FLORIDA PRACTITIONER GUIDE

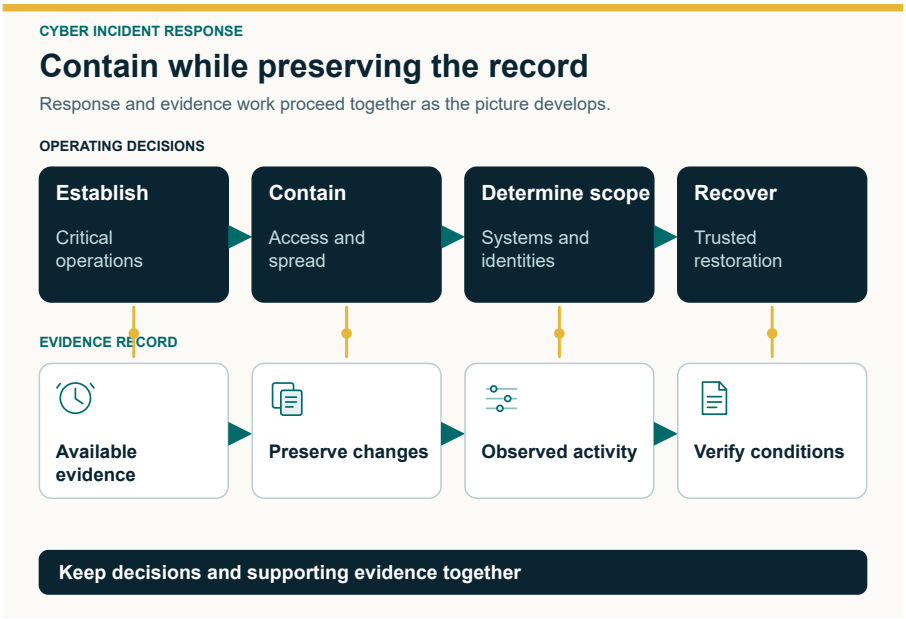
Florida Data Breach Response Under Section 501.171

Florida gives a breached organization 30 days from the determination of a breach to notify affected residents, adds Attorney General notice at 500 Floridians and credit bureau notice above 1,000, and gives counties, cities and state agencies as little as 12 hours to report ransomware. This guide lines up each deadline with the forensic facts it depends on.

Edition 2026-11-03 · Updated November 3, 2026 · miami-computer-forensics.com/guides/florida-breach-notification/

Every notice decision in a Florida breach rests on facts the forensic examination establishes: what was accessed, whose data it was, how many Florida residents are affected, when the organization determined a breach occurred and whether the data was encrypted. Get those facts wrong and the notices are late, overbroad or inaccurate. Get them right and the organization can meet the statute and answer the Department of Legal Affairs with confidence.

GDF responds around the clock on (800) 868-8189. Our examiners contain the incident while preserving the evidence, then scope the data exposure so counsel can make the notice decisions on a documented record.



Containment and the evidence record move together from the first hour.

1. Know What Counts as a Breach in Florida

Section 501.171(1)(a) defines a breach of security as unauthorized access of data in electronic form containing personal information. Good faith access by an employee or agent of the covered entity is not a breach, provided the information is not used for an unrelated purpose or subject to further unauthorized use.

© 2026 Global Digital Forensics, Inc. All rights reserved.

A covered entity is any commercial entity that acquires, maintains, stores or uses personal information, and for the notice requirements the term also includes governmental entities. [1]

The trigger is access, not proven theft. That makes the examiner's access analysis central: authentication logs, mailbox audit records, file access events and network traffic show which records an intruder could read and which it actually touched.

2. Personal Information Under Section 501.171

Personal information means a first name or first initial and last name combined with any of these elements: a social security number; a driver license, identification card, passport, military identification or similar government number; a financial account or card number with any required security code, access code or password; medical history, condition, treatment or diagnosis information; a health insurance policy or subscriber number or other insurer identifier; biometric data as defined in section 501.702; or geolocation information. It also includes a user name or email address combined with a password or security question and answer that permits access to an online account. Information made publicly available by a government entity is excluded, as is information that is encrypted, secured or modified so that it no longer identifies an individual or is otherwise unusable. [1]

The encryption exclusion is a technical finding. We document whether affected data was encrypted at rest, whether keys were exposed and whether the attacker had a path to decrypted data, because that determines which records count.

3. Thirty Days to Notify Affected Floridians

Under section 501.171(4), a covered entity must notify each Florida individual whose personal information was, or is reasonably believed to have been, accessed as expeditiously as practicable and without unreasonable delay, and no later than 30 days after the determination of a breach or reason to believe a breach occurred. A law enforcement agency may delay notice in writing if notice would interfere with a criminal investigation. Notice may be skipped only if, after an appropriate inquiry, which the statute calls an investigation, and consultation with law enforcement, the entity reasonably determines the breach has not and will not likely result in identity theft or other financial harm; that determination must be documented in writing, kept for at least 5 years and provided to the Department of Legal Affairs within 30 days. [1]

The notice goes by mail or email and must include the date, estimated date or date range of the breach, a description of the personal information accessed and contact information for inquiries. Substitute notice by website posting and media is permitted when direct notice would cost more than $250,000, would reach more than 500,000 people, or contact information is lacking, and notice given under the rules of the entity's primary or functional federal regulator is deemed compliant. Every one of those content elements comes from the examination: the date range from the intrusion timeline, the data description from the access analysis. [1]

4. Attorney General Notice at 500 Florida Residents

A breach affecting 500 or more individuals in Florida requires written notice to the Department of Legal Affairs no later than 30 days after the determination of the breach or reason to believe one occurred. The notice includes a synopsis of the events, the number of Floridians affected, any free services offered and

© 2026 Global Digital Forensics, Inc. All rights reserved.

how to use them, a copy of the individual notice and a contact person. If good cause for delay is provided in writing within those 30 days, the entity may receive 15 additional days to provide the individual notice. [1]

On request, the covered entity must give the Department a police report, incident report or computer forensics report, its breach policies and the steps taken to rectify the breach. Section 501.171(11) makes the information the Department receives confidential and exempt from public records disclosure while its review is active, with limited sharing for official duties and with other governmental entities, and keeps a computer forensic report confidential and exempt after the review ends. Write the forensic report expecting the Department to read it. [1]

5. Credit Bureaus Above 1,000 Notices and Agents Within 10 Days

When notice is required for more than 1,000 individuals at a single time, the covered entity must also notify, without unreasonable delay, the nationwide consumer reporting agencies of the timing, distribution and content of the notices. A third party agent that maintains, stores or processes personal information for a covered entity must notify that entity of a breach of its system as expeditiously as practicable and no later than 10 days after determining the breach or having reason to believe it occurred, and must provide all the information the covered entity needs to give its own notices. An agent may send notices on the covered entity's behalf, but a failure in those notices counts as the covered entity's violation. [1]

Vendor breaches are where timelines slip. We help covered entities obtain and validate the agent's evidence quickly, so the 30 day clock is run on facts rather than on a vendor's summary.

6. Penalties Accrue Per Breach and Grow Every Month

A violation of section 501.171 is treated as an unfair or deceptive trade practice in an action by the Department of Legal Affairs. A covered entity that violates the Department or individual notice requirements faces a civil penalty of $1,000 for each day up to the first 30 days, then $50,000 for each subsequent 30 day period or portion of one for up to 180 days, and up to $500,000 if the violation continues beyond 180 days. The penalties apply per breach, not per individual. Section 501.171 itself creates no private cause of action. [1]

Covered entities and third party agents must also take reasonable measures to protect personal information in electronic form and to dispose of customer records so the personal information is unreadable. The post incident review is the moment to show what those measures were.

7. Counties, Cities and State Agencies Report in Hours

Under the Local Government Cybersecurity Act, section 282.3185(5), a county or municipality must report every ransomware incident, and every cybersecurity incident it rates at severity level 3, 4 or 5, to the Cybersecurity Operations Center, the Cybercrime Office of the Florida Department of Law Enforcement and the sheriff with jurisdiction, no later than 12 hours after discovering a ransomware incident and 48 hours after discovering any other reportable incident. The report covers the facts, the date of the most recent backup and its location, the types of data compromised, the estimated fiscal impact, the ransom demand details and whether assistance is requested. An after action report goes to the Florida Digital Service within 1 week after remediation. [2]

© 2026 Global Digital Forensics, Inc. All rights reserved.

State agencies report to the Cybersecurity Operations Center and the Department of Law Enforcement on the same 12 and 48 hour schedule under section 282.318, submit an after action report within 1 week after remediation and give breach notice under section 501.171. Section 282.3186 bars a state agency, county or municipality experiencing a ransomware incident from paying or otherwise complying with a ransom demand, so recovery has to come from backups and rebuilding, and the backup facts in the report matter. [3] [4]

Call the Hotline While the Clock Is Running

Call (800) 868-8189 the moment you suspect unauthorized access; the hotline answers around the clock. On the first call a senior responder covers containment that preserves the evidence, the systems and data at issue, the Florida deadlines that may already be running and the facts the notices and any 282.3185 report will need. Engagements run under the direction of counsel when you choose.

Call the Miami office at (786) 219-1210 or the 24/7 hotline at (800) 868-8189, or write to info@evestigate.com. Requests and case assessments are handled in confidence. To keep preparing, read the Florida law guides in our library.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Florida Matter Intake Checklist

Gather what you can quickly and leave affected systems running as they are, so the responder preserves the evidence the notices depend on.

Note who controls each password, recovery key or unlock code, and share the completed checklist through the secure method agreed on the first call.

When did the organization determine, or have reason to believe, that a breach occurred?

Record the date, time and the event that triggered the conclusion. The 30 day notice periods in section 501.171 run from this point.

Answer:

Who confirmed it, from which record, and on what date:

Which systems, accounts and data stores are involved?

List servers, mailboxes, cloud tenants, databases and vendors, with the administrator for each.

Answer:

Who confirmed it, from which record, and on what date:

Which personal information elements may have been accessed, and was the data encrypted?

Note names combined with social security, license, financial, medical, insurance, biometric or geolocation data, or online credentials, and whether encryption keys were exposed.

Answer:

Who confirmed it, from which record, and on what date:

How many Florida residents may be affected?

An estimate is fine. The thresholds are 500 for Department of Legal Affairs notice and more than 1,000 notices for consumer reporting agency notice.

Answer:

Who confirmed it, from which record, and on what date:

Is a third party agent involved, and when did it notify you?

Record the vendor, the date of its notice and what information it has provided.

Answer:

Who confirmed it, from which record, and on what date:

© 2026 Global Digital Forensics, Inc. All rights reserved.

Has law enforcement been contacted or asked for a delay?

Note the agency, the contact and any written request to delay notice.

Answer:

Who confirmed it, from which record, and on what date:

Is the organization a county, municipality or state agency, or is ransomware involved?

Public bodies have 12 hour and 48 hour reporting windows and cannot pay a ransom; record discovery times and the date of the most recent backup.

Answer:

Who confirmed it, from which record, and on what date:

Does a federal regulator's breach rule also apply?

Note any HIPAA, banking or other federal notice obligation, since notice under a primary or functional federal regulator's rules can satisfy the Florida individual notice requirement.

Answer:

Who confirmed it, from which record, and on what date:

Florida Statutes, Rules and Sources

Sources checked November 3, 2026.

1: Fla. Stat. 501.171, Security of confidential personal information (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0500-0599/0501/Sections/0501.171.html

2: Fla. Stat. 282.3185, Local Government Cybersecurity Act (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0200-0299/0282/Sections/0282.3185.html

3: Fla. Stat. 282.318, State Cybersecurity Act (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0200-0299/0282/Sections/0282.318.html

4: Fla. Stat. 282.3186, Ransomware incident compliance (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0200-0299/0282/Sections/0282.3186.html

Get Incident Help Now

If an incident is under way, call the 24/7 hotline first. For readiness work, bring this guide to a free consultation and we will set out the response plan, the evidence to preserve and the deliverables.

Miami office: (786) 219-1210 · **24/7 hotline:** (800) 868-8189 · **Email:** info@evestigate.com

miami-computer-forensics.com

© 2026 Global Digital Forensics, Inc. All rights reserved.