ACTION _ PLAN

Table of Contents

Executive Summary

Incident ID: FFCU-IR-RW-24-1201
Organization: FinanceFirst Credit Union
Incident Type: Ransomware with suspected data exfiltration (REvil/Sodinokibi)
Detection Date: December 11, 2025
Detection Time: 06:25 AM
Severity: CRITICAL

FinanceFirst Credit Union experienced a confirmed ransomware incident impacting multiple internal systems, including file servers, email, backups, and the primary member database. Core banking, ATMs, and digital banking platforms remained operational due to effective isolation controls.

Following forensic assessment and executive review, Option C: Complete Network Rebuild was approved to ensure full eradication of attacker persistence, reduce reinfection risk, and align with regulatory best practices. External forensic, legal, and cyber insurance partners were engaged.

This plan documents response actions, executive decisions, regulatory alignment, recovery timelines, and validation metrics in accordance with NIST SP 800-61 Rev. 3, GLBA, NCUA, and FFIEC requirements.

INTRODUCTION

This Incident Response Action Plan (IRAP) outlines the structured response to the ransomware attack detected at FinanceFirst Credit Union on December 1, 2025. The plan follows the NIST Incident Response Lifecycle (SP 800-61 Rev. 3) and is tailored to the regulatory environment governing financial institutions, including GLBA, NCUA, and FFIEC requirements.

The purpose of this document is to provide a clear, actionable framework for the Computer Security Incident Response Team (CSIRT) and key stakeholders, ensuring coordinated containment, eradication, recovery, and post-incident activities. This plan reflects decisions made in response to injections throughout the 72-hour simulation and is designed to serve as both an operational guide and an auditable record of response actions.

PHASE 1: DETECTION AND ANALYSIS Incident ID: FFCU-IR-RW-24-1201

1.1 INITIAL ASSESSMENT AND TRIAGE

- This is a confirmed security incident because there is direct evidence of malicious activity (encryption, ransom note, service disruption).
- The type of incident is ransomware attack with potential data exfiltration, likely REvil/Sodinokibi.
- The organization's critical business functions (file services, email, database server) are impacted, indicating a widespread compromise.

1.2 EVIDENCE PRESERVATION

We are going to employ technical and administrative steps in the evidence preservation during this incident response.

1.2.1 Technical Steps

- Isolate but DO NOT power off affected systems
- Disconnect compromised servers/workstations from the network to stop ransomware spread while maintaining volatile memory.
- Capture forensic images of impacted devices
- Memory dumps for servers with active encryption processesFull disk images for servers/workstations containing ransom notes
- Secure and export security logs
- Collect logs from SIEM, Windows Event Logs, PowerShell logs, firewall logs, VPN logs, AD logs.
- Preserve the ransom note and file indicators
- Hash values, timestamps, and filenames of encrypted files.
- Initiate formal chain-of-custody documentation

1.2.2 Administrative Steps

- Restrict employee access to affected systems.
- Prevent accidental alteration of logs.
- Notify legal counsel to apply attorney–client privilege to evidence handling

1.3 SCOPE DETERMINATION

This is a multi-system, multi-location ransomware incident with possible data theft, affecting core business services and creating immediate operational and reputational risk. The details of affected and non-affected systems are as follows:

1.3.1 Critical servers encrypted:

- 8/12 file servers
- Primary member database server
- Email server
- Backup server
- Workstations: 45 endpoints impacted.
- Compromised credentials: Domain admin credentials used for lateral movement.

1.3.2 Non-Affected Systems

- Core banking (isolated AS/400 environment)
- Online banking portal (third-party cloud)
- Mobile banking app
- ATM network
- Network infrastructure

1.3.3 Threat Behavior Indicators

- Ransomware variant: REvil/Sodinokibi
- Encryption start time: 6:25 AM
- Suspicious PowerShell activity for 3 weeks
- Backups encrypted before production systems
- Likely long-dwell intrusion (3 weeks inside the network).

1.3.4 Business Impact

- Headquarters administrative functions down
- No email access.
- Payroll at risk.
- Branches partially operational.
- Members are still able to access online/mobile banking.

1.4 SEVERITY CLASSIFICATION

The severity of this ransomware incident happening in a financial institution like FinanceFirst Credit Union is classified as CRITICAL for the following reasons:

1.4.1 High Impact to critical systems

- Member database server encrypted.
- Email is down.
- The backup server is compromised.

1.4.2 Potential Data Exfiltration

- Attackers claim to have 3 weeks' worth of stolen data
- Stolen data includes SSNs, account numbers, payroll data(GLBA-protected)

1.4.3 Disruption to Business Operations

- Members cannot access key services.
- Payroll at risk.
- HQ functions are severely impaired.

1.4.4 Regulatory and Legal Exposure

Gramm-Leach-Billey Act (GLBA), Federal Financial Institutions Examinations Council(FFIEC), National Credit Union Administration(NCUA), and other state breach laws triggered if exfiltration is confirmed.

1.4.5 Ransomware active in Environment

- Continued lateral movement possible.
- Attackers may still be inside the network.

PHASE 2: CONTAINMENT Incident ID: FFCU-IR-RW-24-1201

2.1 SHORT-TERM CONTAINMENT ACTIONS (IMMEDIATE – FIRST 0–4 HOURS)

Objectives: Stop spread, preserve evidence, maintain essential business operations.

2.1.1 Technical Actions:

2.1.1.1 Isolate Affected Systems Immediately

- Disconnect all compromised servers (file servers, email server, database server, backup server) from the network.
- Disable network ports for affected workstations.
- Purpose: Stop encryption spread and prevent attackers from maintaining access.

2.1.1.2 Block Command-and-Control (C2) Communication

- Apply firewall rules to block suspicious outbound IPs and TOR addresses.
- Implement network segmentation urgently to isolate critical systems.

2.1.1.3 Disable Compromised Accounts

- Immediately reset all domain admin credentials found compromised.
- Force company-wide password reset.

2.1.1.4 Preserve Evidence

- Acquire forensic images of affected servers.
- Export SIEM, firewall logs, PowerShell logs.
- Document all steps, ensuring chain of custody.

2.2 LONG-TERM CONTAINMENT STRATEGY (4–24 HOURS)

Objective: Stabilize environment, prevent reinfection, prepare for eradication and recovery.

2.2.1 Technical Measures

2.2.1.1 Network Segmentation Hardening

- Separate critical assets (core banking, CRM, ATMs, cloud systems) from production networks.
- Apply least-privilege access.

2.2.1.2 Backdoor Identification & Removal

- Work with forensic team to locate persistent mechanisms:
- Scheduled tasks
- Registry run keys
- Dropped malware
- Stolen credentials
- Remote access tools
- Remove after full analysis.

2.2.1.3 Implement Temporary Monitoring Enhancements

- Deploy endpoint detection tools (EDR).
- Enable advanced logging (PowerShell transcript logging, DNS logging, firewall verbose logging).

2.2.1.4 Secure Clean Zones

- Create a clean VLAN for safe systems.
- Move essential workloads to cloud services where applicable.

2.3 BUSINESS CONTINUITY MEASURES

Because branch operations rely heavily on the core banking system (which is not affected), continuity actions focus on enabling minimal services.

2.3.1 Maintain Critical Banking Services

- Keep core banking system online for deposits/withdrawals.
- Ensure ATMs remain operational (isolated network).
- Offer manual fallback process for loan operations.

2.3.2 Internal Workarounds

- Enable temporary Gmail/Office365 cloud communication for staff.
- Use encrypted external storage for essential documents.
- Activate manual payroll preparation procedures to meet Wednesday deadline.

2.3.3 Communication

- Daily updates to executives, CSIRT, communications team.
- Notify staff about restricted systems, temporary workflows.

2.4 EXTERNAL RESOURCE ENGAGEMENT

2.4.1 Forensic Investigation Firm (Recommended)

Reason:

- Attack is advanced (REvil), multi-week dwell time, data exfiltration, credential theft.
- Cost: $35,000 (as stated).
- Value: Verifies TTPs, helps eradicate persistence, supports regulatory evidence.

2.4.2 Ransomware Negotiation Specialist (Conditional Recommendation)

Consider only if the ransom option is being evaluated.
Provides:

- Communication expertise
- Validation of decryption reliability
- Lower risk of reinfection

2.4.3 Legal Counsel (Strongly Recommended)

Justifications:

- GLBA and multiple state laws require guidance.
- Required for breach notification timelines and liability management.

2.4.4 Cyber Insurance Carrier (Mandatory)

Reasons:

- Must notify carrier early or risk claim denial.
- Insurance may cover forensics, recovery, notification, PR, and ransom negotiation.

2.5 CONTAINMENT DECISION SUMMARY

1. Should affected systems be disconnected? YES
Justification:

- Ransomware actively spreads.
  - Encryption observed on many servers.

- C2 communication must be broken.

2. Should the entire network be shut down? NO (Partial Shutdown Only)
Reason:

- Core banking, ATMs, online banking are unaffected and isolated.
- Full shutdown would cause massive operational damage.
- Segmented partial shutdown is safer and less disruptive.

3. Should branches close? NO, but operate at reduced capability
Reason:

- Branches can continue with the core banking system.
- Closing branches increases customer panic and reputational damage.

4. Communication Strategy Regarding Member Notification
Recommendation: Do NOT notify members yet (in containment phase)
Reasoning:

- Member notification before confirming exfiltration may cause unnecessary panic.
- Preliminary evidence suggests encryption but not confirmed leakage at this stage.
- Must wait for forensic verification before public disclosure.

However:

- Prepare draft notifications pending forensic confirmation.
- Comply with GLBA and state timelines once breach confirmed.

PHASE 3: ERADICATION AND RECOVERY Incident ID: FFCU-IR-RW-24-1201

3.1Objective:

To eradicate all ransomware artifacts, restore business operations through a secure network rebuild, validate systems before return-to-service, and ensure compliance with regulatory notification and validation requirements.

3.2 Simulation Decision Context:

Based on forensic findings and executive review, Option C (Complete Network Rebuild) was selected. This aligns with the forensic team's recommendation, ensures total eradication, minimizes reinfection risk, and supports long-term security hardening.

3.3 ERADICATION STRATEGY

Goal: Eliminate attacker presence, backdoors, and compromised credentials to prevent reinfection.

Action	Method	Timeline
Credential Remediation	Reset all domain, service, and local admin passwords; implement MFA.	Hours 0–12
Malware & Backdoor Removal	EDR full scan; manual removal of IOCs; wipe and rebuild infected hosts.	Hours 12–36
Patch Vulnerabilities	Apply critical patches to Windows Server, Exchange, and network devices.	Hours 36–48
Network Segmentation Enforcement	Implement new VLANs, firewall rules, and micro-segmentation.	Hours 48–72

3.4 RECOVERY APPROACH AND TIMELINE

Strategy: Complete Network Rebuild (Option C) – Phased by business criticality.

Priority	System / Service	Recovery Method	Timeline	Owner
P1	Core Banking (AS/400)	Integrity check; maintain isolated ops	Ongoing	IT Ops
P1	Email (Office 365)	Restore from Microsoft 365 backup	Day 1–2	Infrastructure
P2	Member Database	Restore from 45-day backup + log replay	Day 2–5	DB Admin
P2	File Servers	Rebuild from gold image + restored clean data	Day 3–7	Systems Team
P3	Internal Apps	Redeploy from source; data validation	Day 5–10	Development
P4	Non-critical Services	Staggered deployment after P1–P3 stable	Day 10+	IT Ops

3.5 VALIDATION AND TESTING PROCEDURES

Before any restored system was approved for production use, the following validation steps were performed:

- Cryptographic Integrity Checks
  - SHA-256 checksums compared between backup and restored datasets
- Transaction Sampling
  - Randomized audit of member balances, payroll records, and transaction logs
- Log Replay Validation
  - Database transaction logs replayed and reconciled
- Malware Scanning
  - EDR scan confirms 0 malicious artifacts
- User Acceptance Testing (UAT)
  - Business owner sign-off required

Only systems passing 100% validation were authorized for go-live.

Goal: Ensure restored systems are secure, compliant, and functionally sound.

Test Type	Procedure	Compliance Check
Security Scan	Run Tenable/Nessus vuln scan; EDR malware scan.	NCUA/GLBA security control validation.
Functional UAT	Business unit sign-off on core banking, lending, member services workflows.	FFIEC CAT testing alignment.
Data Integrity	Compare restored data with backup checksums; sample audit of member balances.	HIPAA/PCI DSS data integrity requirement.
Performance & Load Test	Simulate peak transaction volume; validate API integrations.	Core banking resilience per FFIEC guidelines.
Backup Test	Perform test restoration of critical systems.	NCUA backup adequacy verification.

Deliverable: Validation Certificate signed by CISO, Compliance Officer, and Business Lead.

Validation success criteria

Test area	Success threshold
Malware detection	0 threats detected post-eradication
Data integrity	100% match with audit logs
Backup restore test	100% successful restore
Vulnerability scan	No critical or high findings
Authentication controls	MFA enforced on 100% privileged accounts
Performance testing	≥ 99.9% transaction success rate

3.6 RETURN TO NORMAL OPERATIONS

Goal: Transition from recovery to BAU with enhanced monitoring.

Step	Activity	Timeline
Phased Reintegration	Reconnect network segments with increased monitoring.	Day 7–14
Stakeholder Notification	Notify members, employees, and regulators of restored services.	Day 10
Post-Recovery Monitoring	30-day enhanced SIEM alerting and weekly vulnerability scans.	Day 14–44
Documentation Update	Update IR plan, network diagrams, and BCP/DRP with new architecture.	Day 21
Lessons Learned Integration	Handoff to Phase 4 for formal review and improvement planning.	Day 30

3.7 RACI MATRIX

Activity	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)
Credential Reset & MFA Rollout	Security Team	CISO	IT Ops, HR	All Employees
System Rebuild from Gold Images	Infrastructure Team	IT Director	Security, App Owners	Executive Leadership
Data Migration & Validation	Database Team	Data Governance Lead	Compliance, Business Units	CISO, COO
Vulnerability Patching	Systems Team	IT Director	Security, Vendors	IT Ops
Security & Compliance Testing	Security & Compliance	CISO	External Auditor, Legal	Board, NCUA
Stakeholder Communications	Comms Officer	CEO	Legal, Compliance	Members, Employees, Media
Monitoring & Handoff to Phase 4	IR Manager	CISO	IT Ops, Security	Executive Team

3.8 COMMUNICATION TIMELINE FOR RECOVERY UPDATES

Time	Audience	Key Message	Channel
Daily	Executive Leadership	Recovery progress, timeline updates, resource needs, risks.	Secure Video Conference
Daily	Employees	System availability status, temporary workarounds, support contacts.	Email, Intranet
Weekly	NCUA / Regulators	Formal written update on recovery, evidence of secure restoration.	Secure Regulatory Portal

After P1 Live	Members	Service restoration notice, apology, reassurance of security.	Website Banner, Email
As Needed	Media / Public	Holding statement: Recovery in progress, member security is priority.	Press Release

3.9 COMMUNICATION TEMPLATES

Internal Holding Statement

"FinanceFirst Credit Union is currently responding to a cybersecurity incident. Core banking services remain operational. Certain internal systems are temporarily unavailable while security teams work to restore services safely. Further updates will be provided daily."

Member Notification (Post-Recovery)

"We recently experienced a cybersecurity incident that affected some internal systems. There is no evidence at this time of unauthorized access to your accounts. We have enhanced our security controls and restored services. Your trust and security remain our highest priority."

PHASE 4: POST-INCIDENT ACTIVITIES Incident ID: FFCU-IR-RW-24-1201

A formal account of the post-incident activities undertaken following the ransomware attack on FinanceFirst Credit Union is provided. These actions are described and consistent with NIST SP 800-61 Rev. 3 guidance and reflect industry expectations for financial institutions subject to Gramm-Leach-Bliley Act(GLBA), Federal Financial Institutions Examination Council (FFIEC), and National Credit Union Administration (NCUA) supervisory requirements.

4.1 POST-INCIDENT REVIEW AND LESSONS LEARNED

Following stabilization of critical business operations, FinanceFirst initiated a structured post-incident review to document the incident comprehensively, assess organizational performance, and identify opportunities for improvement. The review was conducted within 72 hours of operational recovery and included representatives from the CSIRT, Cybersecurity, IT Operations, Legal and Compliance, Corporate Communications, Human Resources, and Executive

Management. External forensic consultants also contributed key findings regarding the attack timeline and threat actor behavior.

4.1.1 Lessons Learnt:

- **Comprehensive documentation is critical for effective incident management:** Consolidating all logs, forensic data, communications, and decisions into a single incident dossier enabled accurate analysis, supported regulatory reporting, and strengthened legal defensibility.
- **Existing controls and practices provided key operational advantages:** The isolation of the core banking system, uninterrupted cloud services, strong executive support, and disciplined CSIRT documentation helped limit operational disruption.
- **Critical gaps in security architecture increased the severity of the incident:** Weak phishing defenses, inadequate segmentation, insufficient detection tuning, and exposed backups allowed the attacker to persist undetected and caused widespread encryption.
- **Regular IR plan testing is essential for coordinated response:** The absence of prior exercises contributed to early uncertainty about roles, escalation paths, and decision-making authority. Routine testing would improve team readiness.
- **Privilege mismanagement creates significant organizational risk:** The lack of multi-factor authentication and privileged access controls enabled compromise of domain administrator credentials, which the attacker used to escalate access.
- **Backup resilience must be a priority:** Backups connected to production networks were easily targeted and encrypted. Implementing immutable, offline, or air-gapped backups is essential to ensure recovery options remain intact.
- **Early detection capabilities must be strengthened:** The attacker's three-week dwell time demonstrates that monitoring rules and SIEM coverage were inadequate. Enhancing detection engineering is necessary to reduce attacker persistence.

4.2 ROOT CAUSE ANALYSIS

A structured root cause analysis was conducted using the Five Whys methodology. This analysis established that the fundamental drivers of the incident were systemic rather than isolated technical failures.

The ransomware attack succeeded primarily due to weak email security controls that allowed malicious attachments to be delivered and executed. Once inside, the malware was able to run

because privileged access management and multi-factor authentication were not in place, enabling compromise of domain administrator credentials. The attacker then moved laterally for three weeks without detection because the network lacked proper segmentation and had significant detection engineering gaps. Privileged credentials were easily compromised due to widespread reuse of domain admin accounts and the complete absence of MFA. Finally, the attacker was able to encrypt both backups and production servers because the backup environment was not hardened, remained reachable from production networks, and lacked immutability protections.

4.2.1 Root Causes:

- Inadequate email security controls
- Lack of privileged access management and MFA
- Poor network segmentation
- Insufficient detection engineering and SIEM tuning
- Backups not architected for ransomware resilience
- Incident response plan not tested, resulting in initial coordination delays

These root causes reflect architectural, procedural, and governance gaps that increased the organization's exposure and impeded timely detection and containment.

4.3 IMPROVEMENT RECOMMENDATIONS

Based on the findings of the post-incident review, FinanceFirst developed a comprehensive improvement program spanning people, processes, and technology. These recommendations are designed to enhance resilience, strengthen detection and response capabilities, and align cybersecurity practices with regulatory expectations.

4.3.1 People , Training and Workforce Preparedness

- Implement a revised organization-wide security awareness program, including monthly phishing simulations and mandatory remediation training for users who fail.
- Provide specialized training for privileged administrators, SOC analysts, and incident responders focused on ransomware, credential security, and forensic readiness.
- Conduct quarterly incident response exercises, ensuring participation from IT, Legal, Communications, and executive leadership.

4.3.2 Process, Governance, IR Planning, and Business Continuity

- Update the Incident Response Plan to incorporate ransomware-specific procedures, clearer escalation thresholds, legal review checkpoints, and predefined communication templates.
- Strengthen breach notification workflows to ensure compliance with GLBA and state breach laws, including timelines, evidence documentation, and regulatory liaison protocols.
- Enhance Business Continuity and Disaster Recovery procedures, incorporating ransomware scenarios, manual fallback strategies, and cross-departmental coordination.
- Expand third-party risk assessments to evaluate vendor preparedness for ransomware and data recovery support.

4.3.3 Technology, Security Architecture and Technical Controls

- Implement a Privileged Access Management (PAM) solution with MFA enforcement for all privileged accounts.
- Introduce Zero Trust controls, including micro-segmentation of high-value assets and restrictions on east-west network traffic.
- Modernize SIEM and detection engineering to ensure coverage of common ransomware TTPs, including PowerShell abuse, credential theft, and data exfiltration.
- Deploy immutable and air-gapped backup solutions and enforce a 3-2-1 backup strategy.
- Upgrade endpoint and email security platforms to include behavioral ransomware detection, advanced sandboxing, and hardened macro policies.
- Implement CIS benchmark hardening for domain controllers, file servers, and other critical infrastructure.

4.4 PERFORMANCE MEASUREMENT AND METRICS

To enable continuous improvement and provide objective evidence of cybersecurity readiness, FinanceFirst will implement a set of Key Performance Indicators (KPIs) for monitoring incident response maturity and organizational resilience.

KPI	Definition	Target
Mean Time to Detect (MTTD)	Time from compromise to detection	< 6 hours
Mean Time to Respond (MTTR)	Time from detection to containment	< 2 hours
Mean Time to Contain (MTTC)	Time to isolate threat	< 1 hour
Mean Time to Recovery (MTTR)	Time to restore business operations	< 48 hours
Phishing Failure Rate	Percentage of employees clicking on simulated phishing	< 5%
Incident Response Test Frequency	Tabletop / functional testing	Quarterly
Backup Integrity Pass Rate	Successful restore tests	100%
Privileged Access Review Frequency	Review of admin accounts and rights	Monthly
SIEM Detection Coverage	Critical TTP detections in place (MITRE ATT&CK)	95%

CONCLUSION

This Incident Response Action Plan provides a comprehensive, phased approach to managing the ransomware incident at FinanceFirst Credit Union. By following the NIST IR lifecycle and incorporating regulatory requirements, the plan ensures a balanced response that prioritizes member security, business continuity, and legal compliance.

The Complete Network Rebuild strategy (Option C) was selected to eliminate attacker persistence, rebuild a more secure architecture, and ensure long-term resilience. While recovery will take 14–21 days, this approach minimizes reinfection risk and aligns with forensic and regulatory recommendations.

Post-incident activities will focus on continuous improvement through structured lessons learned, root cause analysis, and measurable security enhancements. This plan not only addresses the immediate incident but also strengthens FinanceFirst's security posture against future threats.