INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-22 14:03 UTC

Wright-Ryan Data Breach: Social Security Numbers and Driver's Licenses Compromised

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0193
Type	Data Breach
Severity	HIGH
Affected Products	Wright-Ryan Construction Inc., employees, contractors, and/or clients (specific count unconfirmed)
Published	2026-06-22
Discovery Source	Gemini

Executive Summary

Wright-Ryan Construction Inc., a Maine-based construction firm, disclosed a data breach exposing Social Security Numbers and driver's license numbers belonging to employees, contractors, and/or clients. The specific number of affected individuals and the attack vector remain unconfirmed, as no authoritative breach notification filing or state AG disclosure was identified in available sources. Organizations with workforce or vendor relationships with Wright-Ryan should treat affected individuals as at elevated risk for identity theft and targeted fraud.

Technical Analysis

Wright-Ryan Construction Inc. reported a data breach involving sensitive PII, specifically Social Security Numbers (SSNs) and driver's license numbers. No CVE is applicable; this is an organizational breach, not a software vulnerability. CWE classification cannot be assigned, as the root cause (unauthorized access, ransomware, insider threat, or third-party exposure) has not been disclosed in available source material. No attack vector, intrusion timeline, affected system, or patch status has been confirmed. MITRE ATT&CK technique mapping is not possible without root cause data. Source quality score is 0.56, reflecting discovery via search grounding and reliance on T3 sources rather than authoritative breach notification filings or T1 news outlets.

Action Checklist

1. Step 1: Assessment. If your organization employs or contracts with Wright-Ryan Construction, verify whether your firm shared PII with them and assess exposure scope, including which employees or

contractors may have submitted SSNs or driver's license numbers and whether any shared systems or portals were involved.

2. Step 2: Detection. Monitor for anomalous use of SSNs or driver's license numbers associated with affected individuals; review identity monitoring alerts and HR/vendor onboarding data logs for signs of unauthorized access or data exfiltration (NIST SI-4: System Monitoring; CIS 8.2: Collect Audit Logs).

3. Step 3: Eradication. Root cause is unconfirmed; no specific patch or configuration remediation can be prescribed. Engage Wright-Ryan directly or monitor Maine AG breach notification filings for official disclosure detailing the attack vector and affected systems before taking targeted eradication steps (NIST IR-2: Incident Response Coordination).

4. Step 4: Recovery. Notify affected individuals per applicable state breach notification requirements; coordinate with HR and legal to assess notification obligations. Validate that any shared access or vendor portal credentials associated with Wright-Ryan are rotated (NIST IR-4: Incident Handling; D3-CRO: Credential Rotation).

5. Step 5: Post-Incident. Review third-party vendor data-sharing agreements and PII handling practices; confirm that vendors are contractually obligated to disclose breaches within defined timeframes. Map control gaps to NIST IR-8 (Incident Response Plan) and assess whether vendor risk assessments include breach notification SLA requirements.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if any evidence emerges that your organization's employee or contractor SSNs or driver's license numbers were among the Wright-Ryan-exposed records, or if Maine AG breach notification filings confirm a regulated notification obligation applies to your organization as a downstream-affected party.
Recovery Notes	Post-containment, monitor affected individuals' identity posture for a minimum of 12 months given that SSNs and driver's license numbers are non-revocable identifiers with long fraud lifecycles — coordinate with HR to offer credit monitoring services (Experian, Equifax, or equivalent) to confirmed affected individuals. Verify that all Wright-Ryan-linked vendor portal accounts have been fully disabled and that no residual shared credentials exist in password managers or CI/CD secrets stores. Continue polling the Maine AG breach notification viewer monthly until an official Wright-Ryan filing is published, as the disclosed attack vector will determine whether additional eradication actions are required.

Forensic Artifacts	HR and vendor onboarding platform audit logs (ADP, Workday, or equivalent) — filter for export or download events on records containing SSN or government ID fields within 180 days preceding breach disclosure, as unauthorized bulk export is a primary exfiltration pattern for workforce PII breaches | Email gateway/DLP logs for outbound messages or attachments to Wright-Ryan domains containing SSN-pattern data (regex \d{3}-\d{2}-\d{4}) or driver's license format strings, which would indicate PII was transmitted in cleartext via email rather than a secure portal | Shared vendor portal (e.g., Procore, Textura, or proprietary Wright-Ryan credentialing system) authentication logs — specifically failed login attempts, unusual geographic login origins, and bulk record access events that would indicate credential stuffing or unauthorized session activity against the portal holding employee/contractor PII | Maine AG breach notification filing (maine.gov/agviewer) — when published, the official notification will specify attack vector, affected record categories, date of discovery, and affected individual count, all of which are required inputs for scoping your downstream notification obligations and targeted eradication actions | Internal PII data-sharing inventory and vendor data processing agreements for Wright-Ryan — these documentary artifacts establish which specific PII fields were transmitted, the legal basis for transmission, and whether Wright-Ryan's contractual breach notification SLA was met, directly informing regulatory exposure under applicable state notification laws

Per-Action IR Details

Step 1: Containment — If your organization employs or contracts with Wright-Ryan Construction, identify which employees or contractors may have shared PII with the firm and assess whether any shared systems or portals were involved in the breach.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Query your HR or vendor management system exports (CSV/Excel) for any personnel records transmitted to Wright-Ryan (W-9s, I-9s, onboarding packets, background check authorizations). Cross-reference against any shared portals or vendor credentialing platforms (e.g., Procore, Textura, BuildingConnected) by auditing access logs manually. A 2-person team can use grep or PowerShell Select-String against exported logs to identify accounts linked to Wright-Ryan domains.

Evidence: Before suspending any shared portal accounts or revoking Wright-Ryan-linked credentials, preserve: (1) access logs from any shared vendor portals showing Wright-Ryan user activity, session tokens, and IP addresses; (2) email server logs (Exchange message trace or Gmail Admin audit) showing PII attachments or data transfers to Wright-Ryan addresses; (3) HR platform audit trails (e.g., ADP, Workday activity logs) showing which employee/contractor records were shared or exported. Capture these logs before any account suspension alters authentication state.

Step 2: Detection — Monitor for anomalous use of SSNs or driver's license numbers associated with affected individuals; review identity monitoring alerts and HR/vendor onboarding data logs for signs of unauthorized access or data exfiltration (NIST SI-4: System Monitoring; CIS 8.2: Collect Audit Logs).

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, deploy osquery on endpoints to query recently accessed files containing PII patterns: `SELECT * FROM file WHERE path LIKE '%onboarding%' OR path LIKE '%contractor%' AND atime > (strftime('%s','now') - 2592000);`. Use PowerShell to scan Windows Security Event Log for Event ID 4663 (object

access) on HR document directories: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4663} | Select-Object TimeCreated, Message | Export-Csv`. Subscribe to free identity monitoring via HaveIBeenPwned API for affected individual email addresses, and monitor Maine AG breach notification portal (maine.gov/agviewer) manually on a scheduled basis.

Evidence: Because this breach involves SSNs and driver's license numbers, detect downstream misuse by capturing: (1) HR platform login audit logs filtered for access to employee/contractor PII records in the 90 days preceding breach disclosure; (2) DLP or email gateway logs for outbound transmissions of files containing SSN patterns (regex: \d{3}-\d{2}-\d{4}) to external domains; (3) any identity verification or E-Verify system access logs; (4) VPN or remote access logs showing Wright-Ryan-attributed IP ranges accessing internal HR systems. No host volatile state is altered in this detection step, but log preservation is time-sensitive as retention windows may expire.

Step 3: Eradication — Root cause is unconfirmed; no specific patch or configuration remediation can be prescribed. Engage Wright-Ryan directly or monitor Maine AG breach notification filings for official disclosure detailing the attack vector and affected systems before taking targeted eradication steps.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST SI-5 (Security Alerts, Advisories, And Directives), NIST IR-6 (Incident Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Monitor the Maine AG public breach notification viewer at maine.gov/agviewer on a recurring weekly basis (calendar reminder) and set a Google Alert for 'Wright-Ryan Construction breach notification' to detect when the official filing is posted. Document all direct outreach to Wright-Ryan (date, contact, response) in your incident log to satisfy NIST IR-5 tracking requirements. If a shared portal is confirmed involved, treat that portal as compromised and initiate credential rotation and access review regardless of pending disclosure.

Evidence: No host live state is altered in this holding step; however, preserve the following before any future eradication actions become possible once root cause is confirmed: (1) current snapshot of any shared portal configuration and user access lists; (2) Wright-Ryan vendor contract and data-sharing agreement documents establishing what PII was authorized to be transmitted; (3) any breach notification communications received from Wright-Ryan, including metadata (received timestamp, sender headers). These establish scope and legal notice timelines relevant to downstream notification obligations.

Step 4: Recovery — Notify affected individuals per applicable state breach notification requirements; coordinate with HR and legal to assess notification obligations. Validate that any shared access or vendor portal credentials associated with Wright-Ryan are rotated (NIST IR-4: Incident Handling; D3-CRO: Credential Rotation).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), CIS 6.2 (Establish an Access Revoking Process), CIS 5.2 (Use Unique Passwords)

Compensating: Use a free password manager (Bitwarden for Teams free tier) to enforce unique credential rotation for all accounts linked to Wright-Ryan portals, and document rotation timestamps. For notification obligation tracking without legal counsel on retainer, cross-reference the affected individuals' states of residence against the NCSL state breach notification law database (ncsl.org) to identify applicable deadlines — Maine requires notification within 30 days of discovery. Generate a simple notification tracking spreadsheet logging: individual name, state, notification method, date sent, confirmation receipt.

Evidence: BEFORE rotating credentials on any shared vendor portal or HR system, capture: (1) current active session list from the portal (screenshot or API export) showing all active Wright-Ryan-linked sessions and their originating IP addresses; (2) full access control list (ACL) export from the portal showing Wright-Ryan user accounts and their permission levels; (3) authentication logs for the past 90 days from the portal, preserving evidence of any unauthorized access that occurred prior to credential rotation. Credential rotation is a live-state-altering action — these volatile artifacts must be captured first per RFC 3227 order of volatility.

Step 5: Post-Incident — Review third-party vendor data-sharing agreements and PII handling practices; confirm that vendors are contractually obligated to disclose breaches within defined timeframes. Map control gaps to NIST IR-8 (Incident Response Plan) and assess whether vendor risk assessments include breach notification SLA requirements.

NIST Phase: Post Incident

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

Controls: NIST IR-8 (Incident Response Plan), NIST IR-1 (Policy And Procedures), NIST SI-12 (Information Management And Retention), CIS 3.4 (Enforce Data Retention)

Compensating: Conduct a tabletop exercise (no-cost, 2-person) using the Wright-Ryan scenario as the test case: walk through your vendor onboarding checklist and identify which vendors currently receive SSNs or government ID numbers, whether each has a signed DPA with breach notification SLA, and whether your IR plan addresses third-party breach notification as a trigger. Document findings in a gap register. Use the free NIST Cybersecurity Framework Online Informative References tool to cross-map identified gaps to controls. Update vendor contracts at next renewal cycle to include explicit 72-hour breach notification SLA language.

Evidence: No volatile evidence capture is required at the post-incident phase; this step operates on documentary artifacts already preserved. Assemble the post-incident record package: (1) timeline of Wright-Ryan breach disclosure versus your organization's discovery date, to verify whether vendor notification met contractual SLA; (2) inventory of all PII categories transmitted to Wright-Ryan (SSNs, DL numbers, dates of birth) with the legal basis for each transmission; (3) gap analysis document identifying which vendor risk assessment checklist items failed to surface Wright-Ryan's PII custodian status; (4) lessons-learned report per NIST 800-61r3 §4 to update the IR plan with third-party breach trigger criteria.

Detection Guidance

No IOCs, attack vectors, or compromised system identifiers have been confirmed in available source material. Detection guidance is limited to upstream signals. Monitor Maine Attorney General breach notification filings and HaveIBeenPwned or similar identity monitoring services for Wright-Ryan-linked data appearing in breach corpora. If your organization shared employee or contractor PII with Wright-Ryan, alert HR and identity monitoring programs to watch for SSN or driver's license misuse. Per NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs), ensure audit logging is active on any shared vendor portals or HR systems that may have interfaced with Wright-Ryan. No specific log queries, event IDs, or behavioral IOC patterns can be provided without confirmed attack vector data.

Framework Mappings

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **RS.CO-03** — Recovery activities and progress communicated
- **GV.SC-01** — Cybersecurity supply chain risk management program

NIST-800-53R5

- **CP-9** — System Backup
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(6)(ii)** — Response and Reporting

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.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC7.4** — Responds to identified security incidents
- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

Sources

Source	URL	Tier
Wright Ryan: Home	https://www.wright-ryan.com/	T3
[PDF] CONSTRUCTION MANAGER PREQUALIFACTION QUESTIONNAIRE	https://cms6.revize.com/revize/berwickme/Document%20Center/Governme ...	T3
Working at Wright-Ryan Construction | Glassdoor	https://www.glassdoor.com/Overview/Working-at-Wright-Ryan-Construct...	T3
Wright-Ryan Construction, Inc. - LinkedIn	https://www.linkedin.com/company/wright-ryan-construction-inc.	T3
News & Press - Wright Ryan	https://www.wright-ryan.com/news-press/	T3

Generated 2026-06-22 14:03 UTC by TJS Security Command Center