FLORIDA PRACTITIONER GUIDE

Florida Trade Secrets When a Key Employee Leaves

When a key employee leaves for a competitor, Florida law gives employers strong tools: the Uniform Trade Secrets Act, a civil remedy for access to a protected computer after authority ends, restrictive covenants under section 542.335 and, for higher earners, the CHOICE Act. Each one turns on the digital evidence preserved in the first days.

Edition 2026-11-03 · Updated November 3, 2026 · miami-computer-forensics.com/guides/florida-trade-secrets-employee-departure/

A departing employee's laptop, phone and accounts hold the answer to the question every Florida trade secret case turns on: what was taken, how and when. That answer comes from devices preserved before they are wiped, reissued or returned to a vendor, and from accounts suspended rather than deleted.

GDF examines departing employee devices and accounts for Florida employers and their counsel. We establish what information the employee accessed, copied, synced, emailed or printed, and we document it so counsel can put the findings to work in a temporary injunction motion and carry them through trial.



The handling record that keeps a departing employee's devices usable as evidence.

1. What Florida Protects as a Trade Secret

Section 688.002(4) defines a trade secret as information, including a formula, pattern, compilation, program, device, method, technique or process, that derives independent economic value, actual or potential, from not being generally known to or readily ascertainable by others who could profit from it, and that is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. [1]

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

Reasonable secrecy efforts are partly a technical fact. Access controls, permission groups, multifactor authentication, data loss prevention rules, confidentiality banners and audit logging all show the information was protected. We document those controls as they existed during the employee's tenure, because the same configuration records that prove the protection also reveal how the employee reached the data.

2. Misappropriation Means Acquisition, Disclosure or Use

Under section 688.002(2), misappropriation includes acquiring a trade secret by a person who knows or has reason to know it was acquired by improper means, and disclosing or using it without consent in the circumstances the statute lists, including by a person who acquired it under a duty to maintain its secrecy or limit its use. Improper means include theft, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, and espionage through electronic or other means. [1]

Each element maps to artifacts. Acquisition shows up as files staged in archives, copied to removable media, synced to personal cloud storage, uploaded through a browser or forwarded to a personal email account. Disclosure and use show up in the files that later appear on a new employer's systems, in matching document metadata and in communications. We correlate those artifacts into one timeline and separate what the employee's job required from what it did not.

3. Injunctions, Damages and Secrecy in the Courtroom

Florida's Uniform Trade Secrets Act allows a court to enjoin actual or threatened misappropriation and, in appropriate circumstances, to compel affirmative acts to protect a trade secret. A complainant may recover damages for the actual loss and for unjust enrichment not counted in that loss, or a reasonable royalty, and where misappropriation is willful and malicious the court may award exemplary damages of up to twice that amount. Section 688.006 directs the court to preserve the secrecy of an alleged trade secret by reasonable means, such as protective orders, in camera hearings and sealed records. [2] [3] [4]

Threatened misappropriation and affirmative protective acts are why speed matters. A forensic finding that files left on a specific date, on a specific device, supports a motion for relief while the information can still be recovered and its spread contained.

4. Access After Authority Ends Under Section 668.803

Florida provides a civil remedy against a person who, knowingly and with intent to cause harm or loss, obtains information from a protected computer without authorization and causes harm or loss, transmits a program, code or command to a protected computer without authorization, or traffics in a technological access barrier. A protected computer is one used in a business whose information can be reached only through a technological access barrier such as a password, security code, token or key fob. An employee's status as an authorized user ends upon revocation by the owner or upon cessation of employment, and access with a stolen access barrier is access without authorization. [5] [6]

The remedies include actual damages, the violator's profits, injunctive relief and recovery of the misappropriated information and all copies, and the court shall award reasonable attorney fees to the prevailing party. The action must be filed within 3 years after the violation occurred or was or should have

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

been discovered. Post departure sign ins to email, VPN, cloud storage or business applications are the evidence for this claim, so we preserve identity provider and application audit logs before their retention windows close. [7]

5. Restrictive Covenants Under 542.335 and the CHOICE Act

Section 542.335 permits enforcement of a restrictive covenant that is reasonable in time, area and line of business, set out in a writing signed by the person against whom enforcement is sought, and supported by a legitimate business interest that the employer must plead and prove. Legitimate interests include trade secrets as defined in section 688.002(4), valuable confidential business information, substantial relationships with specific prospective or existing customers, customer goodwill tied to a trade name, location or trade area, and extraordinary or specialized training. [8]

Against a former employee, for a restraint not based on trade secrets, a court presumes a post employment restraint of 6 months or less reasonable in time and one longer than 2 years unreasonable; where the restraint protects trade secrets, the presumptions are 5 years or less and more than 10 years. Violation of an enforceable covenant creates a presumption of irreparable injury, and a temporary injunction requires a proper bond. Evidence that a departing employee exported a customer list, synced contacts or downloaded pipeline reports shows the customer relationships the covenant protects are actually at risk. [8]

For higher earners, the Florida CHOICE Act, sections 542.41 through 542.45, adds a second regime. It covers an employee or contractor who earns or is reasonably expected to earn more than twice the annual mean wage of the Florida county where the employer has its principal place of business (or where the employee lives, if the employer is based outside Florida), excluding health care practitioners, who signs a covered noncompete or garden leave agreement of up to 4 years after receiving it at least 7 days before the offer expires, being advised in writing of the right to counsel and acknowledging in writing the receipt of confidential information or customer relationships. On the employer's application, a court must preliminarily enjoin the covered employee from working for anyone else during the noncompete or notice period, and may modify or dissolve the injunction only if the employee shows by clear and convincing evidence, based on nonconfidential information, that a statutory exception applies, such as not performing similar work or using the employer's confidential information or customer relationships. What the employee accessed and took before leaving goes straight to that showing. [9] [10] [11]

6. The First Forty Eight Hours After Notice

Take the laptop, phone and any removable media into controlled custody before IT reimages or reissues them, and record who took them and when. Suspend the accounts rather than deleting them, and document the date access was revoked. Ask the administrators to preserve email, cloud storage, identity provider, endpoint security and data loss prevention logs, and note each one's retention period. Keep the employee's files and any recovered USB drive as they are, so the timestamps an examiner relies on stay intact.

From there, the examination is planned around the claims: which projects and repositories matter, which transfer paths are plausible and which dates bracket the relevant activity. That focus keeps the work proportionate and gets counsel the findings needed for a motion.

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

7. Findings Built for a Florida Courtroom

Our reports tie each finding to the artifact that supports it, state the alternatives considered and record the hash values and chain of custody for every source, so counsel can lay the authentication foundation under section 90.901 and the opinion is built around the reliability elements of section 90.702. GDF experts have testified in federal and state courts, and our work has been accepted by courts. [12] [13]

That same record serves the business. It tells leadership what left, whether it reached a competitor, which customers or projects are exposed and what controls should change before the next departure.

Preserve the Devices Before Anyone Reissues Them

Call as soon as a key employee gives notice under suspicious circumstances or you learn information may have left with them. A free consultation with a senior examiner covers the devices and accounts to preserve today, the claims counsel is weighing, the transfer paths worth examining and the timeline to findings that support a motion.

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

Collect these answers with HR, IT and counsel, describing the devices from records and from the people who handled them, and leave the examination to us.

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

Who left, when, and where did they go?

Record the role, notice date, last day, last authorized access and the new employer if known.

Answer:

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

What specific information is at risk?

Name the projects, customer lists, pricing, source code, designs or processes, and where each is stored.

Answer:

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

What protected that information during the employee's tenure?

List access groups, MFA, data loss prevention, confidentiality agreements and labeling. These support the reasonable secrecy efforts element of section 688.002(4).

Answer:

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

Which devices and accounts did the employee use, and where are they now?

Identify laptops, phones, removable media, email, cloud storage and business applications, with the current custodian of each device.

Answer:

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

Has anything been reset, reissued, deleted or examined already?

Record any reimaging, account deletion, mailbox conversion or informal review, with who acted and when.

Answer:

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

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

When was access revoked, and has anyone signed in since?

Note the revocation date for each account and any alerts of later sign ins, which bear on a claim under section 668.803.

Answer:

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

Is there a signed restrictive covenant or confidentiality agreement?

Note the document, its date, the restraint period and area, and the legitimate business interest it protects under section 542.335.

Answer:

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

Florida Statutes, Rules and Sources

Sources checked November 3, 2026.

1: Fla. Stat. 688.002, Uniform Trade Secrets Act definitions (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0600-0699/0688/Sections/0688.002.html

2: Fla. Stat. 688.003, Injunctive relief (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0600-0699/0688/Sections/0688.003.html

3: Fla. Stat. 688.004, Damages (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0600-0699/0688/Sections/0688.004.html

4: Fla. Stat. 688.006, Preservation of secrecy (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0600-0699/0688/Sections/0688.006.html

5: Fla. Stat. 668.802, Definitions for unauthorized access to a protected computer (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0600-0699/0668/Sections/0668.802.html

6: Fla. Stat. 668.803, Prohibited acts (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0600-0699/0668/Sections/0668.803.html

7: Fla. Stat. 668.804, Remedies (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0600-0699/0668/Sections/0668.804.html

8: Fla. Stat. 542.335, Valid restraints of trade or commerce (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0500-0599/0542/Sections/0542.335.html

9: Fla. Stat. 542.43, CHOICE Act definitions (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0500-0599/0542/Sections/0542.43.html

10: Fla. Stat. 542.44, Covered garden leave agreement (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0500-0599/0542/Sections/0542.44.html

11: Fla. Stat. 542.45, Covered noncompete agreements (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0500-0599/0542/Sections/0542.45.html

12: Fla. Stat. 90.901, Requirement of authentication or identification (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0000-0099/0090/Sections/0090.901.html

13: Fla. Stat. 90.702, Testimony by experts (2026 Florida Statutes)
https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0000-0099/0090/Sections/0090.702.html

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

Talk to a Senior GDF Examiner

Bring this guide to a free consultation. We review your answers, identify what to preserve or test first and set out the work, the timeline 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.