COMMUNICATION _ PORTFOLIO

Table of Contents

1.INTERNAL NOTIFICATIONS (CISO, CEO, CSIRT)

To: CISO (Preparation)
Subject: Urgent: Suspected Ransomware Incident - Initial Findings

At 06:45 AM this morning, we observed a mass file encryption activity and a ransom note on multiple servers. Preliminary indicators point to a ransomware event. See the summary of the incident below:

Incident Details:
Incident Number: FFCU-IR-RW-24-1201
Detection Time: Monday, December 1, 06:45 AM
Severity Level: Critical
Incident Type: Ransomware attack

Affected Systems:

- 8 of 12 file servers encrypted (Windows Server 2019)
- Primary database server encrypted (member account database)
- Email server encrypted (Microsoft Exchange)
- Backup server encrypted (Veeam backup repository)
- 45 workstations are encrypted across the headquarters and 3 branch locations
- 340 GB data potentially exfiltrated
- 85,000 members impacted

Systems NOT Affected (so far):

- Core banking system (IBM AS/400 mainframe - isolated network segment)
- Online banking portal (cloud-hosted by third-party vendor)
- Mobile banking app (cloud-hosted by third-party vendor)
- Network infrastructure (routers, switches, firewalls)
- ATM network (separate isolated network)

Additional Findings:

- Ransomware appears to be REvil/Sodinokibi variant based on file extensions (.sodinokibi)
- Encryption started at approximately 6:25 AM (20minutes before the report)
- Security logs show suspicious PowerShell activity starting 3 weeks ago
- Evidence of lateral movement using compromised domain administrator credentials
- Backup server was encrypted 2 hours before production systems

Business Impact:

- Loss of access to shared drives, operational files, and internal documentation
- Users can’t access the shared folder.

- Branch operations are limited because only core banking system are accessible for basic transactions
- Headquarters administrative functions severely impaired
- High likelihood of delayed payroll processing
- Email service outage, reducing internal communication capability
- Administrative functions severely impaired (loan processing, account onboarding, internal reporting)
- Initial reputational risk due to service disruption

Immediate Actions Required:
1. Isolate affected servers from the network per containment protocol.
2. Engage/activate CSIRT and start evidence preservation.
3. Initiate contact with external forensic and negotiation specialists.

Request:
Kindly authorize a $50,000 emergency fund for forensics and negotiation support. I recommend activating our incident command structure and limiting internal communications to the IR team until we have confirmed the entire scope of the incident.

I will provide a 30-minute status update.

Kind regards,
Incident Response Manager.

2. INTERNAL NOTIFICATION: CEO

To: CEO (Detection & Analysis)
Subject: Incident Status Update - FFCU-IR-RW-24-1201 (Monday, December 1, 06:45 AM)

Executive Summary:
We are responding to a Ransomware incident that was detected at 06:45 AM on Monday, December 1. The incident is currently classified as Critical and below is a summary of the current situation and our response so far.

Current Status:

Systems Affected:
- 8 of 12 file servers encrypted (Windows Server 2019)
- Primary database server encrypted (member account database)
- Email server encrypted (Microsoft Exchange)
- Backup server encrypted (Veeam backup repository)
- 45 workstations are encrypted across the headquarters and 3 branch locations

- 340 GB data potentially exfiltrated
- 85,000 members impacted

Data at Risk:
Preliminary analysis indicates potential compromise of multiple sensitive data categories, including:

- Full member database (names, SSNs, account numbers, balances)
- Employee HR and payroll records
- Internal communications and emails
- Loan application documents and financial statements
- Backup archives stored on the compromised Veeam server

At this stage, exfiltration is suspected due to the attacker's claims and early forensic indicators, but not yet confirmed.

Business Impact:

- Loss of access to shared drives, operational files, and internal documentation
- Users can’t access the shared folder.
- Branch operations are limited because only core banking system are accessible for basic transactions
- Headquarters administrative functions severely impaired
- High likelihood of delayed payroll processing
- Email service outage, reducing internal communication capability
- Administrative functions severely impaired (loan processing, account onboarding, internal reporting)
- Initial reputational risk due to service disruption

Estimated Recovery Time:

- Initial containment and stabilization: 4 - 6 hour.
- System triage and forensic validation: 12 - 24 hours.
- Partial restoration of critical functions: 24 - 48 hours (dependent on decryption/rebuild decisions).
- Full operational restoration: 5 - 10 days, depending on system integrity and recovery method selected.

Actions Taken:

1. Isolated affected servers and workstations from the network to prevent further spread.
2. Activated CSIRT and initiated forensic evidence preservation in line with NIST 800-61 guidance.

Next Steps:

1. Complete forensic assessment to confirm the scope of data exfiltration and identify persistence mechanisms.
2. Present recovery pathway options to leadership (pay ransom, rebuild, or hybrid) and initiate execution upon approval.

Resource Requirements:

- External forensic investigation support (initial 48-hour engagement).
- Additional system administration and network engineering bandwidth for containment and rebuild.

Decision Required: Leadership input is required on the preferred recovery strategy, specifically:

- Approve external forensic engagement
- Authorize emergency funding
- Approve communications plan/spokesperson
- Authorize engagement with ransomware negotiators and potential ransom payment.
- Approve for CSIRT to proceed with a full system rebuild and extended recovery timeline

This decision will set the overall incident response posture, determine restoration speed, regulatory posture, and internal/external impact.

I will update you within 60 minutes with confirmed scope and recommended next steps.

Kind Regards,
Incident Response Manager.

3.INTERNAL NOTIFICATION: CSIRT

To: CSIRT Members (Containment & Eradication)

Subject: CSIRT Action Required - Ransomware Suspected

Dear Team,
We have a suspected ransomware event with file server encryption and a ransom note, and the Computer Security Incident Response Team (CSIRT) has been activated in response.

Incident Details:
Incident Number: FFCU-IR-RW-24-1201
Detection Time: Monday, December 1, 06:45 AM
Severity Level: Critical
Incident Type: Ransomware attack

Affected Systems:

- 8 of 12 file servers encrypted (Windows Server 2019)
- Primary database server encrypted (member account database)
- Email server encrypted (Microsoft Exchange)
- Backup server encrypted (Veeam backup repository)
- 45 workstations are encrypted across the headquarters and 3 branch locations
- 340 GB data potentially exfiltrated
- 85,000 members impacted

Immediate Actions Required:

1. All CSIRT members should check in via the secure communication channel
2. Review your assigned role and responsibilities
3. Ensure you have access to all necessary tools and systems
4. Stand by for the initial incident briefing in 15 minutes.

Please note: Do not discuss this incident via email or public channels.

The following actions are to be executed immediately:

1. Maintain isolation of affected hosts; do not power-cycle encrypted systems unless instructed.
2. Collect volatile logs and preserve images (follow chain of custody).
3. Disable exposed credentials and rotate admin passwords where possible.
4. Provide a list of affected hosts and confirm backup integrity.

Kind Regards,
Incident Response Manager.

4. EXECUTIVE BRIEFING AND RECOMMENDATIONS

To: CEO, CFO, COO, General Counsel (Containment & Eradication)
Subject: Incident Status Update
FFCU-IR-RW-24-1201/Monday, December 1, 06:45 AM

Executive Summary:
We are responding to a Ransomware incident that was detected at 6:45 AM on December 1st, 2024.

The incident is currently classified as Critical, and below is a summary of the current situation and our response so far:

Current Status: Immediate containment initiated.

Systems Affected:

- 8 of 12 file servers encrypted (Windows Server 2019)
- Primary database server encrypted (member account database)
- Email server encrypted (Microsoft Exchange)
- Backup server encrypted (Veeam backup repository)
- 45 workstations are encrypted across the headquarters and 3 branch locations
- 340 GB data potentially exfiltrated
- 85,000 members impacted

Data at Risk: A preliminary analysis of the incident indicates potential compromise of multiple sensitive data categories, including:

- Full member database (names, SSNs, account numbers, balances)
- Employee HR and payroll records
- Internal communications and emails
- Loan application documents and financial statements
- Backup archives stored on the compromised Veeam server

At this stage, exfiltration is suspected due to the attacker's claims and early forensic indicators, but not yet confirmed.

Business Impact:

- Loss of access to shared drives, operational files, and internal documentation
- Users can't access the shared folder.
- Branch operations are limited because only the core banking system is accessible for basic transactions.
- Headquarters administrative functions severely impaired.
- High likelihood of delayed payroll processing.
- Email service outage, reducing internal communication capability.
- Administrative functions severely impaired (loan processing, account onboarding, internal reporting).
- Reputational risk due to service disruption.

Estimated Recovery Time:

- Initial containment and stabilization: 4 - 6 hours.
- System triage and forensic validation: 12 - 24 hours.
- Partial restoration of critical functions: 24 - 48 hours (dependent on decryption/rebuild decisions).
- Full operational restoration: 5 - 10 days, depending on system integrity and recovery method selected.

Actions Taken:

- Isolated affected servers and workstations from the network to prevent further spread.
- Activated CSIRT and initiated forensic evidence preservation in line with NIST 800-61 guidance.

Next Steps:

- Complete forensic assessment to confirm the scope of data exfiltration and identify persistence mechanisms within the next 4hours.
- Engage external forensic specialists support (initial 48-hour engagement) and implemented privileged credential resets across impacted domains.
- Recovery pathway options to decide on (pay ransom, rebuild, or hybrid) and initiate execution upon approval.
- Prepare drafts for regulatory notification, member notification, public statement, media statement, and employee communication for approval.
- Limit both internal and external communications and authorize recognized spokesperson.

Resource Requirements:

- Additional system administration and network engineering bandwidth for containment and rebuild.

Optional, depending on direction chosen:

- Ransomware negotiation services.
- Expanded cloud infrastructure or temporary hardware for parallel rebuild.
- Member support resources (call center expansion, credit monitoring services).

Decision Required: Leadership input is required on the preferred recovery strategy, specifically:

- Approve external forensic specialists and implementation of privileged credential resets across impacted domains.
- Authorize emergency funds and emergency spending up to insurer limit as needed to maintain minimal external disclosure.
- Approve the Internal and external communications plan/spokesperson
- Authorize engagement with ransomware negotiators and potential ransom payment.
- Approve for CSIRT to proceed with a full system rebuild and extended recovery timeline

Kind Regards,
Incident Response Manager.

5.REGULATORY NOTIFICATION - NCUA (INITIAL CONTACT)

To: NCUA Regional Examiner (Recovery & Lessons Learned)
Subject: Breach Notification - FinanceFirst Credit Union - December 1, 2025- 11:45am

Incident description:
Pursuant to NCUA's 72-hour cyber incident reporting requirement, FinanceFirst Credit Union detected unusual activity on several critical file servers on December 1, 2025 at 6:45 AM. Preliminary investigation indicates ransomware consistent with REvil operations, potentially affecting member PII (names, SSNs, account numbers, and transaction history).

Impact Summary

- 8 servers encrypted
- 340 GB of data potentially exfiltrated
- Up to 85,000 members may be impacted

Immediate containment measures were taken to contain the threat, including isolating affected servers and verifying backups. External forensic specialists have been engaged to assess the scope of the attack including log analysis, endpoint imaging, and network traffic review and full results will be provided within 24 hours, and the FBI Cyber Division was notified to coordinate on the investigation. Internal teams have also been actively monitoring systems.

Incident Timeline

Action	Responsible	Date(s)	Description
Breach Discovery	IT Security	Dec 1, 2025	Detect unusual encryption activity on critical file servers.
Initial Containment	IT Security / External Forensics	Dec 1-2, 2025	Isolate affected servers, secure backups, and prevent ransomware spread.
Draft Regulatory Notification	Compliance / Legal Team	Dec 1, 2025	Prepare NCUA notification per GLBA, HIPAA, and state breach laws.
Regulatory Notification / Initial Contact	General Counsel / Compliance	Dec 1-2, 2025	Notify NCUA and respond to the inquiry about the incident.
Internal Review / Executive Briefing	CISO / Executive Team	Dec 2, 2025	Validate incident description, timeline,

			and mitigation measures.
Member Notification Preparation	Communications Team	Dec 2–3, 2025	Draft holding letter for affected members.
Member Notification Distribution	Communications Team	Dec 4, 2025	Notify members and guide monitoring accounts.
Documentation & Closeout	Compliance Team	Dec 5, 2025	Archive notifications and review incident response documents.

Breach Details:
Date of Breach Discovery: December 1, 2025
Date Breach Occurred: Approximately November 10 – December 1, 2025
Number of Individuals Affected: Up to 85,000 members.

Type of PHI Involved:

- Names
- Social Security Numbers
- Account numbers and balances
- Contact Information
- Loan application files
- Internal email communications

Description of Breach:
On the morning of December 1, 2025 at 06:45 AM, FinanceFirst Credit Union identified active ransomware encryption affecting multiple internal systems. Early forensic results indicate that attackers maintained network access for approximately three weeks and exfiltrated an estimated 340 GB of member and employee data prior to launching encryption.
We have isolated affected systems and activated our incident response plan.

Breach Notification:

- Individual breach notifications have not yet been issued, pending final forensic validation.
- A sample of member data has since been posted on a leak site, and full member notifications are being prepared.
- Copies of final member notification letters will be provided to NCUA once released.

Mitigation Measures:

- Engaged third-party forensic investigators
- Contained impacted systems and blocked further unauthorized activity
- Reset privileged credentials and implemented additional access controls
- Coordinating with federal law enforcement (FBI Cyber Division) on Revil ransomware
- Preparing member notification and credit-monitoring support services

Estimated Impact and Recovery Timeline:
Impact: Limited disruption to administrative systems; core banking services remain available
Recovery Timeline:

- Containment: Dec 2, 2025
- Forensic analysis/remediation: December 2-6, 2025
- Full system recovery: Expected December 7-8, 2025

Compliance with Notification Requirements

- NCUA Notification: Initial contact made same day as incident discovery (December 1, 2025) - within 72-hour regulatory requirement
- SAR Reporting: Pending; will file with FinCEN if fraud/theft confirmed
- Member Notification: In compliance with GLBA and state laws; holding letters scheduled December 4, 2025

We will provide the next update at 5:00 PM on December 2, 2025, or sooner if the situation changes.

Contact Information: For questions regarding this notification, please contact:
Incident Response Manager
Phone: 080-0000-0000
Email: irm@financefirstcu.com

Sincerely,
FinanceFirst Credit Union

6 MEMBER NOTIFICATION - HOLDING LETTER
Audience: Members (FinanceFirst Credit Union) (Recovery & Remediation)
Time stamp: December 1, 2025 – 10:15 AM
Subject: Important Notice - Service Disruption

We are currently investigating an internal systems issue affecting certain administrative services within FinanceFirst Credit Union. At this time, your core banking services remain fully available and operational.

Our technical teams, along with external experts, are actively reviewing the situation to understand the cause and determine the full extent of the disruption. We are committed to resolving this issue as quickly and safely as possible.

While the investigation continues, we encourage all members to monitor account activity and report anything unusual to our support line at **080-0000-0000.**

We appreciate your patience and will provide additional updates as soon as more information becomes available.

Kind Regards,
FinanceFirst Incident Response Team.

7. PUBLIC STATEMENT
To: Affected Customers (Recovery & Remediation)
Timestamp: December 1, 2025 – 9:00 AM
Subject: Important Security Notice – Service Disruption and Security Event

Dear Valued Customer,
FinanceFirst Credit Union is writing to inform you of a security incident that may have affected your personal information stored in our systems.

What Happened?
On December 1, 2025, we discovered that an unauthorized activity in our network resulted in the encryption of several internal systems by a ransomware group. We immediately launched an investigation and engaged external security experts to determine the scope of the incident.

What Information Was Affected: Our investigation has determined that the following information may have been compromised:

- Full name
- Social Security number
- Account number and account balance
- Contact information
- Loan and banking-related documents

What We Are Doing: We have contained the incident and taken steps to prevent further unauthorized access

- We are conducting a thorough forensic investigation
- We are notifying all affected individuals
- We are working with law enforcement and regulatory authorities
- We are implementing additional security measures to prevent similar incidents in the future

What You Should Do:

1. Monitor your accounts for any unauthorized activity
2. Consider placing a fraud alert or credit freeze with the credit bureaus
3. Review your account statements regularly
4. Follow standard security cybersecurity practices (strong passwords, do not share login credentials)
5. Contact us if you notice any suspicious activity

We will provide the next update at 5:00 PM on December 2, 2025, or sooner if the situation changes.

Additional Resources:

- FAQ Page: https://www.financefirstcu.com/security-faq
- Free Credit Monitoring Enrollment: https://www.financefirstcu.com/protection
- Contact Us:
  Phone number: 070-0000-0000
  Website: support@financefirstcu.com

We sincerely apologize for this incident and any inconvenience it may cause. Your trust is important to us, and we are committed to protecting your information.

Sincerely,
FinanceFirst Credit Union Security Team

8.MEDIA STATEMENT FOR IMMEDIATE RELEASE (Recovery & Remediation)

FinanceFirst Credit Union Responds to Security Incident
December 2, 2025 – 9:00 AM

FinanceFirst has identified a cybersecurity incident affecting certain internal administrative systems. Our core banking services, including online and mobile banking, remain fully operational.

What We Know:
On December 1, 2025, we discovered evidence of unauthorized access to our systems. We immediately launched an investigation with the assistance of external security experts and have notified law enforcement.

Our Response:

- We have contained the incident and taken steps to prevent further unauthorized access.
- We are conducting a thorough investigation to determine the full scope of the incident.
- We are notifying all affected individuals and regulatory authorities as required by law.
- We are implementing additional security measures to strengthen our defenses and prevent similar incidents in the future.

Recovery & Next Updates:
FinanceFirst is restoring affected systems in a controlled, phased manner following forensic validation. Further updates will be provided within the next 48 hours as recovery milestones are achieved.

The security and trust of our members remain our highest priority.

-FinanceFirst Communications

Media Contact:
FinanceFirst Communications Officer
Phone: 080-0881-4470
Email: media@financefirstcu.com

About FinanceFirst Credit Union:
FinanceFirst Credit Union is a regional financial institution serving over 85,000 members across 12 branch locations. We offer a wide range of products, including personal and business

banking, loans, and digital banking services focused on members' trust and long-term stability while protecting the privacy and security of our members' information.

9.EMPLOYEE COMMUNICATION (Recovery & Lessons Learned)

Audience: All Employees
Phase: Containment & Eradication
Timestamp: December 1, 2025 – 12:30 PM
Subject: Internal Notice - IT Incident

Dear Team,
We detected a cybersecurity incident affecting internal administrative systems. Core banking systems remain fully operational.

Incident Details:

- Detected Dec 1, 2025
- Affected: Internal file servers
- Data potentially affected: Internal records, including member account information

Required Employee Actions (Effective Immediately):

- Multi-Factor Authentication (MFA): Ensure MFA is enabled on all corporate accounts. Do not attempt to bypass MFA prompts.
- Password Resets: Reset your network and email passwords when prompted by IT Security. Do not reuse previous passwords.
- Suspicious Activity Reporting: Report any unusual system behavior, suspicious emails, or login alerts to security@financefirstcu.com within 15 minutes of detection.
- System Handling: Do not open, move, or attempt to recover encrypted files.
- Communications Control: Do not discuss this incident externally or on social media. Refer all inquiries to Communications.
- Operational Guidance: Managers will receive additional instructions to support branch and business continuity.

Further updates will follow as systems are validated and restored.

Thank you for your vigilance and support.

Incident Response Manager
FinanceFirst Incident Response Team.

APPENDIX

1.1 CONFIRMATION OF RECEIPT:

CISO

- GRC Manager sends email to CISO at 06:50 AM, Dec 1, 2025.
- CISO acknowledges GRC Manager's email at 06:51 AM, Dec 1, 2025.
- CISO responds to GRC Manager's email at 06:51 AM, Dec 1, 2025.

CEO

- GRC Manager sends email to CEO at 06:53 AM, Dec 1, 2025.
- CEO acknowledges GRC Manager's email at 07:05 AM, Dec 1, 2025.
- CEO responds to GRC Manager's email at 07:05 AM, Dec 1, 2025.

CSIRT

- GRC Manager sends email to CSIRT at 06:55 AM, Dec 1, 2025.
- CSIRT acknowledges the GRC Manager's email immediately at 06:55 AM, Dec 1, 2025.
- Incident briefing with CSIRT at 07:10 AM, Dec 1, 2025.

1.2 EXECUTIVE BRIEFING

- GRC Manager sends email to the **EXECUTIVE** at 07:00 AM, Dec 1, 2025.
- **EXECUTIVE** acknowledges the GRC Manager's email between 07:00 AM and 07: 10 AM, Dec 1, 2025.