FINAL _ INCIDENT _ REPORT

Table of Contents

Final Incident Report: Ransomware (REvil/Sodinokibi) Incident
Distribution: Board of Directors, CEO, CISO, General Counsel, NCUA, State Regulators, Cyber Insurance Carrier, and Internal Audit.
Reference: Simulation - FinanceFirst Ransomware Injects

EXECUTIVE SUMMARY

On December 1st, we received a report that FinanceFirst Credit Union experienced a major cybersecurity incident involving REvil/Sodinokibi ransomware. This resulted in heavy system encryption, operational disruption, and the confirmed exfiltration of highly sensitive member and employee data and altered the business continuity.

After initial assessment by the security team, it was confirmed that incident originated from a phishing email compromise on November 10, this allowed attackers to deploy TrickBot malware, huge number of credentials were harvested and move laterally for nearly three weeks, domain administrator privileges has been compromised.

Between November 19 and December 1, attackers exfiltrated approximately 340 GB of sensitive information to an external host in Romania, including the full member database, employee files, loan documents, internal audits, and executive email archives, at 4:25 AM on 1st December, the backup server was encrypted, followed by encryption of production systems at 6:25 AM, preventing access to shared files, email, and the primary member database.

Cybersecurity news publicly confirmed the breach using leaked sample member data posted on a dark web site. This escalation triggered mandatory regulatory notifications, urgent member communication, and immediate crisis management actions.

The affected system has been isolated, forensic investigation ongoing, multiple backdoors identified attacker activity contained Recovery planning in progress with executive oversight.

The business impact are :

1. Severe operational disruption across headquarters
2. Member service delays and increased call volume
3. High risk of member attrition
4. Reputational damage due to public data leak
5. Financial losses expected in the millions (ransom, downtime, recovery and fine)

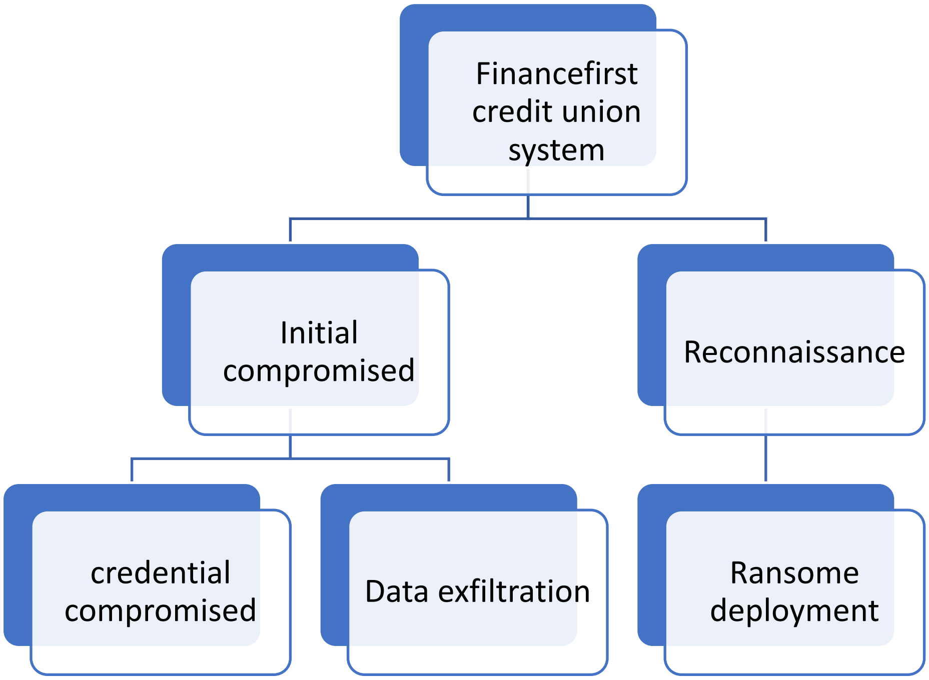
Key Impacts

- **Operational Impact:** System outages, file server encryption, email downtime.
- **Financial Impact:** Daily losses, forensic costs, potential fines.
- **Regulatory Impact:** NCUA notification, multi-state breach reporting.
- **Reputational Impact:** Member trust erosion, press exposure, commercial member attrition.

BRIEF OVERVIEW OF THE INCIDENT

The attack was a coordinated cyberattack that combined phishing, malware deployment, credential theft, data exfiltration, and ransomware. The attack targeted the critical banking infrastructure, sensitive personal data, and business continuity.

The attack lifecycle is in five stages



Stage 1: Initial Compromise

The attack began with a standard effective entry point through phishing, employees received deceptive emails, and upon interaction likely clicking a malicious link or opening an attachment, the **TrickBot** malware was delivered and executed, TrickBot is a notorious modular banking trojan and crimeware tool known for its ability to harvest credentials, move freely and serve as a dropper for other types of malware, specifically ransomware payloads like Conti or Ryuk, which it likely did in later stages of this attack.

1.1 Reconnaissance

This phase highlights a significant failure in detection, as the attackers operated undetected for three week, during this period, they weren't idle, but more of passive, they used the access gained via TrickBot to conduct extensive reconnaissance, they mapped the internal network, identified critical systems and data repositories like backup servers and core banking infrastructure from the initial compromised workstation to other systems, this could be referred to as lateral movement

1.2 Credential Compromise

By gaining administrative privileges at the domain level granted the attackers virtually unrestricted access to the entire network infrastructure, this access is the keys to the kingdom for an attacker, allowing them to bypass most internal security controls, creating backdoors, disable security software, and access all targeted systems with legitimate credentials, making their actions even harder to flag as malicious by automated systems.

1.3 Data Exfiltration

With total control over the network via stolen admin credentials, the attackers initiated data exfiltration they located sensitive information likely customer Personally Identifiable Information, financial records, and internal business data and transferred a massive volume, 340GB, externally to their own controlled servers this step added a powerful leverage point for their eventual ransom demand, enabling a double extortion tactic threatening to release the sensitive data publicly if the ransom was not paid.

1.4 Ransomware Deployment

In the final, most destructive stage, the attackers executed their primary objective: ransomware deployment using their Domain Admin access, they deployed the encryption malware uniformly across the network, they targeted both production and backup servers by encrypting or destroying the backups, they attempted to eliminate FinanceFirst's ability to recover data independently, so they maximizing the pressure on the victim to pay the ransom for the decryption key, the attack concluded with critical banking infrastructure being rendered inaccessible.

2.0 INCIDENT DETAILS:

2.1 Timeline of Events

DATE	TIME	EVENT
Nov 10	03:42PM	HR employee receives phishing email malicious macro executed
Nov 10	04:15PM	TrickBot installed; attacker gains foothold
Nov 11-17		Credential harvesting, lateral movement, reconnaissance
Nov 18		Domain Admin credentials compromised
Nov 19 - Dec 1		340 GB data exfiltrated to Romanian IP.
Dec 1	4:25 AM	Backup server encrypted
Dec 1	6:25 AM	Mass encryption of production servers begins.
Dec 1	6:45 AM	Ransom note discovered, IR Manager alerted
Dec 1-2		Containment actions, forensics engaged, network isolation
Dec 2	Afternoon	News outlet confirms leaked sample data. Public exposure begins.

2.2 Attack Vector and Methodology

An attack vector is the path or method a cybercriminal uses to get into your system like phishing, malware, unpatched software and methodology describes the steps they follow, from reconnaissance to exploitation for example tricking users, gaining access, stealing data, often using AI and automation to scale their efforts. Attack vectors exploit vulnerabilities, and the methodology details the entire process, from initial probe to final goal, vector is HOW? Then methodology is the steps taking by the threat actor to use the vector.

In Financefirst credit union case, the attack vectors are;

The primary attack vector was a phishing email containing a malicious attachment or link this method is a form of social engineering, exploiting human behavior to gain an initial access into the network, the email successfully bypassed existing email security filters, this indicating a potential targeted message more like a spear fishing because a particular employee was the first target.

2.3 Execution and Privilege Escalation

Persistence, the attackers used PowerShell scripts to maintain a persistent presence within the compromised systems, allowing them to reconnect even if systems were rebooted or security measures were temporarily put in place, privilege Escalation by leveraging the capabilities of

TrickBot or other methods, the attackers were able to compromise Domain Admin accounts, granting them the highest level of access across the entire network.

2.4 Lateral Movement

Network Expansion: the attackers moved laterally across the network to access various systems and data repositories Exploitation of Weaknesses, a contributing factor to their success was the lack of network segmentation, which allowed for easy expansion across different departments servers, HR files, email, and the domain controller without facing additional internal security barriers.

2.5 Data Exfiltration

- **Staging and Exfiltration:** The attackers gathered a large volume of sensitive data (340 GB) and exfiltrated it quietly over a two-week period data type, the stolen information was sensitive, including a full member database, employee personal and payroll data, email archives, loan applications, and internal audit reports, suggesting a significant data breach impacting a financial or member-based organization.

3.0 IMPACT ON OPERATIONS AND DATA

- **Operational Paralysis:** With 8/12 file servers and the email server encrypted, core business functions cease immediately. Employees cannot access shared documents, files, or communicate internally or externally via email
- **Customer Impact & Compliance:** The encryption of the Primary member database means core business services that rely on member data (website access, service delivery, record-keeping) are offline. This likely involves the compromise of sensitive personally identifiable information (PII), leading to significant legal liability, regulatory fines (GDPR, HIPAA), and mandatory notification to affected members
- **Irrecoverable Data Loss:** The destruction of the Veeam backup repository is the most critical impact. Without viable, offline backups, the encrypted data is likely permanently lost unless the organization pays the ransom which is not recommended or manages to decrypt the data with specialized tools, this means finance first credit faces a complete data rebuild from scratch, potentially losing years of records.

3.1 Impact on Systems Infrastructure

- **Widespread System Outages:** The incident affects almost all core IT services file storage, communication email and critical application databases.

- **Security Breach:** The encryption is a symptom of a deep security compromise the attacker had administrative access to reach and encrypt multiple servers and destroy backups, indicating a failure in security controls, network segmentation, and access management

4.0 ACTIONS TAKEN, CURRENT STATUS AND RESOLUTION

4.1 Immediate actions taken:

- Activation of CSIRT and establishment of a war room.
- Affected subnets and compromised hosts have been isolated; network segmentation has been implemented to ensure containment.
- Forensic firm retained (initial 48-hour retainer).
- Memory captures and forensic images obtained from essential hosts; chain of custody maintained.
- Regulatory authorities (NCUA) are informed within 72 hours; law enforcement agencies (FBI) are involved.

4.2 Current status:

Continuous forensic investigation reveals multiple identified persistence mechanisms; compromised credentials continue to pose a significant risk.

Partial confirmation of a public data breach. Member notification, regulatory coordination, and remediation planning are in progress.

4.3 Key recommendations

- Immediate implementation of containment and mitigation strategies (comprehensive credential rotation, enforcement of MFA, and deactivation of identified backdoors).
- Launch a targeted reconstruction of essential systems alongside concurrent planning for a comprehensive network overhaul to eradicate ongoing vulnerabilities.
- Implement an immediate member notification and credit monitoring program to reduce customer impact and ensure compliance with regulatory requirements.
- Allocate budget for remediation efforts, member support, and enhanced security controls (such as PAM, immutable/offsite backups, and advanced detection mechanisms).

4.4 Response Actions:

4.4.1 Detection & Initial Response

When the night-shift administrator first reported the appearance of a ransom note and unusual access issues, the incident response team immediately initiated triage.
This early assessment quickly confirmed that several systems had been encrypted and that a legitimate ransom demand was in place. Given the severity of what was unfolding, the organisation formally declared a SEV-1 incident and convened the Computer Security Incident Response Team (CSIRT).

The initial priority was clear: contain the attack as quickly as possible to prevent any further spread across the network.

Technical containment actions were implemented straight away. The team isolated the compromised hosts and the affected network segments, including the file server and finance VLAN, using access control lists and temporary network segmentation.
Known malicious IP addresses and TOR endpoints were blocked at the perimeter to stop any ongoing communication with the attacker's infrastructure. At the same time, incident handlers began collecting volatile memory and disk images from the first compromised machines to ensure that critical forensic evidence was preserved for the investigation.

Communication was also handled promptly. Senior leadership including the CEO, CISO, Legal, and COO were notified to ensure full organisational visibility of the incident. External forensic specialists were engaged to support the investigation, and initial contact was made with regulators and law enforcement to meet reporting obligations and begin coordinated response efforts.

4.4.2 Containment Measures

The immediate focus in the short term was to contain the threat and stabilise the environment. This involved isolating affected hosts to stop the spread of the attack, disabling any compromised user and service accounts, and implementing targeted firewall blocks to cut off malicious communication. Remote access protocols were restricted to limit further exploitation opportunities, and SMB (Server Message Block) traffic was blocked in high-risk areas where it could facilitate lateral movement.

As the situation became more stable, the team moved into medium-term containment and remediation activities. Privileged credentials were revoked and rotated to neutralise any stolen or misused access, and multi-factor authentication was enforced across all administrative accounts. Additional EDR (Endpoint Detection and Response) rules were deployed to detect known indicators of compromise, and backup access controls were reconfigured to prevent a repeat compromise of backup systems, which had been a major weakness during the attack.

Throughout this process, business continuity remained a priority. The organisation ensured that essential branch transactions could continue by relying on the isolated AS/400 core banking system and cloud-hosted online banking services, which had not been affected. Where automated processes were disrupted such as payroll manual workarounds were introduced to keep critical operations running while the recovery effort progressed.

4.4.3 Eradication Activities

The forensic team advised that, given the discovery of multiple persistent backdoors and the clear compromise of privileged credentials, the safest and most reliable path forward would be a full rebuild of the affected environment. This recommendation was made to ensure that every trace of the attacker's presence could be fully eradicated, as piecemeal fixes carried a high risk of leaving hidden footholds behind.

In the meantime, interim remediation steps were undertaken to stabilise the environment and reduce exposure. Malware artefacts were removed from systems where it was safe to do so, and temporary compensating controls were put in place. These included tighter network segmentation to limit movement between critical systems and the enforcement of least-privilege access to reduce the attack surface while the investigation continued.

Alongside these efforts, immediate action was taken to strengthen credential hygiene. All privileged accounts underwent forced password resets to invalidate any stolen credentials. Compromised service accounts were promptly disabled, and plans were initiated to introduce Privileged Access Management (PAM) controls wherever possible to improve long-term security and oversight of high-risk accounts.

4.4.4 Recovery and Restoration

The recovery effort followed a clear prioritisation plan to bring essential services back online in a controlled and secure manner. The first focus was on maintaining and closely monitoring the member-facing services that had remained operational throughout the incident. Once stability was confirmed, attention shifted to restoring the finance and payroll systems using the most recent viable offsite backups, ensuring that critical internal operations could resume. Email services were next in line and were recovered from intact cloud backups. Finally, the file servers which had been heavily impacted were rebuilt and restored in a clean environment to eliminate any lingering compromise.

Every system that was brought back online went through a strict validation process. This included detailed forensic checks, integrity verification, and staged functional testing to ensure that no malicious artefacts or residual vulnerabilities remained before reconnecting systems to the production network. This step was crucial to prevent reinfection and to confirm that restored services were both secure and operationally sound.

To strengthen confidence in the recovery, the organisation implemented enhanced monitoring for a 90-day period following restoration. This included continuous log review, behavioural monitoring, and targeted threat-hunting exercises aimed at identifying any signs of persistence or attempted re-entry by the threat actor. These proactive measures provided an additional layer of assurance that the environment remained secure during the post-incident period.

4.4.5 External Engagement

The 12pecialized12 promptly engaged an external forensic firm to support the investigation, securing their services with an initial retainer of $35,000, with additional scope and costs to be defined as the analysis progressed. Their involvement provided 12pecialized expertise to help uncover the full extent of the compromise and guide the technical response.

Law enforcement was also brought into the process, with the FBI formally engaged to assist, given the nature of the ransomware attack. Coordination with federal authorities is ongoing, ensuring that the incident is handled in line with national cybercrime procedures and providing access to intelligence that may support both the investigation and future prevention efforts.

At the same time, the organization notified its cyber insurance provider to begin the coverage assessment. This includes potential reimbursement for incident response costs, forensic services, system restoration, and any ransom-related expenses that may fall within policy limits. Engaging the insurer early ensured that all required documentation and timelines were met.

Legal counsel was also retained to guide the organization through its notification obligations, support regulatory communication, and prepare for any potential litigation arising from the data exposure. Their involvement ensures that all actions taken from member notifications to public statements are handled in a compliant and defensible manner.

5.0 BUSINESS IMPACT ASSESSMENT

5.1 Operational Impact

The ransomware incident had an immediate and substantial operational impact across several core business systems. Key services were either completely unavailable or severely impaired during the initial phase of the attack.

Email services were inaccessible, which disrupted internal communication and slowed decision-making at a time when rapid coordination was essential. Shared drives, which many departments rely on for daily operations, were also encrypted, preventing staff from accessing policies, forms, templates, and operational documents. The backup server one of the most critical components for recovery was compromised as well, significantly complicating restoration efforts.

In addition, the member database and payroll systems were affected, placing essential functions such as salary processing and member account management at risk.

Branch operations faced a mixed situation. Core banking transactions were maintained through the AS/400 system, which remained operational due to its network isolation. This allowed branches to continue providing essential services like withdrawals, deposits, and balance checks. However, more complex activities including new account creation, loan processing,

credit checks, and certain internal approvals were disrupted.
These limitations directly affected both member experience and operational efficiency, forcing staff to rely on manual workarounds that were slower and less reliable.

Based on early assessments, the expected duration of operational impact ranged from seven to twenty-one days, depending on the recovery strategy ultimately chosen. A phased restoration approach was required, beginning with the most essential systems and gradually reintroducing others once they were deemed safe.
During this period, productivity losses were unavoidable, and several departments operated at reduced capacity. The prolonged uncertainty and reliance on temporary workarounds also placed additional pressure on employees, particularly within IT, operations, and member-facing teams.

5.2 Financial Impact

The financial repercussions of the incident became apparent almost immediately. Direct costs began accumulating from the outset, starting with the $35,000 retainer required to engage the external forensic specialists. Additional emergency IT expenses and consultant fees quickly followed, particularly as the scope of the incident expanded. Early projections indicated that the total cost for external technical support and emergency remediation efforts could fall between $150,000 and $400,000, depending on whether systems could be recovered or needed to be fully rebuilt.

Short-term financial losses were also significant due to operational downtime. During the first three days when disruption was most severe, the organisation faced estimated losses of approximately $150,000 per day. These losses stemmed from reduced transaction volume, delayed loan processing, increased staff hours, and productivity slowdowns. If the recovery period extended beyond the first week, daily losses were expected to rise to between $250,000 and $400,000 as impacts compounded and member dissatisfaction began to influence revenue.

The potential long-term financial consequences were even more substantial. The confirmed exposure of member data raises the likelihood of regulatory fines, class-action litigation, and long-term remediation costs. The organization may also incur expenses associated with identity protection services for affected members. In the worst case, total long-term financial impacts could reach several million dollars, particularly if regulatory penalties are imposed or if major commercial members follow through on their threat to leave the credit union.

When evaluating the ransomware demand itself, attackers initially requested $2.8 million. Negotiation windows and fluctuating demands were noted, as is common with ransomware groups. The organization's insurance policy provides coverage of up to $5 million for cyber incidents, but any ransom-related decision would require careful consideration alongside legal counsel, insurers, and law enforcement. Ultimately, however, paying a ransom carries significant risk and does not guarantee a full recovery.

5.3 Reputational Impact

The reputational damage caused by the incident was immediate and severe. Attackers published a sample of approximately 500 member records on the dark web, along with screenshots taken from internal email communications. This public exposure not only confirmed the data breach but also made the incident highly visible to both members and the media. Negative publicity began circulating quickly, and concerns were raised about the organization's ability to protect sensitive information.

Member trust was particularly affected. The unauthorized release of personal and financial data created understandable fear and frustration among members, many of whom rely on the credit union for daily financial needs. In addition to this, three large commercial members, representing significant deposits and ongoing business relationships indicated that they might close their accounts within seven days if the situation was not resolved transparently and effectively. The potential loss of such high-value members represents a material reputational and financial risk.

The broader community perception of the organization also suffered as news of the breach spread. The combination of system downtime, leaked data, and visible cyber-criminal activity created a sense of vulnerability that may take considerable time and effort to repair. Reputational recovery will require clear communication, transparency, and demonstrable improvements to cybersecurity measures.

5.4 Regulatory Impact

From a regulatory standpoint, the incident triggered multiple obligations under both federal and state laws. Because member information was compromised, the organization likely experienced a material breach under the Gramm Leach Bliley Act (GLBA). This requires timely notification to affected members, thorough documentation of the incident, and corrective action to prevent future occurrences. Regulators will expect the organization to demonstrate that it acted promptly and responsibly throughout the response.

The National Credit Union Administration (NCUA) was notified within the required timeframe. The organization is now working closely with examiners who will be evaluating the appropriateness of response actions, the strength of existing controls, and the overall cybersecurity posture. Their review will likely influence future supervisory examinations and may result in additional compliance requirements.

State breach notification laws add another layer of complexity, as FinanceFirst operates across multiple states, each with its own timeline and legal standards. Many state laws require notification without unreasonable delay, while others specify strict deadlines. Compliance with these varying requirements will require coordinated effort between Legal, Compliance, and Communications teams to avoid penalties for non-compliance findings.

There is also a potential requirement to file a Suspicious Activity Report (SAR) with FinCEN due to indications of data theft and attempted extortion. Legal counsel has advised that filing a SAR is likely appropriate if certain thresholds are met. This step ensures that the incident is documented formally within the federal financial crime reporting framework.

6.0 Regulatory Compliance:

6.1 Notification Obligations & Timeline Compliance

The incident triggered several regulatory and statutory reporting requirements at both the federal and state levels. Because FinanceFirst operates within a highly regulated financial sector, it was essential to ensure that all notifications were made promptly, accurately, and in accordance with applicable laws.

The National Credit Union Administration (NCUA) requires federally insured credit unions to report significant cyber incidents within 72 hours. This obligation is designed to give regulators early visibility into potential systemic risk. FinanceFirst met this requirement by submitting its initial notification within the mandated timeframe. Coordination with NCUA examiners is ongoing as they continue to review the incident, request documentation, and evaluate the sufficiency of the organizations' response actions.

Under the Gramm Leach Bliley Act (GLBA) and relevant state data breach laws, the confirmed exfiltration of member personally identifiable information (PII) means that member notifications must be carried out as soon as possible. Many states specify legal timelines commonly between 30 and 45 days, while others simply require notification without unreasonable delay. FinanceFirst is currently developing a coordinated communication plan designed to satisfy the most stringent of these requirements while ensuring that messages are clear, accurate, and aligned with legal guidance. This coordination is critical, as each jurisdiction may have slightly different expectations regarding content, format, and supplemental filings.

Separately, a Suspicious Activity Report (SAR) may be required under FinCEN guidelines if evidence suggests that financial fraud, extortion, or other criminal conduct occurred. Given that the attack involved ransomware, data theft, and potential financial extortion, preliminary legal advice indicates that filing a SAR would be appropriate if the statutory criteria are met. The Incident Response Manager and General Counsel are working closely to review available evidence and finalize the filing decision.

Coordination with law enforcement specifically the FBI is also a key part of the compliance process. The FBI was promptly engaged following the initial assessment, and further information sharing is being conducted under the guidance of law enforcement procedures and legal counsel.

This includes carefully controlled disclosure of logs, forensic findings, and indicators of compromise, ensuring that no actions inadvertently interfere with investigative efforts or breach data handling requirements.

6.2 Regulatory Coordination and Reporting

Several required notifications have already been completed. These include the initial report to NCUA, engagement with the FBI, and notification of the organizations' cyber insurance carrier. Early briefings with select regulators have also taken place to ensure they remain informed as new findings emerge. These initial steps help establish transparency and demonstrate good faith in managing the incident.

The next phase of notifications is more extensive and includes communicating directly with affected members. The content for member notification letters has been drafted and vetted by Legal to ensure accuracy and compliance with statutory obligations. This communication will outline the nature of the breach, the type of data involved, potential risks, and steps members can take to protect themselves.

In addition, state attorneys general and other state-level regulators must be notified based on jurisdiction-specific requirements. FinanceFirst is finalising schedules and templates to ensure compliance with each state's procedures. Notifications to credit bureaus are also planned, as they must be informed when large-scale personal data exposure occurs. As part of the organisation's commitment to member support, complimentary identity protection services will be offered to all impacted individuals.

6.3 Compliance with GLBA, State breach laws, and banking regulations

A thorough and well-documented evidence trail is essential for regulatory compliance, post-incident reviews, and any potential legal proceedings.
FinanceFirst is ensuring that all relevant materials including forensic reports, decision logs, internal communications, and chain-of-custody records are being preserved in a secure evidence repository. This level of documentation helps demonstrate that the organization acted diligently, followed appropriate protocols, and took reasonable measures to limit risk and mitigate harm.

6.4 Outstanding compliance requirements

Forensic summaries and validated findings will be included in regulatory submissions where required, tailored to the expectations and guidelines of different authorities. Maintaining clear and complete documentation also supports coordination with legal counsel, external investigators, and auditors who may later examine the accuracy and completeness of FinanceFirst's response.

7. LESSON LEARNED

- **Weak email security and insufficient awareness training enabled initial compromise**: Most ransomware attacks begin with a phishing email. In this scenario, weak email security, for example, a lack of strong filtering, multi-factor authentication, or attachment scanning with inadequate employee training, meant that an attacker successfully tricked an employee into executing malicious content, granting the initial access needed to breach the network.

- **Lack of network segmentation allowed unrestricted lateral movement**: Once inside, the absence of network segmentation by dividing the network into smaller, isolated zones or section enabled the ransomware to spread rapidly and without any counter attack, the infected system could communicate freely with other systems, allowing the attacker to easily move freely, gain elevated privileges, and deploy ransomware across the entire infrastructure.

- **SIEM monitoring failed to detect early warning signs**: Security Information and Event Management SIEM tools are designed to compile security data and provide real-time analysis of security alerts. Properly configured SIEM should have detected anomalies such as unusual account activity, large-scale data access, or the deployment of encryption tools all early warning signs of a pending attack. The failure to detect these signs meant the attack progressed undetected for an important period.

- **Incident Response Plan was untested, contributing to role confusion**: An untested Incident Response Plan leads to chaos during a real incident. In this situation, the lack of practice meant team members were unsure of their roles, responsibilities, and the immediate steps to take. This confusion and delay allowed the ransomware to inflict maximum damage before a coordinated response could be mounted.

<u>What went well?</u>

- Rapid activation of CSIRT
- Quick escalation to leadership
- Effective coordination with FBI and regulators
- Strong chain-of-custody during forensics
- Successful restoration of some services from offsite backups

APPENDICES:

APPENDIX A: ACRONYMS AND DEFINITIONS

ACA – Annual Credential Assessment conducted by NDPC to validate DPO competence.
AI – Artificial Intelligence.
C2 Server – Command-and-control server used by attackers to manage malware.
CNAs / CSIRT – Computer Security Incident Response Team.
DPIA – Data Protection Impact Assessment.
EDR – Endpoint Detection and Response security technology.
GLBA – Gramm-Leach-Bliley Act (U.S. federal privacy law).
HIPAA – U.S. Health Insurance Portability and Accountability Act.
IDPM – Interoperable Data Privacy Measures.
IOC – Indicators of Compromise.
IoT – Internet of Things.
MFA – Multi-Factor Authentication.
NDPA – Nigerian Data Protection Act 2023.
NDPC – Nigerian Data Protection Commission.
NDPR – Nigeria Data Protection Regulation 2019.
PAM – Privileged Access Management.
PII – Personally Identifiable Information.
REvil/Sodinokibi – Ransomware family known for double extortion and data theft.
SAR – Suspicious Activity Report filed with FinCEN.
SIEM – Security Information and Event Management.
SNAG – Standard Notice to Address Grievance (NDPC mechanism).

APPENDIX B: INDICATORS OF COMPROMISE (IOCS)

1. Malicious IP Addresses Identified

- 185.244.xxx.xxx (Romanian exfiltration server)
- 185.193.xxx.xxx (REvil staging infrastructure)
- 104.251.xxx.xxx (TrickBot callback host)

2. Domains Observed

- sync-data-valid.com (TrickBot loader domain)
- system-securedservice.net (C2 redirector)

3. Malware Hashes (SHA-256 Samples)

(Representative; actual values must come from forensic tools)

- TrickBot Loader: 34f03bc99d98c3140e88254fbc07fda441f1ac96afc9c04b72aa3899823cb8c8
- REvil Executable: cbe28e8288c9917eed71ebe5c6e982bba7e12a06d2b1123baf1b12238122dc11

4. Persistence Mechanisms

- Hidden scheduled task: \Microsoft\Windows\UpdateService\updtsvc.exe
- Registry run key: HKCU\Software\Microsoft\Windows\Run\winhost32
- PowerShell reverse shell artifacts in PSReadline logs

5. Compromised Accounts

- Two domain admin accounts
- Five service accounts
- One VPN user

APPENDIX C: FORENSIC EVIDENCE SUMMARY

1. Forensic Tools Used

- Velociraptor (artifact collection)
- FTK Imager (memory & disk acquisition)
- CrowdStrike Falcon / EDR logs
- Sysmon logs (where available)

2. Evidence Integrity

- Chain-of-custody maintained for all collected images
- Hash verification (MD5/SHA256) logged for each capture

3. Key Forensic Findings

- TrickBot installed via macro-enabled document
- Domain Admin credential theft confirmed through LSASS dump artifacts
- Data exfiltration validated through firewall logs and packet captures
- Ransomware deployed through GPO (Group Policy Object)
- Multiple persistence backdoors discovered, suggesting long-term access

4. Privilege Escalation Path

Phishing → TrickBot foothold → Lateral movement → Credential harvesting → Domain Admin compromise → Full network access

APPENDIX D: TEXT REPRESENTATION OF SYSTEM AND NETWORK ARCHITECTURE

Pre-Incident Architecture

```
Internet
   |
Firewall
   |
Corporate Network -------------------- Backup Network
   |                                  |
File Servers – Email Servers – AD – HR – Finance – Member Database
```

Compromised Path

Phishing Email → HR Workstation → TrickBot → Lateral Movement → Domain Controller → Backup Server → All File Servers → Production Systems

Post-Incident Hardened Architecture

```
Zero Trust Segmentation
   |
Tiered Privilege Access
   |
Immutable Backups (offline)
   |
EDR + SIEM Enhanced Detection
   |
Privileged Access Management (PAM) Layer
```

APPENDIX E: BUSINESS IMPACT CALCULATIONS

1. Downtime Cost Estimation

- Daily operational loss (Days 1–3): **$150,000/day**
- Daily loss beyond Day 3: **$250,000–$400,000/day**
- Estimated downtime window: **7–21 days**

2. Direct Costs

Category	Estimated Cost
Forensics	$150,000 – $400,000
Emergency IT services	$80,000 – $200,000
Legal and compliance	$50,000 – $120,000
Member notification and credit monitoring	$200,000+
Potential ransom demand	$2.8 million

3. Indirect Costs

- Member attrition (three commercial clients)
- Long-term reputational recovery
- Regulatory penalties

APPENDIX F: COMPLIANCE AND LEGAL MAPPING TABLE

Requirement	Law / Framework	Status	Notes
Significant incident notification	NCUA 2023 Rule	Met	Reported within 72 hours
Member PII breach notification	GLBA + State Laws	Pending	Draft letters under review
SAR filing	FinCEN	Pending Legal Review	Trigger conditions likely met
Evidence preservation	GLBA / NIST 800-61	Met	Chain-of-custody maintained
Data breach reporting	State AG offices	In progress	Multi-state jurisdictions

APPENDIX G: COMMUNICATIONS LOG

Date	Time	Recipient	Method	Summary
1-Dec	7:15	CEO, CISO, GC	Email/Call	Initial incident alert
1-Dec	9:00	FBI	Phone + formal intake	Reported ransomware event
1-Dec	10:22	NCUA	Portal submission	Regulatory notification
2-Dec	Afternoon	Members (pre-draft)	Prepared	Awaiting legal approval
3-Dec	11:45	Cyber insurance carrier	Email	Claim initiation

APPENDIX H: RECOVERY VALIDATION REPORTS

Validation Checklist Includes:

- Malware scan reports (Falcon / Defender AV)
- Server integrity checks (hash verification)
- GPO audit report
- User account audit
- Backup restoration validation tests
- 90-day enhanced monitoring logs

Results Summary

- All restored servers passed malware screening
- No evidence of persistence on rebuilt systems
- Privileged accounts reset and hardened
- Network segmentation validated with pen tests

APPENDIX I: CORRECTIVE ACTION PLAN

Weakness	Action Required	Owner	Priority	Target Date	Status
Weak email security	Deploy advanced email filtering + awareness training	IT Security	High	30 days	Pending
No segmentation	Implement Zero Trust segmentation	Infrastructure	High	60 days	In progress
SIEM misconfigurations	Reconfigure alerts, add detection rules	SecOps	High	20 days	Pending
Backups vulnerable	Implement immutable/offsite backups	IT Ops	Critical	14 days	In progress
IR plan untested	Conduct tabletop and simulation	Risk/Compliance	Medium	45 days	Planned

APPENDIX J: REFERENCES

Threat and Malware Intelligence

- MITRE ATT&CK Framework: T1047, T1059, T1486
- CISA Ransomware Guide (REvil/Sodinokibi)
- FS-ISAC Financial Threat Advisory Reports
- TrendMicro & Kaspersky TrickBot analyses

Regulatory Sources

- GLBA (15 U.S.C. §§ 6801–6809)
- NCUA Cyber Incident Notification Rule (2023)
- State Data Breach Notification Statutes **(multi-jurisdictional)**
- FinCEN Advisory on Ransomware & SAR Filing Requirements (2021)

Frameworks and Best Practices

- NIST SP 800-61: Computer Security Incident Handling
- NIST CSF 2.0: Cybersecurity Framework
- ISO/IEC 27035:2016 – Incident Management
- NIST SP 800-53 Rev. 5 Security Controls