INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-26 13:30 UTC

Ransomware Attack on JRK Property Holdings Triggers Class-Action Lawsuit Over PII Exposure

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0103
Type	Data Breach
Severity	HIGH
Affected Products	JRK Property Holdings Inc., tenant and customer PII data (estimated 111,000 individuals)
Published	2026-04-25
Discovery Source	Gemini

Executive Summary

In April 2025, ransomware group 'The Gentlemen' breached JRK Property Holdings Inc., exposing names and Social Security numbers for approximately 111,000 tenants and customers. A proposed federal class-action lawsuit (Fongaro et al. v. JRK Property Holdings Inc.) alleges inadequate security controls, the Connecticut Attorney General has engaged directly with the company, and congressional calls for federal investigation are active. Organizations in the real estate and property management sector face heightened scrutiny; this incident signals that residential landlords holding sensitive PII are now primary ransomware targets with significant legal downstream consequences.

Technical Analysis

JRK Property Holdings suffered a ransomware intrusion attributed to 'The Gentlemen' in April 2025. No CVE has been publicly assigned; the initial access vector and specific vulnerability exploited have not been confirmed in open sources as of this analysis. Mapped CWEs indicate likely weaknesses in PII exposure controls (CWE-359), inadequate security architecture (CWE-1008), and failure of protection mechanisms (CWE-693). MITRE ATT&CK techniques associated with this incident include phishing for initial access (T1566), valid account abuse (T1078), data exfiltration over C2 channel (T1041), and data encrypted for impact (T1486). Approximately 111,000 records including Social Security numbers were exfiltrated and/or encrypted. No patch, CVE identifier, or vendor advisory is available; remediation guidance is based on MITRE technique mapping and observed threat actor TTPs. CVSS and EPSS scores are not applicable given the absence of a disclosed vulnerability.

Action Checklist

1. Containment: Identify all systems storing tenant or customer PII, particularly names and Social Security numbers; isolate any systems showing indicators of lateral movement or unauthorized encryption activity. Prioritize property management platforms, CRM systems, and file servers accessible by remote or contractor accounts.

2. Detection: Review authentication logs for anomalous use of valid accounts (T1078): look for off-hours logins, impossible travel, or accounts accessing bulk PII stores. Audit email gateway logs for phishing delivery (T1566). Monitor endpoint and network logs for large outbound data transfers to unknown external IPs (T1041). Check for file rename events consistent with ransomware staging (T1486).

3. Eradication: No vendor patch is available for this incident. Harden access controls on systems holding SSN data: enforce MFA on all remote access paths, rotate credentials for any accounts with access to PII repositories, and disable unused service accounts. Review email filtering rules and tighten attachment/link policies to reduce phishing exposure.

4. Recovery: Validate integrity of PII datastores against known-clean backups. Confirm backup systems were not encrypted or exfiltrated. Restore from clean backup only after confirming threat actor persistence has been removed. Engage forensic support to verify no backdoors or scheduled tasks remain. Monitor restored systems for re-encryption or beaconing activity for a minimum of 30 days.

5. Post-Incident: Conduct a gap assessment against NIST SP 800-53 controls AC-2 (Account Management), MP-6 (Media Sanitization), and SI-3 (Malware Protection). Review data minimization practices: retain SSNs only where legally required and reduce retention periods. Develop or update an incident response playbook specific to ransomware targeting PII-heavy property management environments. Evaluate cyber liability insurance coverage adequacy given active litigation.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal counsel, the Connecticut Attorney General liaison, and the organization's cyber liability insurer if forensic analysis confirms SSN exfiltration for any portion of the estimated 111,000 affected individuals, if 'The Gentlemen' publishes data on their leak site, if restored systems show re-encryption or active beaconing within the 30-day monitoring window, or if the incident response team lacks the forensic capability to conclusively rule out backup compromise — all four conditions carry direct regulatory notification obligations and active litigation exposure.
Recovery Notes	Restore PII datastores only after independent forensic verification confirms no persistence mechanisms (scheduled tasks, WMI subscriptions, implanted service accounts) remain on the hosting systems and network segments. Given the active class-action lawsuit and Connecticut AG engagement, all restored systems must maintain enhanced audit logging (NIST AU-2, AU-12) at maximum verbosity for a minimum of 90 days — not the standard 30 — to support legal discovery and demonstrate due diligence to regulators. Continuously monitor restored property management platforms and CRM systems for anomalous bulk-read activity against SSN fields for at least 30 days post-restoration, using file system auditing or database query logging as a compensating control if EDR is unavailable.

Forensic Artifacts	VSS shadow copy deletion records — query Windows Application Event Log for Event ID 8193 (VSS error) and System Event Log for vssvc.exe termination events in the hours preceding confirmed encryption; absence of shadows on PII-hosting servers is a primary indicator of 'The Gentlemen' pre-encryption preparation and establishes the timeline anchor for the breach. | Ransom note files dropped in encrypted directories across property management file shares — these are threat-actor-specific artifacts containing victim ID strings, C2 contact addresses, and 'The Gentlemen' branding that support law enforcement attribution, FBI IC3 reporting, and OFAC sanctions screening before any ransom payment consideration. | Windows Security Event Log Event ID 4663 (Object Access — File Read) on file servers hosting tenant SSN data — a burst of 4663 events from a single account or process within a compressed timeframe (thousands of reads in minutes) represents the exfiltration staging event and is the primary evidence for quantifying the 111,000-individual exposure scope in regulatory notifications. | Network flow data (NetFlow, IPFIX, or pcap) from the egress router or firewall covering the 72-hour window before the ransomware detonation — large sustained TCP sessions to non-corporate external IPs, particularly over ports 443, 80, or 22 from internal PII-hosting servers, document the T1041 exfiltration channel and destination infrastructure used by 'The Gentlemen' for double-extortion leverage. | Active Directory replication metadata ('repadmin /showchanges' or DCSync detection via Event ID 4662 with GUID 1131f6aa-9c07-11d1-f79f-00c04fc2dcd2) — ransomware operators targeting PII repositories commonly perform credential harvesting via DCSync or LSASS dump (T1003) prior to lateral movement; this artifact establishes whether domain admin credentials were compromised, which directly affects the scope of mandatory credential rotation and the litigation narrative around access control adequacy.

Per-Action IR Details

Containment — Identify all systems storing tenant or customer PII, particularly names and Social Security numbers; isolate any systems showing indicators of lateral movement or unauthorized encryption activity. Prioritize property management platforms, CRM systems, and file servers accessible by remote or contractor accounts.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST SI-4 (System Monitoring), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run 'net share' and 'Get-SmbShare' on Windows file servers to enumerate all shares accessible by contractor or remote accounts. Use osquery ('SELECT * FROM shared_resources;') to enumerate shares across Linux/Windows endpoints without an EDR agent. Block outbound SMB (445/TCP) and RDP (3389/TCP) at the perimeter firewall immediately. Isolate affected segments by VLAN or firewall rule — do not wait for full scope confirmation before isolating systems with confirmed encryption activity.

Evidence: Before isolating any system, capture: (1) full memory dump using WinPmem or Magnet RAM Capture from any actively encrypting host; (2) VSS shadow copy status via 'vssadmin list shadows' — 'The Gentlemen' ransomware group uses VSS deletion as a pre-encryption step, so absence of shadows is itself an indicator; (3) running process list via 'tasklist /v /fo csv > tasklist.csv' and 'Get-Process | Export-Csv' to capture the ransomware process before isolation kills it; (4) active network connections via 'netstat -anob > netstat.csv' to document C2 IP addresses before network isolation severs the connection; (5) Windows Security Event Log 4624/4625 (Logon/Logon Failure) and 4648 (Explicit Credential Use) for all remote and contractor accounts active within 72 hours of first encryption event.

Detection — Review authentication logs for anomalous use of valid accounts (T1078): look for off-hours logins, impossible travel, or accounts accessing bulk PII stores. Audit email gateway logs for phishing delivery (T1566). Monitor endpoint and network logs for large outbound data transfers to unknown external IPs (T1041). Check for file rename events consistent with ransomware staging (T1486).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: For T1078 without a SIEM: run 'Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4624} | Export-Csv logons.csv' and filter for LogonType 10 (RemoteInteractive) or 3 (Network) outside business hours. For T1566 phishing delivery: export email gateway delivery logs (Exchange message tracking: 'Get-MessageTrackingLog -EventId RECEIVE -Start [date]') and grep for attachments with double extensions (.pdf.exe, .docx.lnk) or URLs to newly registered domains. For T1041 exfiltration: use Wireshark or tcpdump on the network egress point — filter 'tcp.len > 1000 && !(ip.dst == [known-good-CIDR])' to surface large sustained transfers. For T1486 file rename events: deploy Sysmon with Event ID 11 (FileCreate) and configure a Sigma rule targeting mass file renames with unknown extensions appended (consistent with 'The Gentlemen' ransomware extension appending behavior).

Evidence: Collect before any log rotation or overwrite: (1) Exchange or O365 message trace logs covering 30 days pre-incident — filter on attachments delivered to property management and HR staff who have access to SSN repositories; (2) VPN/remote access authentication logs (Cisco ASA, Fortinet, Pulse, or equivalent) — export full session logs including source IP, username, session duration, and bytes transferred; (3) Active Directory Security Event Log Event ID 4720 (Account Created), 4732 (Member Added to Security Group), and 4776 (Credential Validation) from all domain controllers — 'The Gentlemen' TTPs include creating persistence accounts post-compromise; (4) DNS query logs from the resolver serving property management systems — large volumes of NXDomain responses or queries to DGA-pattern domains indicate active C2 beaconing; (5) File system audit logs (enable via 'auditpol /set /subcategory:"File System" /success:enable /failure:enable') on the file servers hosting SSN data — look for a single account reading hundreds of files in a short window, which indicates bulk PII staging prior to exfiltration (T1041 precursor).

Eradication — No vendor patch is available for this incident. Harden access controls on systems holding SSN data: enforce MFA on all remote access paths, rotate credentials for any accounts with access to PII repositories, and disable unused service accounts. Review email filtering rules and tighten attachment/link policies to reduce phishing exposure.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For MFA enforcement without enterprise IAM: enable Windows Hello for Business or configure RADIUS-based MFA via Duo Security free tier for VPN and RDP gateways. Credential rotation for PII-repository accounts: run 'net user [username] [newpassword] /domain' or use 'Set-ADAccountPassword' for bulk resets — prioritize all accounts flagged in the T1078 detection step. For service account audit: 'Get-ADServiceAccount -Filter *' and 'Get-WmiObject Win32_Service | Select Name, StartName' — disable any service account not linked to a running business-critical service. For email hardening: configure attachment blocking for .lnk, .vbs, .js, .iso, and macro-enabled Office formats in Exchange Transport Rules or equivalent — these are common 'The Gentlemen' initial access vectors based on ransomware group TTPs documented in threat intelligence.

Evidence: Before eradicating accounts or rotating credentials: (1) export the full current Active Directory account list with last logon timestamps ('Get-ADUser -Filter * -Properties LastLogonDate | Export-Csv ad_accounts.csv') to preserve pre-eradication state for forensic comparison; (2) dump scheduled tasks on all PII-hosting systems ('schtasks /query /fo CSV /v > scheduled_tasks.csv') — ransomware operators commonly plant scheduled tasks for persistence that survive credential rotation; (3) export registry run keys from all affected systems: 'HKLM\Software\Microsoft\Windows\CurrentVersion\Run', 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run', and 'HKLM\SYSTEM\CurrentControlSet\Services' — look for entries with randomized names or paths pointing to temp directories; (4) collect WMI subscription persistence artifacts via 'Get-WMIObject -Namespace root\subscription -Class __EventFilter' and '__EventConsumer' — these survive reboots and are invisible to scheduled task audits.

Recovery — Validate integrity of PII datastores against known-clean backups. Confirm backup systems were not encrypted or exfiltrated. Restore from clean backup only after confirming threat actor persistence has been removed. Engage forensic support to verify no backdoors or scheduled tasks remain. Monitor restored systems for re-encryption or beaconing activity for a minimum of 30 days.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-9 (System Backup), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-9 (Protection of Audit Information), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For backup integrity validation without enterprise backup tooling: compute SHA-256 hashes of backup files before and after restoration ('Get-FileHash -Algorithm SHA256 -Path [backup_path] | Export-Csv hashes.csv') and compare against pre-incident hash baselines if available. To detect backup system compromise: check the backup server's own VSS shadow copies and event logs for ransomware-associated Event ID 7045 (New Service Installed) or 524 (System Audit Log Cleared) within the incident window. For 30-day post-recovery monitoring without EDR: deploy Sysmon with a configuration targeting network connection events (Event ID 3) and process creation (Event ID 1) on restored PII systems — pipe to Windows Event Forwarding (WEF) into a free ELK stack or even a centralized log file reviewed daily by a team member.

Evidence: Before restoring from backup: (1) snapshot the encrypted file system state — record ransomware-appended file extensions across all affected directories ('Get-ChildItem -Recurse | Where-Object {$_.Extension -notin [known-good-extensions]} | Export-Csv encrypted_files.csv') to support forensic reconstruction of the encryption timeline and scope of the 111,000-individual PII exposure; (2) verify whether backup agent service accounts appear in the T1078 lateral movement logs — if backup credentials were harvested, the backup repository must be treated as compromised; (3) capture the ransom note files (typically dropped in each encrypted directory) and preserve for threat intelligence — 'The Gentlemen' ransom notes contain C2 contact information and victim-specific identifiers that support law enforcement referral and threat actor attribution; (4) document the last known-clean backup timestamp relative to the earliest confirmed intrusion indicator — this gap defines the maximum PII exposure window for regulatory notification purposes under state breach notification laws applicable to JRK's tenant locations.

Post-Incident — Conduct a gap assessment against NIST SP 800-53 controls AC-2 (Account Management), MP-6 (Media Sanitization), and SI-3 (Malware Protection). Review data minimization practices: retain SSNs only where legally required and reduce retention periods. Develop or update an incident response playbook specific to ransomware targeting PII-heavy property management environments. Evaluate cyber liability insurance coverage adequacy given active litigation.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-8 (Incident Response Plan), NIST AC-2 (Account Management), NIST SI-3 (Malicious Code Protection), NIST AU-11 (Audit Record Retention), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 3.4 (Enforce Data Retention)

Compensating: Gap assessment without a GRC platform: create a spreadsheet mapping each NIST 800-53 control to current state (Implemented / Partial / Not Implemented) using CIS Controls v8.1 IG1 safeguards as the minimum baseline — this is achievable by one analyst in 2-3 days for a mid-size property management environment. For data minimization audit: run a targeted file content search using PowerShell ('Select-String -Path \\[fileserver]\shares* -Pattern "\b[0-9]{3}-[0-9]{2}-[0-9]{4}\b" -Recurse') or ClamAV with a custom SSN-pattern signature to enumerate where SSNs are stored outside of designated PII repositories. For playbook development: use the CISA Ransomware Response Checklist (freely available at cisa.gov) as a baseline template and annotate it with property management-specific system names, backup locations, and regulatory notification contacts for each state in which JRK operates.

Evidence: Preserve for post-incident review and litigation hold: (1) complete incident timeline reconstruction from all log sources collected during detection, containment, and eradication phases — this is directly relevant to the Fongaro

et al. class-action discovery process and Connecticut AG engagement; (2) before-and-after access control configurations for PII repositories, demonstrating what controls were in place at time of breach versus post-remediation — required for regulatory response and insurance claims; (3) data flow diagram or inventory documenting where SSNs for the estimated 111,000 affected individuals resided, how they were accessed, and what access controls governed them — this directly maps to the 'inadequate security controls' allegation in the complaint; (4) all ransom communications and negotiation records (if any) — preserve under legal hold as they may be discoverable in the class-action proceeding and relevant to FBI/CISA reporting under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) rulemaking timeline.

Detection Guidance

No confirmed IOCs have been publicly released for this incident. Detection should rely on behavioral indicators mapped to the associated MITRE techniques. For T1078 (Valid Accounts): query authentication logs (Windows Event ID 4624, 4625, 4648; Azure AD SignInLogs) for accounts accessing PII stores outside normal business hours or from unfamiliar source IPs. For T1566 (Phishing): review email gateway logs for messages with password-protected attachments or links to newly registered domains in the 30 days preceding April 2025. For T1041 (Exfiltration over C2): alert on large outbound transfers (>500MB) to external IPs not in your approved vendor list, particularly over HTTPS on non-standard ports. For T1486 (Data Encrypted for Impact): monitor file system audit logs for mass file rename or extension change events, which precede ransomware completion. Apply CWE-693 lens: verify that data loss prevention (DLP) controls are logging attempted bulk exports from PII datastores. No confirmed IP, domain, or hash IOCs are available from open sources as of this analysis.

Framework Mappings

MITRE-ATTACK

- **T1041** — Exfiltration Over C2 Channel
- **T1566** — Phishing
- **T1486** — Data Encrypted for Impact
- **T1078** — Valid Accounts

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

- **IR-4** — Incident Handling

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration
T1566	Phishing	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Ransomware attack leads to lawsuit against multistate landlord	https://today.westlaw.com/Document/I1f7e38b53ff111f1a07194109c7dee8...	T3
Federal investigation calls grow for real estate giant behind ...	http://larson.house.gov/media-center/in-the-news/federal-investigat...	T1
Connecticut Office of the Attorney General - Facebook	https://www.facebook.com/CTAttorneyGeneral/posts/earlier-today-i-ha...	T3
Fongaro_et_al_v_JRK_Property...	https://www.pacermonitor.com/public/filings/DUDPGC5Q/Fongaro_et_al_...	T3
Federal investigation calls grow for real estate giant ... - YouTube	https://www.youtube.com/watch?v=oSHiAGCSftg	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-26 13:30 UTC by TJS Security Command Center