INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-10 19:21 UTC

Karl Auto Group Data Breach Exposes Social Security Numbers and Other Sensitive Data

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0159
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Karl Auto Group (Karl Malone Auto Group), Iowa automotive dealership group; customers whose data was held on file
Published	2026-06-10
Discovery Source	Gemini

Executive Summary

Karl Malone Auto Group, an Iowa-based automotive dealership chain, disclosed a data breach discovered April 4, 2026, exposing customer Social Security numbers, driver's license numbers, financial account details, passport information, and full names. The FBI is actively investigating, and operational disruption to Iowa dealerships has been confirmed. Organizations holding similar customer PII face heightened regulatory scrutiny, class-action litigation risk, and reputational exposure as legal action against Karl Auto Group is anticipated.

Technical Analysis

Karl Malone Auto Group suffered a confirmed cyberattack resulting in unauthorized access to customer PII. The attack vector has not been publicly confirmed; no specific malware family, ransomware variant, or CVE has been attributed as of available reporting. MITRE techniques associated with this incident pattern include T1078 (Valid Accounts, potential initial access vector), T1041 (Exfiltration Over C2 Channel), T1657 (Financial Theft), and T1486 (Data Encrypted for Impact, consistent with ransomware-type disruption). Relevant CWEs: CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor), CWE-693 (Protection Mechanism Failure), CWE-284 (Improper Access Control). No CVE is assigned. Operational disruption to dealerships suggests possible ransomware or destructive component. The breach notice was filed formally, indicating regulatory notification obligations were triggered. Primary authoritative notice is the organization's own filing per JD Supra reporting.

Action Checklist

1. Step 1: Containment, If your organization operates in automotive retail or holds similar PII profiles (SSNs, DL numbers, financial accounts, passport data), audit third-party vendor access immediately. Verify no shared infrastructure or data-sharing agreements exist with Karl Auto Group systems. Suspend any active data feeds to or from the affected entity pending confirmation of scope (NIST AC-20, Use of External Systems; CIS 1.1, Enterprise Asset Inventory).
2. Step 2: Detection, Review logs for anomalous outbound data transfers, credential use outside business hours, and lateral movement indicators consistent with T1078 (Valid Accounts) and T1041 (Exfiltration Over C2). Query SIEM for bulk export events against customer PII datastores. Check for unauthorized account creation or privilege escalation in identity logs. No confirmed IOCs are publicly available; hunt on behavioral patterns (NIST AU-6, Audit Record Review, Analysis, and Reporting; CIS 8.2, Collect Audit Logs).
3. Step 3: Eradication, No specific patch or CVE remediation applies. Enforce least privilege across customer data repositories (NIST AC-6, Least Privilege; CIS 5.4, Restrict Administrator Privileges). Rotate credentials for all accounts with access to PII stores (NIST IA-4, Identifier Management). Review and tighten access control lists on sensitive data systems (NIST AC-3, Access Enforcement; CIS 3.3, Configure Data Access Control Lists).
4. Step 4: Recovery, Validate that PII datastores are accessible only to authorized accounts and that no unauthorized exports occurred within your environment. Enable enhanced monitoring on customer data repositories post-review. Confirm audit logging is active and forwarding correctly for all systems touching SSNs, financial data, or government-issued ID numbers (NIST AU-12, Audit Record Generation; NIST AU-9, Protection of Audit Information).
5. Step 5: Post-Incident, This incident exposes common control gaps in automotive retail and SMB environments: insufficient segmentation of customer PII, weak third-party access controls, and absence of data activity monitoring. Conduct a tabletop exercise against a ransomware-plus-exfiltration scenario. Review your breach notification procedures and confirm regulatory timelines are documented (NIST IR, Incident Response family; CIS 7.1, Establish and Maintain a Vulnerability Management Process).

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if your organization shares a DMS vendor platform, data-sharing agreement, or third-party integration with Karl Auto Group, or if internal log review reveals bulk PII exports, unauthorized account activity, or any customer records matching the SSN/DL/financial account/passport data profile disclosed in the Karl Auto Group breach notification — FBI involvement and active class-action litigation exposure make delayed escalation a material legal and regulatory risk.

Recovery Notes	Post-containment, maintain enhanced database audit logging on all PII datastores for a minimum of 90 days and preserve all logs under litigation hold given the active FBI investigation and anticipated class-action proceedings against Karl Auto Group. Verify weekly for the first month that no new unauthorized account activity, scheduled jobs, or outbound data transfers appear against customer PII repositories. Confirm your breach notification counsel has reviewed whether your organization's exposure to the same customer data profile triggers independent state notification obligations independent of Karl Auto Group's own disclosure.
Forensic Artifacts	DMS application audit logs (CDK Global, Reynolds & Reynolds, DealerSocket, or equivalent) — these systems are the primary repositories for automotive customer PII including SSNs, DL numbers, and financial application data, and would contain query history, report exports, and user session records most directly relevant to a data exfiltration event of this profile | SQL Server or MySQL query logs and default trace files on databases containing customer finance application tables — specifically large-row-count SELECT operations or bulk export events (BCP, OPENROWSET, SELECT INTO OUTFILE) against columns containing SSN, driver_license, account_number, or passport fields executed in the 90 days preceding April 4, 2026 | VPN and remote access authentication logs for all vendor accounts and service accounts with DMS or customer database access — focusing on off-hours authentication, geographically anomalous source IPs, and concurrent sessions, given that T1078 (Valid Accounts) is the most likely initial access vector in dealership-sector PII breaches where direct CVE exploitation is not confirmed | Windows Security Event Log Event ID 4663 (Object Access — file or database object read) and Event ID 4688 (Process Creation) on servers hosting PII datastores — particularly any instances of sqlcmd.exe, bcp.exe, mysqldump, or scripting interpreters (powershell.exe, wscript.exe, python.exe) spawned under service account or vendor account context | Network flow data or perimeter firewall logs showing outbound large-payload transfers (>10MB sustained) from DMS servers or database hosts to non-standard external destinations during the period January 1, 2026 through April 4, 2026 — specifically flagging transfers to cloud storage endpoints, residential IP ranges, or TOR exit nodes as indicators consistent with T1041 (Exfiltration Over C2) in the absence of confirmed public IOCs

Per-Action IR Details

Step 1: Containment — If your organization operates in automotive retail or holds similar PII profiles (SSNs, DL numbers, financial accounts, passport data), audit third-party vendor access immediately. Verify no shared infrastructure or data-sharing agreements exist with Karl Auto Group systems. Suspend any active data feeds to or from the affected entity pending confirmation of scope (NIST AC-20 — Use of External Systems; CIS 1.1 — Enterprise Asset Inventory).

NIST Phase: Containment

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

Controls: NIST AC-20 (Use Of External Systems), NIST AC-4 (Information Flow Enforcement), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run 'netstat -ano' on systems holding PII datastores and cross-reference active outbound connections against your known vendor IP list. Use Windows Firewall 'wf.msc' or iptables to immediately block outbound traffic to Karl Auto Group IP ranges while investigation is underway. Document all third-party data-sharing agreements in a shared spreadsheet if no formal CMDB exists — focus on DMS (Dealer Management System) vendors common in automotive retail (CDK Global, Reynolds & Reynolds, DealerSocket) as these are frequent shared-infrastructure points.

Evidence: Before suspending feeds, capture: current active network connections (netstat output saved to file), firewall logs showing recent outbound transfers to Karl Auto Group IP space or shared DMS vendor infrastructure, and any API

gateway or SFTP transfer logs showing data exports to external endpoints within the past 90 days. Preserve these logs to removable media or an isolated log server before making any network changes that could alter connection state.

Step 2: Detection — Review logs for anomalous outbound data transfers, credential use outside business hours, and lateral movement indicators consistent with T1078 (Valid Accounts) and T1041 (Exfiltration Over C2). Query SIEM for bulk export events against customer PII datastores. Check for unauthorized account creation or privilege escalation in identity logs. No confirmed IOCs are publicly available; hunt on behavioral patterns (NIST AU-6 — Audit Record Review, Analysis, and Reporting; CIS 8.2 — Collect Audit Logs).

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM, query Windows Security Event Log directly using PowerShell: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4624,4625,4648,4720,4732,4776)} | Export-Csv auth_events.csv'. Focus Event ID 4648 (explicit credential use) and 4720 (account creation) against service accounts with access to customer PII tables. For database exfiltration hunting, query SQL Server error logs and default trace for large SELECT statements: 'SELECT TOP 1000 * FROM sys.traces' and review fn_trace_gettable output for bulk read operations against tables containing SSN or DL columns. Deploy Sysmon with SwiftOnSecurity config to capture process creation (Event ID 1) and network connections (Event ID 3) if not already present.

Evidence: Capture before analysis: SQL Server or MySQL slow query logs and audit logs showing large row-count SELECT queries against customer PII tables (typically finance_applications, customer_records, or deal_jacket tables in DMS systems); Windows Security Event Log exports for the 90 days prior to April 4, 2026 (breach discovery date); VPN and remote access authentication logs for service accounts and vendor accounts; DMS application-layer logs (CDK, Reynolds & Reynolds, or DealerSocket audit trails) showing data export or report generation events; and any scheduled task or batch job logs that could indicate automated exfiltration staging.

Step 3: Eradication — No specific patch or CVE remediation applies. Enforce least privilege across customer data repositories (NIST AC-6 — Least Privilege; CIS 5.4 — Restrict Administrator Privileges). Rotate credentials for all accounts with access to PII stores (D3-CRO — Credential Rotation). Review and tighten access control lists on sensitive data systems (NIST AC-3 — Access Enforcement; CIS 3.3 — Configure Data Access Control Lists).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST AC-3 (Access Enforcement), NIST AC-2 (Account Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 3.3 (Configure Data Access Control Lists)

Compensating: Use PowerShell to enumerate all accounts with direct SELECT permissions on PII-bearing database tables: 'Invoke-Sqlcmd -Query "SELECT dp.name, dp.type_desc, o.name AS object_name, p.permission_name FROM sys.database_permissions p JOIN sys.database_principals dp ON p.grantee_principal_id = dp.principal_id JOIN sys.objects o ON p.major_id = o.object_id WHERE p.permission_name IN (\"SELECT\",\"EXECUTE\")" -ServerInstance [your_server]'. Immediately disable any vendor or service accounts not actively required. For credential rotation without enterprise tooling, use a tracked spreadsheet with enforced completion deadlines and require confirmation replies from account owners — prioritize any shared credentials used across Karl Auto Group and your organization if a data-sharing relationship existed.

Evidence: Before credential rotation, preserve: a full export of current database permission assignments (sp_helprotect output for all PII tables), Active Directory group membership snapshots for groups with DMS or customer database access (Get-ADGroupMember), and current scheduled tasks and service account configurations (schtasks /query /fo CSV /v > scheduled_tasks.csv) — these establish pre-eradication access baseline for forensic comparison and potential litigation hold requirements given active FBI investigation.

Step 4: Recovery — Validate that PII datastores are accessible only to authorized accounts and that no unauthorized exports occurred within your environment. Enable enhanced monitoring on customer data

repositories post-review. Confirm audit logging is active and forwarding correctly for all systems touching SSNs, financial data, or government-issued ID numbers (NIST AU-12 — Audit Record Generation; NIST AU-9 — Protection of Audit Information).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-12 (Audit Record Generation), NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), NIST AU-4 (Audit Storage Capacity)

Compensating: Enable SQL Server Audit or MySQL General Query Log on all tables containing SSNs, DL numbers, financial account data, and passport fields — capture all SELECT, INSERT, UPDATE, DELETE with user context and timestamp. Forward logs to a dedicated log host separate from the production DMS environment using syslog or WEF (Windows Event Forwarding) to prevent tampering, consistent with NIST AU-9. Verify log storage capacity (NIST AU-4) is sufficient for 12-month retention given potential litigation hold tied to the active FBI investigation and anticipated class-action exposure. Use 'auditpol /get /category:*' on Windows systems to confirm audit policy is fully enabled.

Evidence: Before declaring recovery complete, capture a point-in-time snapshot of: database audit log continuity (confirm no logging gaps between March 1, 2026 and April 4, 2026 discovery date); file integrity baselines of customer PII export directories and report output folders using free tool AIDE or PowerShell Get-FileHash against known-good manifests; and current user session activity on all systems with PII access to confirm no residual unauthorized sessions remain active.

Step 5: Post-Incident — This incident exposes common control gaps in automotive retail and SMB environments: insufficient segmentation of customer PII, weak third-party access controls, and absence of data activity monitoring. Conduct a tabletop exercise against a ransomware-plus-exfiltration scenario. Review your breach notification procedures and confirm regulatory timelines are documented (NIST IR — Incident Response family; CIS 7.1 — Establish and Maintain a Vulnerability Management Process).

NIST Phase: Post Incident

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AC-1 (Policy And Procedures), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Document lessons learned in a structured after-action report within 2 weeks of completing Steps 1–4, specifically addressing: whether your DMS vendor contracts include breach notification obligations to your organization, whether Iowa data breach notification law (Iowa Code §715C) or your state equivalent applies to your customer records, and whether SSN exposure triggers FTC Safeguards Rule (16 CFR Part 314) notification or remediation obligations for auto dealers — this is dealership-sector specific and directly relevant given Karl Auto Group's profile. Use the NIST 800-61r3 lessons learned template questions as a tabletop scenario framework, substituting the Karl Auto Group attack pattern (PII exfiltration from DMS, operational disruption, FBI engagement) as the scenario seed.

Evidence: Compile for the lessons-learned record: a timeline reconstruction of all vendor access events from 90 days prior to April 4, 2026 through containment completion; documentation of which PII categories (SSNs, DL numbers, financial accounts, passport data) exist in your environment mapped to the same profile disclosed in the Karl Auto Group breach notification; and written confirmation from your DMS vendor of their incident status, scope, and any shared infrastructure involvement — this documentation supports both regulatory response and potential litigation defense.

Detection Guidance

No confirmed IOCs (IPs, domains, hashes) have been publicly released as of available reporting. Detection must rely on behavioral indicators. Focus on: (1) Bulk read or export events against tables or datastores containing SSNs, DL numbers, or financial account fields, query SIEM for high-volume SELECT or export

operations outside normal business hours. (2) T1078, anomalous use of valid accounts: logins from new geolocations, unusual hours, or unfamiliar devices against customer data systems. (3) T1041, large outbound transfers to unfamiliar external destinations, particularly compressed or encrypted payloads. (4) T1486, file rename events at scale, shadow copy deletion, or backup tampering consistent with ransomware staging. (5) Monitor local account activity on systems holding PII (NIST AC-2, Account Management). Relevant controls: NIST AU-6 (Audit Record Review), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs).

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1041** — Exfiltration Over C2 Channel
- **T1657** — Financial Theft
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration
T1657	Financial Theft	Impact
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
FBI investigates cyberattack on Iowa's Karl Auto Group - KCCI	https://www.kcci.com/article/fbi-investigates-cyberattack-iowas-kar...	T3
Karl Malone Auto Group Files Notice of Recent Data Breach	https://www.jdsupra.com/legalnews/karl-malone-auto-group-files-noti...	T3
Karl Auto Group cyberattack disrupts Iowa dealerships	https://dysruptionhub.com/karl-auto-group-iowa-cyberattack/	T3
Karl Malone Auto Group Data Breach Investigation	https://www.myinjuryattorney.com/karl-malone-auto-group-data-breach...	T2
Karl Auto Group cyberattack disrupts Iowa dealers - Reddit	https://www.reddit.com/r/CyberIncidentReports/comments/1tx7l7t/karl...	T3

Generated 2026-06-10 19:21 UTC by TJS Security Command Center