INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-15 19:01 UTC

Excelas (Ocelot Ventures) Data Breach Exposes PII, PHI, and Financial Data of Affected Individuals

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0125
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Excelas (Ocelot Ventures, LLC), company systems; affected individuals whose PII, PHI, and financial data was stored
Published	2026-05-13
Discovery Source	Gemini

Executive Summary

Excelas (Ocelot Ventures, LLC), a business services company, disclosed unauthorized access to its systems between November 27 and December 3, 2025, with notification issued in early-to-mid 2026. Compromised data includes full names, dates of birth, Social Security numbers, government-issued ID documents, medical information, and financial account details, a combination that creates significant identity theft and fraud exposure for affected individuals. Multiple law firms have opened class action investigations, signaling probable regulatory scrutiny and litigation costs ahead.

Technical Analysis

An unauthorized actor accessed Excelas company systems during a confirmed window of November 27 through December 3, 2025. The initial access vector has not been publicly confirmed; however, mapped MITRE techniques suggest possible valid account abuse (T1078), cloud storage data access (T1530), and email collection (T1114), with T1486 (data encrypted for impact) as a possible ransomware component, all unconfirmed pending official regulatory filing or vendor statement. Compromised data categories span PII, PHI, and financial account details. No CVE has been assigned; this is an organizational breach rather than a discrete software vulnerability. Applicable CWEs are CWE-284 (Improper Access Control) and CWE-693 (Protection Mechanism Failure). Source quality for technical specifics is medium confidence, primary attribution relies on T3 sources (class action attorneys, breach notification PDF) with no official regulatory filing confirmed as of this writing. Attack vector, affected system architecture, and full scope remain unverified.

Action Checklist

1. Containment, If your organization uses Excelas or Ocelot Ventures services, audit all data-sharing agreements and determine what categories of employee, patient, or client data were transmitted to or processed by Excelas systems. Suspend active data transfers pending breach scope confirmation.
2. Detection, Review outbound data flows and third-party vendor access logs for connections to Excelas or Ocelot Ventures infrastructure during the November 27 to December 3, 2025 window. Cross-reference any shared credential sets or federated access granted to Excelas with your identity provider logs.
3. Eradication, Revoke any API keys, shared credentials, or SSO access granted to Excelas systems. If employee or client PII was shared with Excelas, treat those data sets as compromised and initiate internal notification workflows per your incident response plan.
4. Recovery, Validate that no lateral access pathways from Excelas systems remain active in your environment. Monitor affected individuals' accounts for anomalous activity; coordinate with HR and legal on notification obligations if your organization's data was in scope.
5. Post-Incident, Review third-party vendor risk assessments for all vendors handling PII, PHI, or financial data. This incident highlights gaps in CWE-284 (access control enforcement) and CWE-693 (protection mechanisms) at vendor level. Require breach notification SLA language and data minimization commitments in all vendor contracts.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if your organization's data inventory confirms that employee, client, or patient SSNs, government IDs, medical information, or financial account numbers were transmitted to or processed by Excelas systems during the November 27–December 3, 2025 breach window, as this triggers mandatory breach notification obligations under HIPAA (HHS OCR, 60-day clock), GLBA, and applicable state breach notification statutes, and exposes the organization to class action liability consistent with the litigation already filed against Ocelot Ventures LLC.
Recovery Notes	Post-containment, maintain heightened authentication monitoring on all accounts associated with individuals whose SSNs, DOBs, government IDs, or financial account numbers were within Excelas scope — specifically watch for credential stuffing attempts (Event ID 4625 bursts) and new account creation using compromised identity elements. Given the multi-month notification delay (breach November 2025, notification early-to-mid 2026), assume affected PII has already been circulated in criminal marketplaces and treat downstream identity fraud as an active risk rather than a hypothetical. Continue elevated monitoring for a minimum of 12–18 months post-notification, consistent with the extended fraud window for SSN and government ID exposure, and coordinate with HR and benefits providers to offer credit monitoring services to affected employees if your organization's data was in scope.

Forensic Artifacts	IdP sign-in logs (Azure AD, Okta, AD FS) for Nov 27–Dec 3, 2025: export all authentication events for service accounts, federated identities, and OAuth tokens scoped to Excelas or Ocelot Ventures — these establish whether your credentials were active during the breach window and what data scopes were accessible | Outbound data transfer logs from your email gateway, SFTP server, or secure file exchange platform showing files or data payloads sent to Excelas/Ocelot Ventures addresses or endpoints — cross-reference file names and sizes against known PII/PHI data exports to determine breach scope for notification purposes | Network flow records (NetFlow, IPFIX, or firewall session logs) for connections to Excelas IP ranges during Nov 27–Dec 3, 2025 — preserve immediately as firewall log retention windows (typically 30–90 days) may expire before your investigation is complete, making this evidence irretrievable | Your executed data-sharing agreements and data processing addenda with Excelas/Ocelot Ventures — the gap between contractually permitted data categories and actual data transmitted is a key forensic and legal finding that will determine regulatory exposure and notification scope | DLP policy match history and data classification audit logs for any Excelas-tagged or Excelas-destined data flows — these artifact records establish what categories of sensitive data (SSN-class PII, PHI, financial account numbers) were in the transmission pipeline during and prior to the breach window

Per-Action IR Details

Containment — If your organization uses Excelas or Ocelot Ventures services, audit all data-sharing agreements and determine what categories of employee, patient, or client data were transmitted to or processed by Excelas systems. Suspend active data transfers pending breach scope confirmation.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected third-party data pathways to prevent continued exposure of PII, PHI, and financial data processed by Excelas during the November 27–December 3, 2025 unauthorized access window

Controls: NIST IR-4 (Incident Handling) — implement containment actions consistent with the IR plan for third-party breach scenarios, NIST SA-9 (External System Services) — enforce contractual obligations and security requirements for Excelas as an external service provider, CIS 3.2 (Establish and Maintain a Data Inventory) — use your data inventory to identify which data categories (SSNs, DOBs, medical, financial) were shared with Excelas and are now in scope, CIS 3.3 (Configure Data Access Control Lists) — suspend data access pathways to Excelas systems based on need-to-know reassessment post-breach disclosure

Compensating: Export your DLP or email gateway logs (e.g., Microsoft 365 Compliance Center > Content Search, or Proofpoint archive) filtered for any outbound transfers to excelas.com or ocelotventures.com domains. If no DLP exists, run a PowerShell query against Exchange Online: `Get-MessageTrace -RecipientAddress *@excelas.com -StartDate 2025-11-01 -EndDate 2026-03-04 | Export-Csv ExcelasOutbound.csv`. For file shares, use `robocopy` audit mode or `icacls` to enumerate any shared drives mapped to Excelas endpoints. Block the Excelas IP ranges and domains at your perimeter firewall immediately using a deny-all ACL.

Evidence: Before suspending data transfers, capture: (1) all data-sharing agreement documents referencing Excelas/Ocelot Ventures with data category classifications (PII, PHI, financial); (2) network flow logs (NetFlow/IPFIX) showing outbound connections to Excelas infrastructure during Nov 27–Dec 3, 2025 — preserve these logs in write-protected storage before any firewall rule changes flush connection tables; (3) email and secure file transfer logs showing what files or data payloads were sent to Excelas accounts in the breach window; (4) your own DLP alert history for any Excelas-tagged data classification labels during that period.

Detection — Review outbound data flows and third-party vendor access logs for connections to Excelas or Ocelot Ventures infrastructure during the November 27 to December 3, 2025 window. Cross-reference any shared credential sets or federated access granted to Excelas with your identity provider logs.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate third-party vendor access telemetry and identity provider logs to determine whether your organization's data was within the Excelas breach scope and whether any federated access was abused during the November 27–December 3, 2025 unauthorized access period

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review and analyze IdP and network logs for the specific Nov 27–Dec 3, 2025 Excelas breach window, NIST AU-3 (Content of Audit Records) — ensure IdP and access logs contain sufficient detail (user, timestamp, source IP, resource accessed) to reconstruct Excelas-related access events, NIST SI-4 (System Monitoring) — monitor for anomalous access patterns originating from or destined for Excelas infrastructure during the breach window, CIS 5.1 (Establish and Maintain an Inventory of Accounts) — enumerate all accounts granted federated or shared-credential access to Excelas systems to scope credential compromise risk

Compensating: Query your Azure AD / Okta / AD FS sign-in logs for any service accounts, federated SSO sessions, or OAuth tokens scoped to Excelas during Nov 27–Dec 3, 2025. Azure AD CLI: `az monitor activity-log list --start-time 2025-11-27 --end-time 2025-12-03 | grep -i excelas`. For on-prem AD, run `Get-ADUser -Filter * | Where-Object {$_.Description -like '*Excelas*'}` and cross-reference with Windows Security Event Log Event ID 4648 (explicit credential logon) and Event ID 4624 (successful logon) filtered by accounts associated with Excelas. For network flows without a SIEM, use Zeek (Bro) or Wireshark pcap replay on captured traffic archives filtered by known Excelas IP ranges to reconstruct outbound connection timelines.

Evidence: Preserve before analysis: (1) Azure AD / Okta / AD FS sign-in logs for the Nov 27–Dec 3, 2025 window, specifically filtering on Excelas-affiliated service principals, OAuth app tokens, or SAML assertions — export to immutable storage immediately as retention windows may expire; (2) DNS query logs from your internal resolver showing any lookups for excelas.com or ocelotventures.com subdomains during the breach window; (3) VPN or proxy logs showing authenticated sessions destined for Excelas IP space during Nov 27–Dec 3, 2025; (4) any CASB (Cloud Access Security Broker) alerts flagging anomalous data volume to Excelas endpoints.

Eradication — Revoke any API keys, shared credentials, or SSO access granted to Excelas systems. If employee or client PII was shared with Excelas, treat those data sets as compromised and initiate internal notification workflows per your incident response plan.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove all trust relationships and credential access granted to Excelas from your identity infrastructure, and initiate data-breach notification workflows for PII, PHI, and financial data categories confirmed or suspected to have been processed by Excelas during the breach window

Controls: NIST IR-4 (Incident Handling) — execute eradication actions per the IR plan, including credential revocation and downstream notification workflows, NIST IR-6 (Incident Reporting) — report suspected or confirmed compromise of employee or client PII/PHI to appropriate internal stakeholders and, where applicable, regulators (HIPAA covered entities: HHS OCR; financial data: applicable state AG or FTC), NIST AC-2 (Account Management) — disable or delete all accounts, API keys, and service principals associated with Excelas access, CIS 6.2 (Establish an Access Revoking Process) — execute documented access revocation for all Excelas-associated accounts, tokens, and federated identities, CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) — confirm no Excelas service accounts had elevated privileges in your environment that could enable lateral movement post-compromise

Compensating: Enumerate and revoke Excelas-related API keys using your secrets manager (HashiCorp Vault: `vault lease revoke -prefix `; AWS: `aws iam delete-access-key --access-key-id `). For OAuth tokens in Azure AD, run: `Get-AzureADServicePrincipal | Where-Object {$_.DisplayName -like '*Excelas*'} | Remove-AzureADServicePrincipal`. Rotate any shared passwords immediately using a forced password reset: AD PowerShell `Set-ADAccountPassword -Identity -Reset -NewPassword (ConvertTo-SecureString -AsPlainText '' -Force)`. Document each revocation action with timestamp and actor for regulatory audit evidence (HIPAA, GLBA, state breach notification). Use a spreadsheet or ticketing system as your chain-of-custody log if no GRC platform is available.

Evidence: Before revoking credentials, capture: (1) a full export of all active API keys, OAuth tokens, and service principals associated with Excelas from your identity provider — this establishes scope for downstream notification; (2) last-used timestamps for each credential to determine whether any were actively used during the Nov 27–Dec 3, 2025 breach window; (3) access scope/permission sets attached to each credential (to assess what data Excelas could have accessed through your systems if the credential was compromised at their end); (4) your data classification records showing which PII, PHI, or financial data fields were accessible via those credentials, which directly informs notification

obligation scope under HIPAA, GLBA, or applicable state breach laws.

Recovery — Validate that no lateral access pathways from Excelas systems remain active in your environment. Monitor affected individuals' accounts for anomalous activity; coordinate with HR and legal on notification obligations if your organization's data was in scope.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore and verify the integrity of your access control posture by confirming all Excelas trust relationships are severed, and initiate continuous monitoring of accounts associated with individuals whose PII, PHI, or financial data was processed by Excelas during the breach window

Controls: NIST IR-4 (Incident Handling) — coordinate recovery actions including account monitoring and notification with HR, legal, and affected business units, NIST IR-8 (Incident Response Plan) — invoke the plan's notification and recovery procedures for third-party breach scenarios involving employee or client PII, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — implement heightened audit log review for accounts belonging to individuals whose data was in Excelas scope, targeting anomalous authentication or financial transaction patterns, CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce or verify MFA is active on all accounts associated with affected individuals to reduce fraud risk from SSN and credential-grade PII exposure, CIS 7.2 (Establish and Maintain a Remediation Process) — document and track recovery actions as part of your risk-based remediation process for this vendor breach

Compensating: Run a network scan using nmap to confirm no active connections remain to Excelas IP ranges: `nmap -sn ` from your internal network. Review firewall deny logs post-block to catch any retry attempts. For account monitoring without a SIEM, configure Windows Event Log subscriptions (Event ID 4625 — failed logon, Event ID 4740 — account lockout) on accounts belonging to affected individuals and forward to a central syslog server (even rsyslog on a Linux VM is sufficient). Alert HR and legal with a scoped list of affected individuals using your data inventory cross-referenced against Excelas data-sharing scope — use this list to drive state breach notification letter generation. If HIPAA applies, document the breach in your HIPAA breach log immediately and assess the 60-day HHS OCR notification clock.

Evidence: Before closing recovery: (1) firewall and proxy logs confirming zero active outbound connections to Excelas infrastructure post-revocation — capture a timestamped snapshot as evidence of remediation; (2) IdP audit logs showing all Excelas-associated tokens and service principals are in a disabled/deleted state; (3) a signed attestation from your network/security team confirming no active sessions or tunnels to Excelas systems remain, to satisfy regulatory evidence requirements; (4) the scoped list of affected individuals (name, data categories exposed) derived from your data inventory, preserved for notification obligation documentation under applicable state breach notification laws and, if applicable, HIPAA §164.400–414.

Post-Incident — Review third-party vendor risk assessments for all vendors handling PII, PHI, or financial data. This incident highlights gaps in CWE-284 (access control enforcement) and CWE-693 (protection mechanisms) at vendor level. Require breach notification SLA language and data minimization commitments in all vendor contracts.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct a lessons-learned review specific to third-party vendor access control failures exemplified by the Excelas breach, and update vendor risk assessment and contract templates to mandate breach notification SLAs, data minimization, and access control enforcement requirements

Controls: NIST IR-4 (Incident Handling) — incorporate lessons from the Excelas breach into updated IR procedures for third-party vendor breach scenarios, NIST SA-9 (External System Services) — update external service provider contracts to require breach notification SLAs, data minimization commitments, and access control enforcement aligned with CWE-284 remediation, NIST IR-8 (Incident Response Plan) — revise the IR plan to include a vendor breach notification intake and response workflow, triggered by any data processor disclosing unauthorized access to PII, PHI, or financial data, NIST RA-3 (Risk Assessment) — re-evaluate residual risk for all third-party vendors handling PII, PHI, or financial data in light of the Excelas CWE-284/CWE-693 failure pattern, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — extend your vulnerability management process to include third-party vendor security posture reviews, using questionnaires or attestations that specifically assess access control enforcement and

data protection mechanisms, CIS 3.4 (Enforce Data Retention) — require all PII/PHI vendors to demonstrate contractual data retention and disposal commitments, minimizing breach blast radius for future incidents

Compensating: Build a vendor PII/PHI risk register in a spreadsheet (columns: vendor name, data categories shared, volume of records, breach notification SLA in contract Y/N, data minimization commitment Y/N, last security assessment date, next review date). Prioritize vendors sharing SSN-grade PII or PHI for immediate contract review — the Excelas incident demonstrates that business services vendors with access to this data tier present breach-notification regulatory exposure (HIPAA, GLBA, state laws). Draft a one-page vendor security addendum requiring: (1) 72-hour breach notification to your organization, (2) annual SOC 2 Type II or equivalent attestation, (3) data minimization and deletion-on-contract-termination clauses. Use SANS vendor assessment questionnaire templates (freely available) as a baseline for reassessing your remaining vendor population.

Evidence: For the lessons-learned record: (1) the Excelas breach disclosure notification letter and any supplemental communications from Ocelot Ventures LLC — preserve as the triggering event documentation; (2) your data-sharing agreement with Excelas (or absence thereof) — the gap between what data was shared and what was contractually scoped is a key finding; (3) the output of your vendor risk register audit showing which other vendors share similar data categories without adequate breach notification SLA language — this drives the remediation roadmap; (4) the timeline from Excelas breach occurrence (Nov 27, 2025) to your organization's notification receipt (early-to-mid 2026) — this multi-month gap is the primary evidence for requiring contractual notification SLA improvements.

Detection Guidance

No IOCs (IPs, domains, hashes) have been publicly confirmed for this breach. Detection focus should be on secondary exposure: if your organization shared data with Excelas, treat affected records as potentially compromised. Monitor identity theft indicators for affected individuals, anomalous account creation attempts, new credit inquiries, or SSN-linked fraud alerts. If your organization uses a third-party breach monitoring feed (HaveIBeenPwned enterprise, SpyCloud, or similar), flag Excelas and Ocelot Ventures for watchlist inclusion. Watch for spear-phishing campaigns targeting individuals whose SSNs and medical data are now in threat actor hands, as this data combination is high-value for synthetic identity fraud.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1486** — Data Encrypted for Impact
- **T1530** — Data from Cloud Storage
- **T1114** — Email Collection

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **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.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

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
T1486	Data Encrypted for Impact	Impact
T1530	Data from Cloud Storage	Collection
T1114	Email Collection	Collection

Sources

Source	URL	Tier
Excelas Data Breach Reported, Class Action Lawsuit Possible	https://www.classaction.org/data-breach-lawsuits/excelas-may-2026	T3
Excelas Data Breach Lawsuit - Class Action U	https://classactionu.org/current-data-breaches/excelas/	T3

Source	URL	Tier
Excelas Breach Lawsuit Investigation - Levi & Korsinsky, LLP	https://consumer.zlk.com/data-breach/excelas/	T3
[PDF] Ocelot Ventures, LLC dba Excelas (“Excelas”) Notice of Privacy ...	https://www.classaction.org/media/excelas-data-breach-online-notice...	T3
Excelas Data Breach Investigation - Cole & Van Note	https://colevannote.com/2026/05/13/excelas-data-breach-investigation/	T3

Generated 2026-05-15 19:01 UTC by TJS Security Command Center