FCI

FIRM SECURITY

URGENT INCIDENT RESPONSE

When something is wrong, every minute counts.

FCI provides hands-on forensic investigation for urgent cybersecurity incidents — whatever the surface, wherever the evidence leads. Our work is led by cybersecurity experts who regularly present findings to the FBI, financial regulators, and cyber insurance carriers. This is not an automated process. It is manual, evidence-driven work performed by people who know what examiners and insurers need to see.

30+
years serving financial services

40,000+
endpoints under management

1,000+
incidents successfully responded, mitigated, and documented

SCOPE

What this service covers.

This document outlines FCI's urgent incident response and forensic investigation service. When the firm calls, we don't assume we know what happened. The surface could be an endpoint, an email account, a cloud application, a network, a file share, a user, or something that doesn't fit any of those. Wire transfer fraud, business email compromise, account takeover, ransomware, phishing with malware, unauthorized access, data loss — the starting point is always the same: we listen.

We begin by asking who found the incident, when, and what they observed. From there, FCI scopes the investigation, deploys the right tooling where the evidence lives, isolates what needs to be isolated, and conducts a forensic examination.

GOAL

Help the firm determine what happened — and what it means.

The purpose of every investigation is to give the firm the information it needs to make an informed decision. Not every incident is the same, and the regulatory and insurance implications depend entirely on what the evidence shows. FCI's report is designed to help the firm answer the question that matters most: what kind of incident is this?

INCIDENT OR BREACH DETERMINATION

Non-Reportable Incident | Reportable Incident | Breach

THE PROCESS

Initial Phase: five steps from intake to report.

The initial phase of every investigation follows the same structured process, no matter where the incident sits. What happens after the initial phase depends on the findings: the report may be final, or it may recommend a second phase with a separate scope and estimate.

01 **Intake**

FCI listens to the firm. Who found the incident, when, and what they observed. From that initial conversation, we determine the starting scope of the investigation and what surfaces need to be examined.

02 **Containment & Tool Deployment**

FCI deploys investigation tooling where the evidence lives — endpoints, identity, email, cloud, network, file shares, whatever the situation requires — and isolates the affected systems or accounts. From this point forward, the compromised surface is under FCI's control for the duration of the investigation.

03 **Forensic Investigation**

FCI's team reviews logs, follows the evidence trail, and determines what happened. This is manual, expert-driven work — not just a simple scan. Where the investigation goes depends on what the logs show, what evidence is available, what the user had access to, and what the attackers were able to do. One thing is critical to understand: we can only find what the evidence shows. If the affected surface was not properly protected before the incident — if logging was limited, if key controls were not in place — the investigation may not produce the answers the firm is hoping for.

04 **User Interview**

If needed, FCI speaks directly with whoever first observed the incident and anyone else who saw something relevant. What they saw, when they saw it, and what actions they took can provide context that logs alone cannot.

05 **Report Delivery**

FCI delivers a written report of findings — either a final report if the investigation is conclusive, or an initial report with an estimate for the next phase.

TOOLING

What gets deployed.

FCI deploys investigation tooling to whatever surface the incident implicates. The exact tools vary by situation — remote access, endpoint detection and response, log collection, email forensics, cloud audit review, identity monitoring. What stays constant is the intent: secure access for our team and real-time visibility into what is happening. All tooling is removed when the work is complete.

Access & Visibility

Secure remote access for FCI's team and real-time visibility into the affected surface for the duration of the investigation.

Evidence Collection

Detection, logging, and forensic tooling appropriate to the incident — endpoint, identity, email, cloud, network — so the evidence trail is preserved and investigable.

SETTING EXPECTATIONS

What every firm should understand before an investigation begins.

Incident response is inherently unpredictable. Every case is different — even incidents that start the same way can lead to very different places. FCI will always be transparent about where the investigation is heading, but the following is true for every engagement.

AFFECTED SYSTEMS ISOLATED

Once FCI isolates an affected surface — a device, an account, an application — nobody can use it except FCI. We cannot accept pressure to release it early; the integrity of the investigation depends on it.

UNKNOWN TIMELINE

We do not know in advance how long the investigation will take or when we can release the affected systems. The timeline depends entirely on what the evidence shows.

SCOPE MAY EXPAND

The investigation may not stop where it started. If the compromised user or system had access to other drives, cloud applications, or systems, FCI may need to follow the evidence beyond the original surface.

NO FIXED PRICE BEYOND INITIAL PHASE

Except for the initial phase, additional work cannot be quoted upfront — the cost depends on the environment, the evidence available, and the scope of the compromise. FCI provides an estimate before any additional phase begins.

> "We go where the evidence takes us. Even when we use tools, this is a manual task performed by a team of cybersecurity experts — not an algorithm, not a scan."

INITIAL ENGAGEMENT

Getting started.

The initial engagement covers intake, tool deployment, containment, and the first phase of the forensic investigation. In some cases, five hours is enough to complete the work entirely and produce a final report — but we never know going in. When additional investigation is needed, the firm receives an initial report with findings to date and an estimate before committing further.

INITIAL INVESTIGATION

$1,299

This represents a combined effort across a project manager, cybersecurity expert, lead technician for tool deployment and removal, evidence gathering, review forensics, report preparation, and senior leadership final review and approval of the report. At the end of the initial engagement, FCI delivers either a final report or an initial report with findings to date and an estimate for the next phase.

IF IT TURNS OUT TO BE A FALSE ALARM

If we engage and quickly determine there was no incident — just a false alert, nothing to report — we charge you only for the time we actually spent. That can mean a final price below the initial fee. We never know going in, but if that is where the evidence leads, we will be honest about it and refund any overpayment.

DELIVERABLES

What the firm receives.

Every engagement produces a written report suitable for submission to regulators, home offices, and cyber insurance carriers. Depending on the case, the report may cover areas including but not limited to:

Point of Compromise

How and when the attacker gained access to the environment.

Attacker Activity

What was installed, executed, or used during the incident — and whether it remains active.

Client PII Exposure

Whether personally identifiable information was accessed or exfiltrated.

Data Exfiltration

Whether data was transferred out of the firm's environment.

Account Compromise

Which accounts were affected and what access they provided.

Remediation & Next Steps

What FCI did to contain the incident and what the firm should do to prevent recurrence.

BREACH PREPAREDNESS

If it's a breach, the clock is already running.

When FCI's investigation confirms a breach determination, the situation changes. Regulatory notification timelines start counting. The firm may need to report to FINRA, state regulators, the SEC, or cyber insurance carriers — and depending on the nature and scope of the breach, the FBI may be involved. There is no grace period for getting organized after the fact.

One of the first things regulators and affected individuals will ask about is the firm's existing cybersecurity posture: policy documents, the most recent vulnerability scan, and the latest network penetration testing. If those don't exist — or if they're outdated — it creates an immediate credibility problem at exactly the wrong moment.

> THE QUESTION THEY WILL ASK
>
> *Can you show us your cybersecurity policies and the results of your last vulnerability assessment and network penetration testing?*

FCI maintains an emergency response team that can perform a rapid vulnerability assessment and network penetration testing on a compressed timeline. If the firm needs this work done — because it was never performed, because the results are stale, or because the scope of the breach demands a fresh assessment — FCI can mobilize quickly.

This is not a fixed-price service. Every firm's environment is different, and the scope of the assessment depends on the applicable cyber regulations, the infrastructure involved, the number of endpoints, and the urgency of the regulatory timeline. When the need arises, FCI provides a quote based on what the situation actually requires.

> "The worst time to find out your policies are missing or your last network penetration testing was three years ago is when a regulator is asking for them."

Ready to discuss urgent incident response for your firm?

FCI works with broker-dealers and branch offices, insurance carriers and agencies, and RIAs. Call us to discuss your situation — there is no commitment until you decide to engage.

PHONE
973-227-8878

WEB
fcicyber.com