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

Figure Technology Solutions, Inc. discloses cybersecurity incident (8-K), ~1,000,000 records affected

DATA BREACH | HIGH | CVSS 9.0

SCC Item ID	SCC-DBR-2026-0160
Type	Data Breach
Severity	HIGH
CVSS Base Score	9.0
Affected Products	Figure Technology Solutions, Inc., customer/user records (~1,000,000 individuals)
Published	2026-06-10
Discovery Source	Sec 8K

Executive Summary

Figure Technology Solutions, Inc. disclosed a cybersecurity incident via SEC 8-K filing affecting approximately 1 million user records. The breach carries litigation risk, law firm Lynch Carpenter has announced a formal investigation, and the disclosure coincides with Figure's pending acquisition of Kiavi, Inc., which may complicate due diligence and deal timelines. Attack vector, compromised data types, and intrusion timeline are not yet publicly confirmed; organizations with customer or vendor relationships with Figure should treat this as an active exposure until details are clarified.

Technical Analysis

Figure Technology Solutions disclosed a data breach via SEC 8-K affecting approximately 1,000,000 user records. No CVE has been assigned, consistent with a data breach incident rather than a discrete software vulnerability. The CVSS base score of 9.0 supplied in the source data is an operator estimate; no published CVSS vector string is available for independent verification. CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor) is mapped. MITRE ATT&CK techniques associated with the incident pattern are T1530 (Data from Cloud Storage), T1078 (Valid Accounts), and T1566 (Phishing); these reflect the probable technique space for this breach class and are not confirmed from attribution evidence in the source material. No threat actor has been publicly attributed. The attack vector, affected systems, and data types compromised (e.g., PII, financial records, credentials) have not been confirmed in publicly available disclosures. The SEC 8-K filing index is sourced from EDGAR (T1 source). Secondary coverage from SecurityWeek and Lynch Carpenter (both T3) reports the ~1 million record figure. The merger context (Figure acquiring Kiavi, Inc.)

is material; breach disclosure timing and data scope may intersect with transaction obligations and regulatory review.

Action Checklist

1. Step 1: Containment, Identify any direct data-sharing, API integrations, or vendor relationships with Figure Technology Solutions. Suspend or isolate data flows to/from Figure systems until breach scope is publicly clarified. Per NIST AC-20 (Use of External Systems), review and restrict external system connections where the third party's security posture is unconfirmed.
2. Step 2: Detection, Review access logs for any accounts or credentials shared with Figure Technology Solutions or its systems. Monitor for anomalous authentication attempts or unexpected data access events consistent with T1078 (Valid Accounts) abuse. Audit cloud storage access logs (aligned with T1530) for unauthorized data egress. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting); query SIEM for access events involving Figure-affiliated accounts, IP ranges, or data segments within the past 90 days. CIS 8.2 (Collect Audit Logs), confirm logging is active across all systems that may have interfaced with Figure.
3. Step 3: Eradication, Rotate any shared credentials, API keys, or service account tokens used in integrations with Figure Technology Solutions per D3-CRO (Credential Rotation). If phishing (T1566) is confirmed as an initial access vector in future disclosures, conduct targeted email header analysis and block associated sender infrastructure. Apply D3-CH (Credential Hardening) to any accounts with exposure to Figure's environment.
4. Step 4: Recovery, After credential rotation, verify no residual unauthorized sessions exist using D3-LAM (Local Account Monitoring). Confirm that access control lists governing data shared with Figure are reset to least privilege per NIST AC-6 (Least Privilege) and CIS 3.3 (Configure Data Access Control Lists). Monitor for follow-on activity consistent with data re-use, credential stuffing, targeted spear-phishing, or synthetic identity fraud over the 30 days following containment.
5. Step 5: Post-Incident, Conduct a third-party vendor risk review. Assess whether your vendor onboarding process captures breach notification obligations and data-sharing minimization requirements. Reference NIST AC-20 (Use of External Systems) and CIS 3.2 (Establish and Maintain a Data Inventory) to close gaps in external data exposure visibility. Document findings and update vendor risk register.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if forensic review confirms your organization transmitted PII (names, SSNs, financial account data, or contact information) to Figure Technology Solutions, as this triggers state breach notification obligations (CCPA, GLBA, and applicable state laws) and creates direct exposure to the Lynch Carpenter class action investigation; also escalate if any Figure-affiliated credentials are identified as actively abused in your environment.

Recovery Notes	Post-containment, maintain a 30-day elevated monitoring period specifically watching for credential stuffing attacks against customer-facing authentication endpoints, as exfiltrated Figure records covering ~1 million individuals represent a ready-made target list for automated account takeover tools. Verify that all data-sharing interfaces with Figure remain suspended or re-established only under revised contractual terms with explicit security posture requirements, particularly given the unresolved breach scope and pending Kiavi acquisition due diligence. Retain all forensic artifacts, log exports, and remediation documentation in legal hold status given Lynch Carpenter's active investigation — do not alter or delete any records created during or after the response window.
Forensic Artifacts	API gateway and application-layer HTTP access logs for all Figure Technology Solutions integration endpoints — filter for bulk GET/POST requests, unusually large response payloads, and off-hours access patterns that would indicate automated data exfiltration of the ~1 million record dataset | OAuth token issuance and revocation logs from your identity provider (Okta, Azure AD, or equivalent) for all service accounts and federated identities authorized to access Figure-affiliated systems — preserving token lifetimes and scope grants to establish unauthorized access windows | AWS CloudTrail or Azure Monitor activity logs for any cloud storage buckets, databases, or data lakes containing customer records shared with Figure — specifically 'GetObject', 'ListBucket', and 'AssumeRole' events that would indicate data staging or exfiltration by an unauthorized party leveraging compromised Figure credentials | Email gateway logs (full headers, sender IP, SPF/DKIM/DMARC pass-fail results) for inbound messages from figure.com and related domains over the past 90 days, to establish a baseline for phishing detection if T1566 is confirmed as the Figure breach initial access vector in subsequent public disclosures | Executed data processing agreements, data sharing addenda, and security questionnaire responses from Figure Technology Solutions vendor onboarding — these are the primary documentary artifacts needed to assess your organization's regulatory exposure and demonstrate due diligence to regulators or in response to Lynch Carpenter investigation subpoenas

Per-Action IR Details

Step 1: Containment — Identify any direct data-sharing, API integrations, or vendor relationships with Figure Technology Solutions. Suspend or isolate data flows to/from Figure systems until breach scope is publicly clarified. Per NIST AC-20 (Use of External Systems), review and restrict external system connections where the third party's security posture is unconfirmed.

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 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run 'netstat -ano' or 'ss -tunap' on boundary hosts to enumerate active connections to Figure-owned IP ranges (cross-reference Figure's ASN via WHOIS/BGP lookup). Block Figure-affiliated CIDR blocks at the perimeter firewall using explicit deny rules. For API integrations, revoke OAuth tokens or rotate API keys immediately and disable the integration endpoint at the application layer. A 2-person team can execute this with firewall CLI access and a spreadsheet-based vendor integration register in under 2 hours.

Evidence: BEFORE suspending data flows, capture full NetFlow or firewall session logs showing all connections to/from Figure Technology Solutions IP ranges and API endpoints over the past 90 days. Export firewall allow/deny logs filtered on Figure's domains (e.g., figure.com, hometap.com if applicable) and any registered API gateway access logs showing outbound POST/GET calls to Figure endpoints. Preserve these logs to an offline or write-protected location prior to any firewall rule changes.

Step 2: Detection — Review access logs for any accounts or credentials shared with Figure Technology Solutions or its systems. Monitor for anomalous authentication attempts or unexpected data access events consistent with T1078 (Valid Accounts) abuse. Audit cloud storage access logs (aligned with T1530) for unauthorized data egress. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) — query SIEM for access events involving Figure-affiliated accounts, IP ranges, or data segments within the past 90 days. CIS 8.2 (Collect Audit Logs) — confirm logging is active across all systems that may have interfaced with Figure.

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), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use PowerShell to query Windows Security Event Log for Event ID 4624 (Successful Logon) and 4648 (Logon with Explicit Credentials) filtering on service accounts or federated identity tokens associated with Figure integrations: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4624,4648) -and $_.Message -match "figure"}'. For cloud storage (AWS S3 or Azure Blob), use AWS CloudTrail or Azure Monitor activity logs — export via CLI ('aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventName,AttributeValue=GetObject') and filter on buckets containing data shared with Figure. Use Sigma rule 'win_suspicious_service_account_login.yml' (SigmaHQ repo) adapted to flag Figure-affiliated account strings.

Evidence: Capture authentication logs (Windows Event IDs 4624, 4648, 4768, 4769 for Kerberos) for any service accounts or SSO identities used in Figure integrations over the past 90 days. Export AWS CloudTrail 'GetObject', 'PutObject', and 'DeleteObject' events or equivalent Azure Blob Storage diagnostic logs for any data buckets shared with Figure. If a customer data API was involved, capture application-layer HTTP access logs showing request volumes, response codes, and payload sizes to detect bulk data exfiltration patterns (unusually high 200-OK GET responses with large response bodies) consistent with unauthorized enumeration of ~1 million records.

Step 3: Eradication — Rotate any shared credentials, API keys, or service account tokens used in integrations with Figure Technology Solutions, per D3-CRO (Credential Rotation). If phishing (T1566) is confirmed as an initial access vector in future disclosures, conduct targeted email header analysis and block associated sender infrastructure. Apply D3-CH (Credential Hardening) to any accounts with exposure to Figure's environment.

NIST Phase: Eradication

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

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), NIST IA (Identification and Authentication) — no mapped control from knowledge base for credential rotation specifically, CIS 5.2 (Use Unique Passwords), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software)

Compensating: Enumerate all API keys and service account tokens tied to Figure integrations using your secrets manager or, if absent, a grep/search across configuration files and CI/CD pipeline environment variables ('grep -r "figure" /etc/app/ --include="*.env" --include="*.yaml"'). Invalidate each token at the issuing system (your OAuth provider, AWS IAM, or application admin console) and issue new credentials. For email threat hunting if T1566 is later confirmed, parse email gateway logs using 'mxtoolbox' header analysis or manual inspection of 'Received' and 'Reply-To' headers for spoofed Figure-affiliated domains. Block identified sender IPs/domains at the email gateway.

Evidence: Before rotating credentials, document all currently active sessions and tokens associated with Figure-linked accounts — export OAuth token issuance logs, AWS IAM 'ListAccessKeys' output, and application session tables. Capture a snapshot of any email gateway quarantine logs for messages purportedly from Figure Technology Solutions domains in the past 90 days, preserving full headers, to establish a baseline if phishing is later confirmed as the Figure breach vector. This preserves the forensic record of pre-rotation account state.

Step 4: Recovery — After credential rotation, verify no residual unauthorized sessions exist using D3-LAM (Local Account Monitoring). Confirm that access control lists governing data shared with Figure are reset to least privilege per NIST AC-6 (Least Privilege) and CIS 3.3 (Configure Data Access Control Lists). Monitor for follow-on activity consistent with data re-use — credential stuffing, targeted spear-phishing, or synthetic

identity fraud — over the 30 days following containment.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-6 (Least Privilege), NIST AC-12 (Session Termination), NIST AU-12 (Audit Record Generation), CIS 3.3 (Configure Data Access Control Lists), CIS 5.3 (Disable Dormant Accounts)

Compensating: Run 'query session' (Windows) or 'who -a' / 'last' (Linux) on systems that interfaced with Figure to identify any lingering active sessions tied to rotated accounts — terminate any found. Use osquery ('SELECT * FROM logged_in_users;') for cross-platform active session enumeration on endpoints. For the 30-day follow-on monitoring window, configure authentication failure rate alerting using Windows Event ID 4625 (Failed Logon) threshold rules in Windows Event Forwarding (WEF) to a central collector — flag any spike in failed logins on customer-facing or internal accounts whose data may have been exposed, as credential stuffing using exfiltrated Figure data is a realistic follow-on threat given the ~1 million record scope.

Evidence: Before resetting ACLs, export the current permission sets on all data stores (S3 bucket policies, database role grants, filesystem ACLs) that contained data shared with Figure — use 'aws s3api get-bucket-acl' or equivalent — to document pre-recovery state. Capture Windows Event ID 4672 (Special Privileges Assigned) for the credential rotation window to verify no privilege escalation occurred during the gap between breach and rotation. Preserve these records for litigation support given Lynch Carpenter's active investigation into the Figure breach.

Step 5: Post-Incident — Conduct a third-party vendor risk review. Assess whether your vendor onboarding process captures breach notification obligations and data-sharing minimization requirements. Reference NIST AC-20 (Use of External Systems) and CIS 3.2 (Establish and Maintain a Data Inventory) to close gaps in external data exposure visibility. Document findings and update vendor risk register.

NIST Phase: Post Incident

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

Controls: NIST AC-20 (Use of External Systems), NIST AC-1 (Policy And Procedures), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Document findings in a structured vendor risk register (a shared spreadsheet with columns for vendor name, data categories shared, contractual breach notification SLA, last review date, and current risk rating is sufficient for a 2-person team). Cross-reference the Figure breach disclosure against your data inventory to identify which customer or user record categories your organization shared with Figure — PII fields such as names, addresses, SSNs, or financial identifiers are the highest-priority entries to document given the litigation context. Review contracts with Figure Technology Solutions specifically for breach notification clause language, as Lynch Carpenter's investigation may generate subpoenas or regulatory inquiries that require you to demonstrate due diligence.

Evidence: Collect and preserve: (1) all executed data processing agreements or data sharing addenda with Figure Technology Solutions; (2) the inventory of data categories transmitted to Figure (pull from your data classification system or, if absent, query ETL/API logs for field-level data sent to Figure endpoints); (3) your vendor risk assessment scores and any prior security questionnaire responses from Figure. These constitute your documentary evidence of reasonable vendor oversight, which is directly relevant given the active Lynch Carpenter investigation and Figure's pending Kiavi acquisition creating additional regulatory scrutiny.

Detection Guidance

No confirmed IOCs (IPs, domains, hashes) have been publicly released for this incident. Detection should focus on behavioral indicators consistent with the mapped ATT&CK techniques. For T1078 (Valid Accounts): query authentication logs for logins from unfamiliar IPs or geographies on accounts associated with Figure integrations; flag concurrent session anomalies (NIST AC-10). For T1530 (Data from Cloud Storage): review cloud access logs (AWS CloudTrail, Azure Monitor, GCP Audit Logs) for large-volume data reads or exports from storage buckets containing customer PII, especially outside of normal business hours. For T1566

(Phishing): if Figure confirms phishing as the initial vector, search email gateway logs for messages originating from Figure-adjacent domains in the 60-day window preceding public disclosure. CIS 8.2 (Collect Audit Logs) compliance is a prerequisite for all of the above. Organizations without centralized log collection will have limited visibility into whether their environment was secondarily affected. Note: detection confidence is constrained by the absence of confirmed IOCs or a vendor-published attack narrative.

Framework Mappings

MITRE-ATTACK

- **T1530** — Data from Cloud Storage
- **T1078** — Valid Accounts
- **T1566** — Phishing

NIST-800-53R5

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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

HIPAA-SECURITY

- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1530	Data from Cloud Storage	Collection

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
SEC EDGAR Filing Index	https://www.sec.gov/Archives/edgar/data/2064124/000149315226028126/.. .	T1
(consolidated)	https://www.sec.gov/Archives/edgar/data/2064124/000149315226028126/.. .	T1
(consolidated)	https://www.sec.gov/Archives/edgar/data/1278027/000110465926072323/.. .	T1
Figure Technology Solutions Data Breach Claims Investigated by ...	https://lynchcarpenter.com/figure-technology-solutions-data-breach-...	T3
Nearly 1 Million User Records Compromised in Figure Data Breach	https://www.securityweek.com/nearly-1-million-user-records-compromi...	T3

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