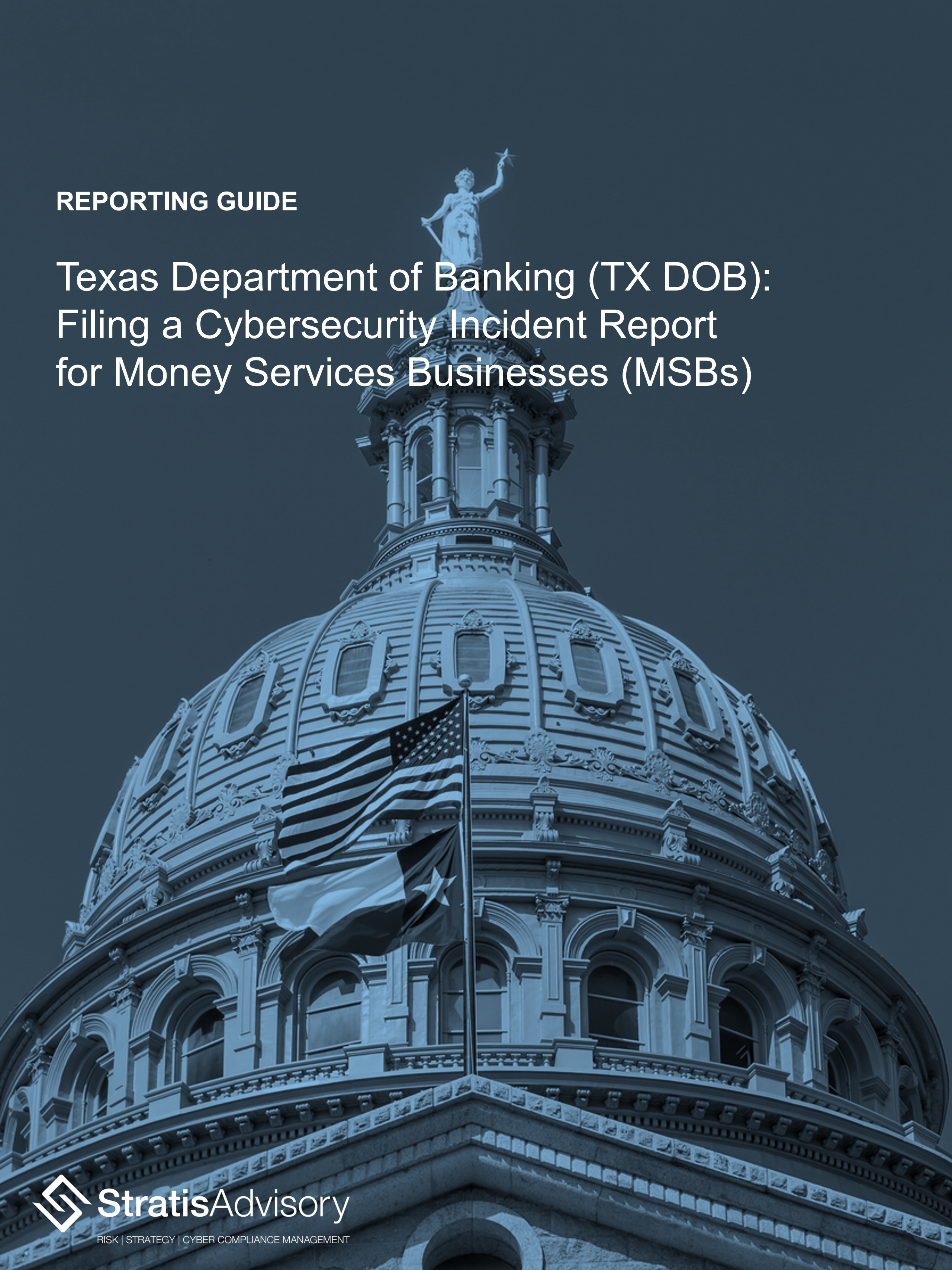
REPORTING GUIDE

Texas Department of Banking (TX DOB): Filing a Cybersecurity Incident Report for Money Services Businesses (MSBs)



StratisAdvisory

RISK | STRATEGY | CYBER COMPLIANCE MANAGEMENT

TX DOB Cybersecurity Incident Reporting Guide

The Texas Department of Banking (TX DOB) requires regulated entities, including money services businesses (MSBs), to promptly report any significant cybersecurity or computer-security related incidents, whether the incident occurred in a system maintained by the MSB, or within its affiliates or third-party service providers.

Who needs to submit a Cybersecurity Incident?

MSBs licensed under the Texas Finance Code Chapter 152, must notify the TX DOB in the event of a cybersecurity incident occurrence.

When should a Cybersecurity Incident be reported?

A notification must be submitted to the TX DOB as soon as possible, no later than 15 days, and prior to consumer notification, upon determination that a cybersecurity incident has occurred.

What is considered as a Cybersecurity Incident Report?

TX DOB defines a cybersecurity incident as "any observed occurrence in an information system, whether maintained by you or by an affiliate or a third-party service provider at your direction, that:

- *Jeopardizes the cybersecurity of the information system or the information the system processes, stores or transmits; or*
- *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."*

What information is included in the Cybersecurity Incident Report?

The MSB must include the following information when notifying the TX DOB:

- *Description of the cybersecurity incident, including the approximate date of the incident, the date the incident was discovered and the nature of data that may have been illegally accessed or obtained;*
- *A list of state, federal or foreign regulatory agencies to whom the notice has been or will be provided; and*
- *Contact information of the entity including the legal entity name, contact name, address, telephone number and email address.*

How is the Cybersecurity Incident reported?

The MSB must notify the TX DOB about the cybersecurity incident either through email or regular mail:

- **Email Address:** msb@dob.texas.gov
- **Mailing Address:** Texas Department of Banking, 2601 N. Lamar Blvd., Austin, TX 78705

Information that contain confidential and personally identifiable information should be uploaded into the correspondence folder found in the Data Exchange (DEX) portal.

Reporting Tips

- *A cybersecurity incident must also be reported if other state or federal laws require security breach notification to a regulatory or law enforcement agency or impacted customers, or if the entity's ability to continue doing business is substantially affected.*
- *Pursuant to the Texas Finance Code, all reports will be treated as confidential.*
- *If not all information is available at the time of discovery, supplemental information must be provided as soon as it becomes available. Entities are encouraged to report right away what is known, rather than wait until all details are confirmed.*
- *Filing a suspicious activity report (SAR) related to the cybersecurity incident is also required under the Bank Secrecy Act (BSA). However, the filing entity should not mention or reference the filing of a SAR in the cybersecurity incident report to TX DOB.*

For more information on the TX DOB's Cybersecurity Incident Reporting: https://www.dob.texas.gov/cybersecurity-incident-report.