data that can have a detrimental impact on a bank if accessed without authorization, including confidential business information, trade secrets, organizational strategies and financial information. Further, a breach of specialized systems such as electronic banking systems, industrial/process controls systems, telephone switching and environmental control systems can have a material adverse effect on a bank's operations and financial performance.

Subsection (b) requires a state bank to notify the banking commissioner as soon as practicable but prior to customer notification, and no later than 15 days following the bank'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) require a data breach notification to one or more customers of the bank under applicable law, or (3) adversely impact, at least temporarily, the ability of the bank to effect customer transactions, accurately report customer transactions, or otherwise conduct bank business.

Subsection (c) specifies the information required to be submitted in the confidential 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 bank's incident response and provide guidance if warranted. 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 bank's incident response. The required notice is confidential pursuant to Finance Code §31.301.

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

New subsection (e), not part of the original proposal, advises a state bank that the notice requirement imposed by new §3.24 must be incorporated into the bank's written incident response plan, maintained as part of the bank's information security program. Federal guidance already includes a requirement to notify a bank's primary federal regulator prior to any notification to customers, see, e.g., 12 C.F.R. part 364, Appendix B, Supplement A, paragraph II.A.1.b.

The commission received comments from the Texas Bankers Association (TBA) and the Independent Bankers Association of Texas (IBAT). Both TBA and IBAT were supportive of the intent of the proposal but requested consideration of certain changes and clarifications.

TBA believes the proposed definition of "cybersecurity incident" is overly broad

given the number of daily attacks attempted on banks, 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 §3.24(a)(1), triggers an investigation, and an incident is reportable only if the bank concludes, based on its investigation, that a consequence listed in §3.24(b)(1) through (3) is likely. Thus, only a few cybersecurity incidents are actually reportable.

TBA and IBAT both argue 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 §3.24(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 §3.24(b)(1) through (3). Minor wording changes were made to clarify this aspect of the rule.

IBAT requested additional guidance or clarity regarding the materiality test in proposed §3.24(b)(3), which required a notice if the bank concludes that the incident would have "a material adverse effect on the financial performance of the bank or on customers of the bank." The department agrees that this provision is too subjective and uncertain to ensure compliance. As adopted, revised §3.24(b)(3) requires a notice if the bank concludes the incident has an adverse impact on the bank's ability to effect transactions on behalf of customers, to accurately report transactions to customers, or to otherwise conduct bank 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 banks 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 §3.24(c) is relatively brief and simple to accomplish, and does not include a disclosure of the existence of related SAR filings, if any. Section 3.24(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 §3.24, 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 §3.24 are nonsubstantive and do not require re-proposal.

The new rule is adopted under Finance Code, §31.003(a)(2), which authorizes the commission to adopt rules necessary or reasonable to preserve or protect the safety and soundness of state banks. As required by Finance Code, §31.003(b), in adopting the new rule, the commission considered the need to promote a stable banking environment, provide the public with convenient, safe, and competitive banking services, preserve and promote the competitive position of state banks with regard to national banks and other depository institutions in this state consistent with the safety and soundness of state banks and the state bank system, and allow for economic development in this state.

§3.24. 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 bank or by an affiliate or third party service provider at the direction of the bank, 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 banking systems, industrial/process control systems, telephone switching and[,] private branch exchange systems, and environmental control systems.

(b) Notice required. A state bank 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 bank's [~~a~~] determination that a cybersecurity incident [~~has occurred~~] regarding the bank's information system [~~, whether maintained by the bank or by an affiliate or third party service provider at the direction of the bank, that~~] will likely:

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

(2) require sending a data breach notification to customers of the bank 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 bank to effect transactions on behalf of customers, accurately report transactions to customers, or otherwise conduct bank business [~~cause a material adverse effect on the financial performance of the bank or on customers of the bank~~].

(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 bank 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 bank 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 bank's written incident response plan, maintained as part of the bank's information security program.