REPORTING GUIDE

California's Department of Financial Protection and Innovation (DFPI): 48-Hour Expectation for Licensees on Reporting Cybersecurity Incidents

StratisAdvisory

RISK | STRATEGY | CYBER COMPLIANCE MANAGEMENT

California DFPI Cybersecurity Incident Reporting Guide

Under California's Department of Financial Protection and Innovation (DFPI) cybersecurity incident guidance, licensed entities are urged to report significant cybersecurity events within 48 hours to help mitigate risks and protect stakeholders. The goal is to encourage early detection, rapid response, and containment of threats that could impact financial systems, client data, or operational integrity.

Who needs to submit a Cybersecurity Incident?

All entities licensed or regulated by the DFPI are mandated to report if they experience cybersecurity incident or have reasons to believe that an incident occurred. Licensees under DFPI include banks, credit unions, mortgage lenders, escrow companies, payday lenders, and FinTech firms.

When should a Cybersecurity Incident be reported?

A cybersecurity incident must be reported to DFPI within 48 hours of discovery or as soon as possible. Early reporting enables DFPI to assess risks to consumers and financial systems quickly. Immediate recognition of a potential cybersecurity helps coordinate containment and mitigation efforts swiftly.

What are the examples of Cybersecurity Reportable Incidents?

A cybersecurity incident is considered reportable if it is:

- *Ransomware attacks*
- *Unauthorized access*
- *Data breaches*
- *Phishing or spear-phishing attacks*
- *Social engineering incidents*
- *Vendor or third-party breaches*
- *Malware infections*
- *Fraudulent fund transfers*

What information is included in the Cybersecurity Incident Report?

The following core information must be included in the Report:

- *Pertinent information of the licensee such as type of license, license number, name, point of contact, number, and email address;*
- *Date and time of discovery;*
- *Systems or data affected and sensitive information compromised;*
- *Incident description and mitigation actions taken; and*
- *Current status of investigation and other regulatory notifications.*

How is the Cybersecurity Incident Report filed?

The Cybersecurity Incident is electronically filed through the DFPI's Cybersecurity Incident Report Form.

Licensees are encouraged to submit even if the details are incomplete, then follow up is required for updates. For questions and further updates on the report, entities can send email to Ask.DFPI@dfpi.ca.gov.

Reporting Tips

- *Entities are encouraged to submit the report within 48 hours of discovery even if the forensic investigation is not yet complete. DFPI emphasizes on early awareness versus polish detail.*
- *Describe the incident type, affected systems, and immediate impact clearly in the report. This ensures DFPI can quickly understand the severity and scope of the incident.*
- *Record what steps were taken such as containment, mitigation, vendor notifications, or law enforcement contact. If other regulatory agencies were notified (FDIC, OCC, etc.), DFPI expects aligned reporting.*
- *Consider vendor oversight at all times because third-party breaches are reportable if they affect consumers.*
- *Look beyond CA for other state reporting requirements that may be applicable. For example, Texas maintains 'as soon as possible, but no later than 15 days.' Whereas under Part 500 in New York, reporting is required within 72 hours of the incident.*

DFPI DEPARTMENT OF FINANCIAL PROTECTION & INNOVATION

For more information, you can visit the how to Report a Cybersecurity Incident page found in California's DFPI website.