



EXAMINATION REPORT (EXCERPT)

Mobile device compromise assessment

An assessment of whether one iPhone has been compromised, prepared for Ms. Maya R. Alder of Harbor Lane Advisory.

Case	SAMPLE-0001
Prepared for	Maya R. Alder, Harbor Lane Advisory
Device	iPhone 17 Pro (fictional unit), iOS 26.4
Evidence	iOS full file system extraction (sample)
Evidence received	July 13, 2026
Examination completed	July 15, 2026
Report date	July 17, 2026
Prepared by	Jordan Reyes, CFCE, Senior Digital Forensic Examiner

Northgate Examination Partners, LLC. northgate.example.com. Sample, fictional data. Every person, device, app, finding and number in this document is invented. It is not a real case and not a result of any real examination.

1 Executive summary

Ms. Maya R. Alder of Harbor Lane Advisory asked us to establish whether her iPhone has been compromised. She reports that details of a private negotiation reached a competitor and that, since a recent software update, the phone drains its battery faster than before. We examined a full file system extraction of the device, taken on July 13, 2026.

We found no exact match between the device evidence and any known threat indicator. We did find one app, RelayLink Companion, that was installed outside the app store, presents a developer identity that does not match its name, and holds microphone, location and background access. A configuration profile from an unfamiliar organization was added to the device on the same day. Together these form a pattern that monitoring software can produce, and that some legitimate remote-support tools produce as well.

Nothing in this report is a verdict. Each finding is a lead for corroboration, shown with the evidence behind it, the benign explanations we considered, and what we recommend next.

What the evidence supports. An app with monitoring capabilities was installed outside the app store on July 6, 2026. **What it does not establish.** Who installed it, whether it was used, or whether it is the route by which the negotiation details left the phone. **Our recommendation in brief.** Keep the device and the extraction as they are until we have spoken with Ms. Alder; then document, remove and update (section 8).

2 Assignment

Ms. Alder asked whether her phone has been compromised. We set three objects for the examination:

1. Whether spyware, stalkerware or mercenary-spyware indicators are present on the device.
2. Whether apps that were installed outside the app store, or that hold unusually broad access, are present.
3. Whether the device's software level and security settings leave it exposed.

3 What we found, object by object

OBJECT OF THE EXAMINATION	WHAT OUR EXAMINATION SUPPORTS
Whether spyware, stalkerware or mercenary-spyware indicators are present on the device.	We found no known indicator. One pattern, an app and a profile added together, is consistent with monitoring software and needs corroboration.
Whether apps installed outside the app store, or with unusually broad access, are present.	Yes: RelayLink Companion. QuickClean Booster holds broad access, but Ms. Alder installed it herself.
Whether the software level and security settings leave the device exposed.	Moderately. The operating system is behind the current release and Lockdown Mode is off.

4 Assessment at a glance

ANALYZED DATA

48,213

observations prepared for our review

THREAT INDICATOR COMPARISON

0

exact matches against about 648,000
known indicators

FINDINGS

5

1 High, 2 Moderate, 1 Low, 1
Informational

CORRELATION LEADS

7

4 awaiting corroboration

TECHNICAL EXPOSURE

Moderate

the software is behind the current
release

SECURITY CONFIGURATION

79%

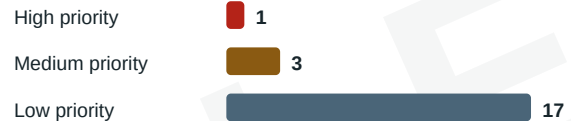
of settings could be established

Findings by rating



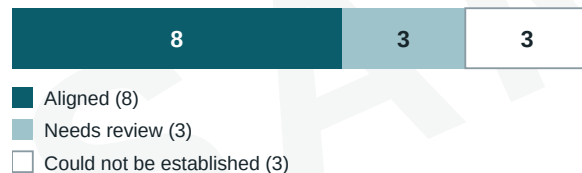
Five findings in all. Ratings describe the importance of the
lead for you, not a verdict on the device.

Applications that did not ship with the device



We reviewed 21 applications and rated them by the access
they hold and how they were installed.

Security settings reviewed (14)



Settings we could not establish from this evidence are left
out of the result; the 79 percent coverage is stated beside it.

Technical exposure: Moderate

We rate technical exposure Moderate. The device is
behind the current vendor release, and three issues
that are known to be exploited apply to the installed
version. Each is fixed in a later release.

Threat indicator comparison

We found no exact match between the device evidence and a library of about 648,000 known threat indicators. One context-only match, rated Low and labeled, concerns a shared analytics address used by many ordinary apps. A result of no findings means that no known indicators were found in the evidence provided. It is not proof that the device is clean.

5 Findings

Each finding carries a rating, the evidence references behind it, our interpretation, the benign explanations we weighed, and what we recommend. This excerpt reproduces three of the five findings in full; F-03 and F-05 appear in the overview only.

REF	FINDING	RATING
F-01	RelayLink Companion: installed outside the app store with broad access Requires review	High
F-02	Configuration profile from an unfamiliar organization Requires review	Moderate
F-03	QuickClean Booster holds location access at all times Informational context	Low
F-04	Operating system is behind the current release Exposure	Moderate
F-05	Lockdown Mode is not enabled Informational context	Informational

F-03 was reviewed and rejected as benign: Ms. Alder recognizes and uses that app. F-05 has not yet been reviewed.

High Requires review. We confirmed this as a lead for corroboration.

F-01. RelayLink Companion: installed outside the app store with broad access

What we found	The app was installed through an enterprise distribution route rather than the app store. The developer identity on the app does not match the name it presents. It holds microphone, location (always) and background access, and it starts with the device.
Evidence references	Analyzed Data, Applications (E-1042) Permission Correlation, RelayLink Companion (E-1043) Correlation analysis, lead L-1 (E-2210)
Our interpretation	These traits are shared by monitoring software and by some legitimate remote-support tools. We found no exact match to a known threat, so this lead rests on behavior, not on a known indicator.
Benign explanations we considered	An employer's IT team could have installed a remote-support tool this way. Ms. Alder reports that the phone is not enrolled with any employer.
What it means for you	If the app was not installed knowingly, it could have captured audio and location.
What we recommend	Ask Ms. Alder when and by whom it was installed. Document it, then remove it. Review the accounts used on the device.

Moderate Requires review. We confirmed this as a lead for corroboration.

F-02. Configuration profile from an unfamiliar organization

What we found A profile named Relay Services is installed on the device. It was added on the same day as RelayLink Companion, July 6, 2026.

Evidence references Security Configuration, configuration profiles (E-3110)
Analyzed Data, timeline (E-1051)

Our interpretation A profile can permit an app to run without the usual store checks. The matching date supports a link with F-01 but does not prove one.

Benign explanations we considered Managed devices carry profiles routinely. This device is reported as unmanaged.

What it means for you Raises the importance of F-01.

What we recommend Identify who issued the profile. Remove it after it has been documented.

Moderate Exposure. We confirmed this finding.

F-04. Operating system is behind the current release

What we found The device runs iOS 26.4. Later vendor releases fix issues that are known to be exploited on this version.

Evidence references Vulnerability Exposure, operating system (E-4001)

Our interpretation Exposure is not compromise. It shows the device could have been reached by a known method, and the evidence does not show that it was.

Benign explanations we considered A device that is a few releases behind is common.

What it means for you Leaves the device open to issues that are already public.

What we recommend Update the operating system after the evidence has been preserved.

6 Scope and methodology

Our examination covered one iPhone, from a full file system extraction. We carried it out in place: we opened the evidence read-only and never copied it into our analysis platform. We recorded a SHA-256 hash of the evidence before analysis began and checked it again at the end; the two matched. The log-based checks cover July 4 to July 13, 2026. Network traffic, cloud accounts and the device's battery behavior were not part of this examination.

We kept evidence and inference apart throughout, weighed benign explanations for each lead, and tied every material statement to a numbered evidence reference. Analysis performed with SectraTEK Full 1.0.0, build 3f9a1c70d2e8.

7 Limitations

- A full file system extraction is a snapshot. It cannot show what happened after it was taken.
- Our log-based checks cover only the period the device kept, July 4 to July 13, 2026.
- We did not examine network traffic, cloud accounts or battery behavior.
- Three security settings could not be established from this evidence.
- A zero result on any dataset is never proof that the device is clean.

8 Recommendations

1. Keep the device and the extraction as they are until the client interview is done.
2. Ask when, where and by whom RelayLink Companion and the Relay Services profile were added.
3. After documenting them, remove the app and the profile, then update the operating system.
4. Change the passwords of the accounts used on the device, from a different device.
5. Consider a separate examination of Ms. Alder's cloud accounts.

9 Examiner

This report was prepared and is signed by the examiner named below.

Jordan Reyes, CFCE

Senior Digital Forensic Examiner
Northgate Examination Partners

Date

July 17, 2026

A Appendix: evidence reference index

Evidence item numbers are kept exactly as recorded in the examination data. The evidence examined is iOS full file system extraction (sample) of iPhone 17 Pro (fictional unit) (device SAMPLE-DEVICE-0001). The SHA-256 value recorded before analysis, and matched at the end, is 5a1f 9c0e 77d2 b4a8 31e6 0c5d 98fa 2b17 (first 16 bytes shown, sample value).

REFERENCE	RECORD	SUPPORTS
E-1042	Analyzed Data, Applications	F-01
E-1043	Permission Correlation, RelayLink Companion	F-01
E-2210	Correlation analysis, lead L-1	F-01
E-3110	Security Configuration, configuration profiles	F-02
E-1051	Analyzed Data, timeline	F-02
E-1060	Permission Correlation, QuickClean Booster	F-03
E-4001	Vulnerability Exposure, operating system	F-04
E-3102	Security Configuration, device posture	F-05

DATE	CUSTODY AND HASH HISTORY
July 13, 2026	Device received from the client. Extraction taken. Hash recorded.
July 14, 2026	Examination run in place. Evidence opened read-only.
July 15, 2026	Final hash check matched the recorded hash. Examination complete.
July 16, 2026	Dossier approved by the examiner and released.

Northgate Examination Partners, LLC

1200 Sample Avenue, Suite 300, Example City, ST 00000

+1 212 555 0170 | casework@example.com | <https://northgate.example.com>

Confidentiality notice. This report is confidential and was prepared solely for the addressee. It states the findings of the examination of the evidence described in it, subject to the limitations in section 7. It must not be copied, disclosed or relied on by any other party without the written consent of Northgate Examination Partners.