APTORA CORPORATION

DATA SECURITY INCIDENT RESPONSE PACKAGE

Customer Notification and Regulatory Support Materials

This packet is intended to assist Aptora's business customers in understanding the June 22, 2026, cybersecurity incident and supporting their own assessment and response activities.

Because the information maintained within each customer's hosted environment is different, not every section of this packet will apply to every organization.

Customers should review the materials relevant to their organization and contact Aptora's Incident Response Team if additional information is needed.

Incident Date: June 22, 2026
Prepared For: Aptora Business Customers Impacted by Cybersecurity Incident
Prepared By: Aptora Corporation
Address: 8877 Bourgade Street, Lenexa, Kansas 66219

PART 1

SECTION 1

Letter to Our Business Customers Dear Valued Customer,

Aptora Corporation is writing to notify you of a cybersecurity incident that may have involved information maintained within your hosted Aptora environment.

On June 22, 2026, Aptora identified unauthorized activity within portions of its hosted infrastructure. Upon discovery, we immediately activated our Incident Response Plan, secured affected systems, engaged independent cybersecurity and forensic specialists, notified federal law enforcement, and began a comprehensive investigation.

Our investigation determined that an unauthorized third party accessed certain systems and that data maintained on behalf of some customers may have been accessed or acquired without authorization.

Because Aptora hosts information for your organization, we are providing this notification so you may evaluate any legal, regulatory, contractual, or internal notification obligations applicable to your business.

Enclosed is an Incident Response Packet containing:

- A summary of the incident.
- Information regarding the types of data that may have been involved.
- Actions taken by Aptora to contain and investigate the incident.
- A general incident timeline.
- A data controller / data processor responsibility matrix
- Frequently Asked Questions
- Customer Response Checklist
- Supplemental Customer Resource List
- Contact information for Aptora's Incident Response Team.

We recognize that incidents of this nature may create additional work and concern for your organization. We are committed to transparency, cooperation, and providing the information you need to respond appropriately.

If you require additional information to support your internal assessment or regulatory obligations, please contact our Incident Response Team.

We sincerely regret this incident and appreciate your continued partnership.

Sincerely,

James Leichter, President
Aptora Corporation

SECTION 2

Incident Overview

What Happened

On June 22, 2026, Aptora detected unauthorized activity involving portions of its hosted infrastructure.

Our response included immediate containment of the affected environment, engagement of independent cybersecurity professionals, preservation of forensic evidence, notification of federal law enforcement, and a comprehensive forensic investigation.

Based on the investigation, Aptora determined that an unauthorized party gained access to certain systems and may have accessed or acquired information maintained on behalf of some hosted customers.

This notification is being provided to assist your organization in evaluating whether information belonging to your customers, employees, vendors, or other individuals may have been affected.

SECTION 3

Information Potentially Involved

The information maintained within Aptora's hosted environment varies by customer.

Depending upon your organization's configuration and business processes, the affected information may have included one or more of the following:

- Customer names
- Business names
- Mailing addresses
- Email addresses
- Telephone numbers
- Customer account information
- Bank account information (where maintained)
- Payment card information (where maintained)
- Other business records maintained within your hosted environment

At this time, Aptora has no evidence that your information has been used for identity theft or fraud. However, because unauthorized access occurred, we are notifying you so you can take appropriate precautions.

Your organization should review the information provided by Aptora together with your own records to determine whether notification to affected individuals or regulatory agencies may be required.

SECTION 4
Aptora's Response

Immediately following discovery of the incident, Aptora initiated its incident response procedures.

Actions taken included:

- Securing affected systems.
- Containing unauthorized activity.
- Engaging independent cybersecurity and forensic experts.
- Preserving digital evidence.
- Conducting a comprehensive forensic investigation.
- Cooperating with federal law enforcement.
- Restoring hosted services from verified backups.
- Implementing additional security controls and monitoring.
- Reviewing privileged access and administrative security controls.
- Continuing to monitor systems for suspicious activity.

Aptora remains committed to supporting its customers throughout the response process.

SECTION 5
Data Controller / Data Processor Responsibility Matrix

DragonForce Cybersecurity Incident

Incident Date: June 22, 2026

Document Purpose

This matrix is intended to assist Aptora Corporation and its customers in understanding their respective responsibilities following the June 22, 2026 cybersecurity incident. It is based on the typical relationship in which Aptora provides software hosting and related services, while the customer determines the purposes and means of processing personal information.

Unless otherwise provided by contract or applicable law, Aptora acts as a data processor/service provider, and each customer acts as the data controller/data owner for the information contained in its hosted database.

This document is intended for operational guidance only and is not legal advice.

Definitions

Data Controller / Data Owner

The organization that:

- Owns or licenses the personal information.
- Determines what information is collected.
- Determines why the information is collected.
- Determines who may access the information.
- Determines how long information is retained.
- Determines whether information is disclosed to third parties.

For Aptora-hosted environments, this is generally the customer.

Data Processor / Service Provider

The organization that:

- Hosts customer information.
- Stores customer information.
- Processes information solely on behalf of the customer.
- Does not determine why information is collected.
- Does not determine how customer information is used.

For this incident, this is generally Aptora Corporation.

Responsibility Matrix

Activity	Aptora (Processor / Service Provider)	Customer (Controller / Data Owner)
Detect cybersecurity incident	✓	
Contain attack	✓	
Preserve forensic evidence	✓	
Restore hosted systems	✓	
Notify customer of breach	✓	
Provide incident timeline	✓	
Provide technical incident summary	✓	
Provide categories of potentially affected data	✓	
Cooperate with forensic investigation	✓	✓
Determine whose records are affected	Assist	✓
Identify affected individuals	Assist	✓
Determine applicable state/provincial laws	Assist	✓
Determine whether notification is legally required		✓
Notify affected individuals		✓
Notify Attorneys General or privacy regulators		✓

Notify consumer reporting agencies (where required)		✓
Notify industry regulators (IRS, HHS, etc.)		✓
Respond to questions from affected individuals	Support if requested	✓
Provide identity theft protection or credit monitoring (if required by law or chosen voluntarily)	Only if contractually agreed	✓
Document legal basis for notification decisions		✓
Maintain incident response records	✓	✓
Cooperate with law enforcement	✓	✓ (if requested)

Aptora Responsibilities

Following discovery of the incident, Aptora will:

- Promptly notify affected customers.
- Provide a summary of known facts.
- Provide the incident timeline.
- Provide a description of the categories of information potentially affected.
- Provide updates as material information becomes available.
- Cooperate with customer investigations.
- Preserve evidence.
- Coordinate with law enforcement, cyber insurance carriers, digital forensic investigators, and legal counsel.
- Continue implementing additional security improvements.

Aptora cannot determine:

- Which individuals should receive notification.
- Whether notification is legally required in a particular jurisdiction.
- Whether a specific customer must notify a regulator.
- Whether credit monitoring or identity theft protection must be offered.
- Whether contractual obligations require additional actions

Customer Responsibilities

Aptora Corporation hosts customer databases on behalf of its business customers but does not own or control the information contained within those databases.

Because each customer's hosted environment is unique, Aptora cannot determine the specific information maintained by an individual customer or the legal, regulatory, contractual, or business obligations that may arise from this incident.

Each customer is responsible for evaluating its own legal, regulatory, contractual, and business obligations arising from this incident. These responsibilities may include:

- Determining whether individuals associated with your organization were affected.
- Assessing applicable federal, state, provincial, or international notification requirements.
- Consulting with legal counsel regarding notification obligations.
- Notifying regulators, customers, employees, vendors, or other affected parties when required.
- Documenting decisions made during your incident response process.

To assist with these efforts, Aptora has included sample notification templates and supporting reference materials within this packet.

Identity Protection Services

Depending on the types of information involved and the jurisdictions in which affected individuals reside, some organizations may determine whether offering identity protection or credit monitoring services is appropriate or may be required by applicable law.

Customers should evaluate their own circumstances and, where appropriate, consult legal counsel regarding any legal, regulatory, or contractual obligations that may apply.

To assist customers with this evaluation, Aptora has prepared a Supplemental Guide – Identity Protection & Credit Monitoring by State Following a Data Breach. This guide provides a general overview of circumstances in which identity protection services may be appropriate, identifies jurisdictions that may impose specific requirements, and outlines common factors organizations should consider when evaluating their response.

The supplemental guide is provided as a general informational resource only and is not intended to constitute legal advice or a definitive interpretation of applicable law. Customers should review the guide with their legal counsel to verify the legal requirements applicable to their organization and the specific facts of their incident before making decisions regarding identity protection services or breach notification obligations.

SECTION 6

Frequently Asked Questions

Why am I receiving this notification?

Your organization maintains information within Aptora's hosted environment that may have been involved in the June 22, 2026 cybersecurity incident.

Does this mean my organization experienced a data breach?

Not necessarily. Aptora is notifying customers whose hosted environments may have contained information accessed during the incident so that each organization can evaluate its own circumstances and legal obligations.

What information may have been affected?

The information varies by customer and depends upon the records maintained within your hosted environment. Aptora will provide available information to assist your organization in determining what data may have been involved.

Has law enforcement been notified?

Yes. Aptora has notified federal law enforcement and continues to cooperate with the investigation.

Should my organization notify our customers or employees?

Notification requirements vary based on the information involved, the jurisdictions in which affected individuals reside, and applicable legal or contractual obligations. Aptora recommends consulting your legal counsel before making notification decisions.

Is Aptora's hosted environment operational?

Yes. The affected systems have been secured and restored, and additional security measures have been implemented to strengthen the hosted environment.

Will Aptora provide additional updates?

Yes. If additional information becomes available that materially affects your organization or changes our understanding of the incident, Aptora will communicate those updates promptly.

Should I contact Aptora?

Questions regarding your specific information should generally be directed to your business relationship with [Company Name]. Aptora is assisting its customers with incident response and notification requirements.

SECTION 7

Legal Guidance Memorandum

Important Role Clarification

Aptora operates as a technology service provider hosting information on behalf of its customers.

Generally:

Aptora

- Maintains and protects hosted systems.
- Provides notice to customers whose information was affected.
- Provides investigation details and response support.

Aptora Customers

- Determine whether they are legally required to notify individuals.
- Determine who must receive notification.
- Determine applicable state laws.
- Determine whether regulatory notifications are required.

SECTION 8

Customer Response Checklist

Each affected business should complete the following:

Immediate Actions

☐ Notify internal leadership
☐ Notify cyber insurance carrier
☐ Engage legal counsel
☐ Preserve documentation
☐ Identify affected databases
☐ Determine affected individuals

Determine Notification Requirements

☐ Identify states where affected individuals reside
☐ Review applicable breach notification laws
☐ Determine if regulators must be notified

☐ Determine whether law enforcement notification is required
☐ Determine whether consumer notification is required

Customer/Employee Notification Preparation

☐ Prepare notification letter
☐ Review notification with counsel
☐ Establish response phone/email
☐ Prepare FAQ document
☐ Train customer service representatives
☐ Maintain notification records

SECTION 9

Identity Protection Recommendations

Affected individuals should be encouraged to:

Obtain Credit Reports

Free credit reports:

> **Annual Credit Report**
> Website:
> www.AnnualCreditReport.com

Consumers may request reports from:

- Equifax
- Experian
- TransUnion

Consider Fraud Alerts

A fraud alert requires creditors to verify identity before opening new credit accounts.

Consumers can contact any one of the three credit bureaus:

Equifax
Phone: 1-800-525-6285
Website: www.equifax.com

Experian
Phone: 1-888-397-3742
Website: www.experian.com

TransUnion
Phone: 1-800-680-7289
Website: www.transunion.com

Consider Credit Freeze

A credit freeze restricts access to credit files and can help prevent unauthorized accounts from being opened.

Consumers can place freezes directly with:

- Equifax
- Experian
- TransUnion

Report Identity Theft

Federal Trade Commission:

Identity Theft Website:
www.IdentityTheft.gov

Phone:
1-877-438-4338

SECTION 10

Incident Timeline

Summary of Events

The following timeline provides a general overview of Aptora Corporation's response to the cybersecurity incident discovered on June 22, 2026.

Date	Event
June 22, 2026	Aptora identified unauthorized activity within a portion of its hosted environment and immediately activated its incident response procedures.
Immediately Following Discovery	The affected systems were secured, leading cybersecurity professionals were engaged to investigate the incident, and steps were taken to contain the unauthorized activity.
Investigation Phase	A comprehensive forensic investigation was conducted to determine the nature and scope of the incident, identify the information that may have been affected, and confirm the integrity of restored systems.
Law Enforcement & Legal Notification	Aptora notified appropriate law enforcement authorities and worked closely with legal counsel, cybersecurity experts, and its cyber insurance carrier throughout the investigation.
Security Enhancements	Additional security controls and monitoring were implemented to strengthen system security and reduce the risk of similar incidents in the future.
Customer Notification	Once sufficient information was confirmed through the investigation, Aptora began notifying affected customers and providing guidance on steps they can take to help protect their personal information.

SECTION 11

Contact Information

If your organization requires additional information regarding this incident or needs assistance evaluating the information associated with your hosted environment, please contact Aptora's Incident Response Team.

Email: supervisor@aptora.com

Telephone: (913) 492-9930

Hours: Monday through Friday, 11:00 AM– 4:00 PM CST, Monday - Friday

Please reference the **June 22, 2026 Security Incident** when contacting Aptora so we can respond as efficiently as possible.

SECTION 12

Customer Response Checklist

The following checklist is provided to assist your organization in evaluating its response to this incident. Depending on your business, the information involved, and the jurisdictions in which affected individuals reside, not every item may apply.

Review the Information

☐ Review the information provided by Aptora.

☐ Identify the data maintained within your hosted database that may have been involved.

☐ Determine which individuals or organizations may have been affected.

☐ Document your internal assessment and response activities.

Assess Notification Requirements

☐ Consult with legal counsel, if appropriate.

☐ Determine whether applicable laws or regulations require notification to affected individuals.

☐ Determine whether notification to regulators or other governmental agencies is required.

☐ Review contractual notification obligations with customers, vendors, or business partners.

Business Communications

☐ Determine whether customer notification is required.

☐ Determine whether employee notification is required.

☐ Determine whether vendor or business partner notification is required.

☐ Designate a point of contact to respond to questions.

☐ Prepare internal communications for employees, if appropriate.

Insurance and Risk Management

☐ Review your cyber insurance policy to determine whether this incident should be reported.

☐ Notify your insurance carrier if required under your policy.

Ongoing Monitoring

☐ Continue monitoring for unusual activity involving affected information.

☐ Retain documentation related to your response.

☐ Contact Aptora if additional information is needed to support your assessment or notification activities.

SECTION 13

Law Enforcement Coordination

Aptora notified the appropriate federal law enforcement authorities promptly after discovering this incident and continues to cooperate with the ongoing investigation.

To preserve the integrity of the investigation, certain technical and investigative details cannot be disclosed at this time. This does not affect your organization's ability to evaluate the information provided in this packet or determine any notification obligations that may apply.

If additional information becomes available that materially affects your organization, Aptora will provide updates as appropriate**.**

SECTION 14

Executive Summary

On June 22, 2026, Aptora Corporation identified unauthorized activity within portions of its hosted environment supporting customer applications.

Aptora immediately activated its incident response procedures, secured affected systems, engaged independent cybersecurity specialists, and initiated a comprehensive forensic investigation.

The investigation determined that an unauthorized third party gained access to certain hosted systems and that customer databases maintained within the environment may have been accessed or acquired without authorization prior to the deployment of ransomware.

Aptora restored affected systems using verified backups and pre-incident recovery points and has implemented additional security measures to strengthen the hosted environment. Aptora

continues to cooperate with law enforcement and to provide information necessary to assist affected business customers with their response activities.

SECTION 15

Recommended Next Steps

Aptora is providing this information to assist your organization in evaluating the potential impact of this incident. Depending on the information maintained within your hosted environment, your organization's business practices, and applicable legal or contractual requirements, you may wish to consider the following actions:

- Review the information maintained within your hosted database to determine what information may have been affected.
- Identify the individuals, customers, employees, vendors, or other parties whose information may have been involved.
- Review any applicable legal, regulatory, or contractual notification requirements.
- Consider consulting with legal counsel and your cyber insurance carrier regarding your organization's response.
- Determine whether notification to affected individuals, regulators, business partners, or other parties is appropriate.
- Review internal security procedures and monitor for any unusual activity related to the affected information.
- Maintain documentation of your organization's assessment, decisions, and response activities.

Aptora remains committed to supporting your organization throughout this process. If you require additional information regarding the incident or the information associated with your hosted environment, please contact Aptora's Incident Response Team.

Current Status of the Investigation

This packet is based on the information available to Aptora Corporation as of **July 23, 2026**.

The forensic investigation has substantially progressed; however, certain aspects of the investigation remain ongoing. As additional information becomes available, Aptora will provide updates to affected business customers when appropriate.

This packet is intended to provide information to assist your organization in understanding the incident and evaluating its own response. Because each organization's circumstances and legal obligations may differ, you should review this information together with your own records and, where appropriate, consult your legal or privacy advisors.

SECTION 16

Customer Data Assessment Guidance

Purpose

Because Aptora hosts customer databases on behalf of its business customers, the specific information contained within each hosted environment varies. As a result, the potential impact of this incident may differ from one organization to another.

This section is intended to assist your organization in identifying the information that may have been maintained within your hosted database and to support your internal assessment of the incident.

Information to Review

As part of your organization's assessment, you may wish to identify the categories of information that were maintained within your Aptora-hosted environment at the time of the incident, including, where applicable:

Customer Information

- Customer names
- Company names
- Mailing addresses
- Email addresses
- Telephone numbers
- Service history
- Billing and account information
- Customer notes

Employee Information

- Employee names
- Payroll information
- Tax records
- Banking information
- Dates of birth

- Government-issued identification numbers
- Other employment-related records

Vendor and Business Information

- Vendor contact information
- Banking or ACH information
- Tax identification numbers
- Contracts
- Purchase orders
- Invoices
- Other business records

Financial Information

- Payment card information
- Bank account information
- Routing numbers
- Payment history
- Other financial records maintained by your organization

Individuals Potentially Affected

Consider the types of individuals whose information may have been stored within your hosted environment, such as:

- Customers
- Employees
- Former employees
- Applicants
- Vendors
- Contractors
- Business partners
- Other individuals whose information your organization maintains

Geographic Considerations

If your organization maintains information relating to individuals residing in multiple states, provinces, or countries, you may wish to identify those jurisdictions as part of your assessment. Notification requirements can vary depending upon the applicable laws and the types of information involved.

Internal Assessment

Each customer's hosted environment is unique. Your organization should review its own records to determine:

- The categories of information maintained within the hosted database.
- The approximate number of individuals whose information may have been involved.
- Whether any sensitive personal or financial information was maintained.
- Whether contractual, regulatory, or legal obligations may apply to your organization.

SECTION 17

Assistance from Aptora

Aptora remains committed to supporting its customers throughout this process. If your organization requires additional information regarding your hosted environment or the information maintained within your database, please contact Aptora's Incident Response Team.

Additional information will be provided as the investigation progresses and as appropriate under the circumstances.

SECTION 18

Supplemental Customer Resources

Additional response materials are available upon request, including:

- Customer Data Inventory Worksheet
- Sample Individual Notification Letter
- Sample Employee Notification Letter
- Sample Vendor Notification Letter
- Sample Telephone Response Guide
- Sample Public Website Notice
- Supplemental Guide: Identity Protection & Credit Monitoring by State

To request these resources, please contact the Aptora Incident Response Team.

SECTION 19

Contact Information

Incident Response Team
Phone: 913-492-9930
E-mail: supervisor@aptora.com
11:00 AM to 4:00 PM CST, Monday through Friday
Case Reference: June 22, 2026 Cybersecurity Incident

To assist us in responding to your inquiry, please have your company name, primary contact information, and, if applicable, your hosted company file name available.

SECTION 20
Closing Statement

Aptora Corporation recognizes the importance of the trust our customers place in us to host and protect their business information. We sincerely regret this incident and understand the challenges it may create for your organization.

Since identifying the incident, Aptora has worked continuously to contain the threat, restore services, support the forensic investigation, strengthen security controls, and cooperate with law enforcement. These efforts remain ongoing as we continue to evaluate the incident and implement additional safeguards.

We are committed to providing timely updates should material new information become available and to supporting our customers throughout their response activities.

If you have questions or require additional information, please contact the Aptora Incident Response Team using the information provided in this packet.

Thank you for your continued partnership and the opportunity to continue serving your organization.