Supplemental Guide:

Identity Protection & Credit Monitoring Considerations Following a Data Breach

This guide is provided by Aptora Corporation solely as a general informational resource to assist customers in evaluating potential identity protection and credit monitoring considerations following the June 22, 2026 cybersecurity incident.

The information contained in this guide is intended to provide a general overview of commonly applicable legal and regulatory considerations. It is **not** intended to constitute legal advice, a definitive interpretation of any law or regulation, or a substitute for advice from qualified legal counsel.

Data breach notification requirements, identity protection obligations, and related regulatory requirements vary based on numerous factors, including the jurisdiction, the specific categories of information involved, the circumstances of the incident, contractual obligations, and changes in applicable law. These requirements are subject to legislative amendment, regulatory interpretation, and judicial decisions.

Each organization is responsible for evaluating its own legal, contractual, and regulatory obligations. Aptora strongly recommends that customers review this guide with their legal counsel, privacy professionals, and, where appropriate, their cyber insurance carrier before making decisions regarding notification obligations, identity protection services, regulatory reporting, or other incident response activities.

This guide should be used as a reference to support your organization's assessment and response efforts and should not be relied upon as the sole basis for legal or compliance decisions.

Purpose

This guide is intended to assist Aptora customers in understanding when identity theft protection or credit monitoring services may be appropriate following a cybersecurity incident. Requirements vary by jurisdiction and are generally based on:

- The type of personal information involved.
- Whether the information was encrypted or otherwise protected.
- The likelihood that the information could be misused.
- Applicable state, provincial, or federal law.

- Contractual obligations.
- Business risk considerations.

This guide is provided for informational purposes only and should not be considered legal advice.

When Identity Protection Is Commonly Considered

Organizations should evaluate whether identity protection or credit monitoring services are appropriate when the incident involves one or more of the following:

High-Risk Personal Information

- Social Security Numbers
- Taxpayer Identification Numbers
- Driver's License or State Identification Numbers
- Passport Numbers
- Financial Account Numbers with access credentials
- Credit or Debit Card Numbers with security codes or PINs
- Medical Information
- Health Insurance Information
- Biometric Identifiers
- Usernames or email addresses together with passwords or security questions

In many jurisdictions, exposure of only a name, address, telephone number, or email address does **not** by itself create an obligation to provide identity protection services.

States That May Require or Strongly Favor Identity Protection

State	Identity Protection Requirement	Common Trigger
Connecticut	May require identity theft prevention and mitigation services	Breach involving Social Security Numbers or taxpayer identification numbers of Connecticut residents
California	Not generally required by statute, but frequently offered as a best practice	Exposure of Social Security numbers, driver's license numbers, financial account information, or similar sensitive data

Maryland	May be appropriate depending on the sensitivity of the information	High-risk personal information creating a significant risk of identity theft
Washington	Often recommended for high-risk financial or identity information	Sensitive personal information that could facilitate identity theft
New York	Frequently offered as a risk mitigation measure	Social Security numbers, financial account information, or authentication credentials
Other States	Generally not mandatory, but commonly considered	Exposure of sensitive personal or financial information presenting a material risk of identity theft

States Where Identity Protection Is Generally Not Required by Statute

For the following states, breach notification laws generally **do not independently require** organizations to provide identity theft protection or credit monitoring solely because a breach occurred:

- Alabama
- Arizona
- Arkansas
- Delaware
- Florida
- Georgia
- Indiana
- Kansas
- Michigan
- Minnesota
- Missouri
- Nebraska
- New Jersey
- North Carolina
- Ohio
- Oklahoma
- Pennsylvania
- South Carolina
- Tennessee
- Texas
- Virginia

- Wisconsin

Although not generally required, many organizations voluntarily provide identity protection services when Social Security numbers, financial account information, or other highly sensitive personal information may have been compromised.

Business Factors to Consider

Even where not legally required, organizations may decide to offer identity protection services based on:

- The sensitivity of the information involved.
- The number of individuals affected.
- Evidence that information was exfiltrated.
- Contractual commitments.
- Cyber insurance recommendations.
- Customer relations considerations.
- Reputational risk.
- Recommendations from legal counsel.

Recommended Evaluation Checklist

Before deciding whether to offer identity protection services, consider:

☐ Were Social Security numbers involved?

☐ Were taxpayer identification numbers involved?

☐ Were driver's license or passport numbers involved?

☐ Were financial account numbers exposed together with information that could permit unauthorized access?

☐ Were payment card numbers exposed together with security codes or PINs?

☐ Were usernames or email addresses exposed together with passwords or security questions?

☐ Does applicable state law require identity protection services?

☐ Has legal counsel reviewed the circumstances?

☐ Has your cyber insurance carrier provided recommendations?

Recommended Documentation

Organizations should document:

- The categories of information involved.
- The jurisdictions of affected individuals.
- The legal analysis performed.
- The decision regarding identity protection services.
- The rationale supporting that decision.

Maintaining this documentation may assist in demonstrating a reasonable and well-documented response to the incident.