Charles G. Cooper
Commissioner

TEXAS DEPARTMENT OF BANKING

2601 North Lamar Blvd., Austin, Texas 78705
512-475-1300 /877-276-5554
www.dob.texas.gov

Media Contact:
media@dob.texas.gov

INDUSTRY NOTICE 2020-01
February 6, 2020

Requirements for a Cybersecurity Incident Report filed by a Texas State-Chartered Bank or Trust Company

Banks and trust companies are facing a surge of attacks in various forms by cybercriminals. These attacks have the potential to cause significant business disruption and potential loss of confidential business information, trade secrets, organizational strategies, and financial information.

New rules, which became effective January 2, 2020, require banks and trust companies to report cybersecurity incidents to the Banking Commissioner. Title 7, Texas Administrative Code §3.24 and §17.5, respectively, require a state-chartered bank or trust company to promptly notify the Banking Commissioner if it experiences a material cybersecurity incident in its information systems, whether maintained by the entity, an affiliate or third-party service provider.

The new rules require the notice to be submitted to the Department as soon as practicable, prior to customer notification, but not later than 15 days following the entity's determination that a qualifying cybersecurity incident has occurred. A cybersecurity incident must be reported if other state or federal law will require reporting of the breach to regulatory or law enforcement agencies or affected customers, or if the entity's ability to conduct business is substantially affected. The required notice is confidential pursuant to the Texas Finance Code.

The state-chartered bank or trust company shall notify the Banking Commissioner by submitting information that addresses the following:

- Description of the cybersecurity incident to include:
  - Approximate date of the incident;
  - Date incident was discovered, and
  - Nature of any data that may have been illegally obtained or accessed.
- A list of the state and federal regulatory agencies, self-regulatory bodies, and foreign regulatory agencies to whom the notice has been or will be provided. Do not include the filing of a suspicious activity report related to the cybersecurity incident in the list.

- Contact information for the entity regarding the incident. Include:
    - Name;
    - Address;
    - Telephone number; and
    - Email address.

The notice should be supplemented as additional information becomes available. If not all the information above is known, the entity is encouraged to report what is known, rather than wait until all details of the incident are confirmed.

An entity must notify the Department of the incident by either email or regular mail. Any confidential personal identifiable information or other confidential information should be uploaded via the Data Exchange (DEX) portal to the correspondence folder.