Capital Investment Club

Security Incident Detection, Triage, Resolution, and Notification Process

Incident detection, triage, containment, resolution, notification decisions, communications, and evidence.

Last updated: 10/05/2025

Purpose

This process defines how CIC detects, triages, investigates, resolves, documents, and communicates security incidents, including notification procedures for affected users, partners, regulators, vendors, and internal stakeholders when required.

This process supplements the Incident Response Policy by providing an operating workflow for the unchecked due diligence requirements around detection, triage, resolution, and notification.

Scope

This process applies to suspected or confirmed incidents involving:

- Unauthorized access.
- Account takeover.
- Privileged access misuse.
- Data exposure.
- Consumer financial data exposure.
- Wallet, grant, pitch, investment, withdrawal, ledger, or reconciliation integrity risk.
- Support identity verification misuse.
- File upload or data export misuse.
- Vendor breach or third-party incident.
- Production infrastructure compromise.
- Malware, endpoint compromise, or suspicious endpoint activity.
- Critical vulnerability exploitation.

Detection Sources

Incidents may be detected through:

- Monitoring alerts.
- Log review.

- User reports.
- Support reports.
- Vendor notifications.
- Security-tool alerts.
- Failed access attempts.
- Financial reconciliation anomalies.
- Public reports.
- Internal testing.
- Audit or assessment findings.

Triage Workflow

Initial triage must:

1. Record the report or alert. 2. Assign an incident owner. 3. Preserve evidence. 4. Classify severity. 5. Identify affected systems, data, users, organizations, transactions, vendors, and integrations. 6. Determine whether containment is required. 7. Escalate to accountable leadership if high impact is possible. 8. Open an incident record.

Severity Classification

Severity	Description
Critical	Confirmed or likely material data exposure, active compromise, financial integrity issue, or severe production impact
High	Strong indication of unauthorized access, significant vulnerability exploitation, or material user impact
Medium	Suspicious activity requiring investigation or limited impact incident
Low	Informational event or minor issue with no material impact

Containment and Resolution

Containment may include:

- Disabling accounts or sessions.
- Revoking credentials.
- Rotating secrets.
- Blocking IPs or traffic.
- Disabling affected features.
- Pausing financial workflows.
- Revoking vendor access.
- Rolling back deployments.
- Applying patches.
- Restoring from backup.

- Preserving affected records for investigation.

Resolution must address the root cause where practical and document residual risk.

Notification Decision Process

CIC must evaluate whether notification is required based on:

- Type of data involved.
- Number of users affected.
- Jurisdictional requirements.
- Contractual obligations.
- Partner or provider requirements.
- Risk of harm.
- Whether consumer financial data was affected.
- Whether regulators, law enforcement, or payment/financial partners must be notified.

Notification decisions must be documented even when CIC concludes notification is not required.

Notification Recipients

Depending on incident facts, notification may include:

- Affected users.
- Affected organizations.
- CIC leadership.
- Support and operations teams.
- Vendors or subprocessors.
- Financial API providers or payment partners.
- Regulators where legally required.
- Law enforcement where appropriate.

Notification Content

Notifications should be clear, accurate, and approved before release.

Content may include:

- What happened.
- When it happened.
- What information or systems were affected.
- What CIC did to contain or resolve the issue.
- What the user should do.
- Contact or support path.
- Updates or follow-up timing.

Post-Incident Review

After material incidents, CIC must perform a post-incident review covering:

- Timeline.
- Root cause.
- Impact.
- Response effectiveness.
- Notification decision.
- Control gaps.
- Remediation actions.
- Preventive improvements.
- Evidence retained.

Evidence

CIC should retain:

- Incident record.
- Alert or report source.
- Investigation notes.
- Logs and screenshots.
- Timeline.
- Containment actions.
- Notification analysis.
- Notifications sent.
- Remediation tracker.
- Post-incident review.

Review

This process must be reviewed at least annually and after material incidents.