INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-14 05:02 UTC

Lucky Lady Casino Discloses Data Breach Exposing Sensitive Personal and Health Information

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0168
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Casino LLC dba Larry Flynt's Lucky Lady Casino, employee and/or customer records
Published	2026-06-11
Discovery Source	Gemini

Executive Summary

Casino LLC dba Larry Flynt's Lucky Lady Casino confirmed that an unauthorized actor accessed its network in May 2025 and exfiltrated sensitive personal and health information belonging to employees and/or customers. Exposed data includes Social Security numbers, passport numbers, driver's license numbers, dates of birth, and health insurance information, categories that create direct identity theft and fraud exposure for affected individuals. The organization disclosed the breach to the California and Maine Attorneys General approximately 13 months after the incident, a timeline that carries significant regulatory risk under California's breach notification statute.

Technical Analysis

The incident involved unauthorized network access and data exfiltration occurring in May 2025, with public disclosure initiated on or around June 10, 2026. No specific attack vector, malware family, or threat actor has been publicly attributed based on available source material. MITRE ATT&CK techniques associated with this incident pattern include T1041 (Exfiltration Over C2 Channel), T1530 (Data from Cloud Storage), T1078 (Valid Accounts), and T1566 (Phishing). Relevant CWEs are CWE-693 (Protection Mechanism Failure), CWE-284 (Improper Access Control), and CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor). Data categories confirmed or potentially exposed: full names, dates of birth, Social Security numbers, driver's license and state ID numbers, passport numbers, and health insurance information. No CVE identifier applies to this disclosure. The 13-month gap between incident detection and notification is the primary compliance exposure; California Civil Code § 1798.82 requires notification in the most expedient time possible. Regulatory

filings were submitted to both the California OAG and the Maine AG, triggering multi-state notification obligations.

Action Checklist

1. Step 1: Containment, If your organization has business relationships, shared vendors, or third-party integrations with Casino LLC dba Larry Flynt's Lucky Lady Casino, identify and isolate any shared network connections or data exchange points immediately. Review third-party access logs for anomalous activity originating from or destined to affiliated infrastructure.
2. Step 2: Detection, If you process similar sensitive data categories (SSNs, health insurance information, passport numbers), audit your SIEM for indicators matching T1078 (Valid Accounts) and T1566 (Phishing) patterns: unexpected privileged account logons, off-hours authentication events, large outbound data transfers. Reference NIST AU-6 for audit record review frequency. Use CIS 8.2 (Collect Audit Logs) to confirm logging coverage across all systems holding PII.
3. Step 3: Eradication, No specific patch or configuration remediation applies to this third-party breach disclosure. For your own environment, enforce access controls per NIST AC-3 (Access Enforcement) and AC-6 (Least Privilege). Verify that health and identity data stores are not accessible to accounts beyond their defined need-to-know scope, per CIS 3.3 (Configure Data Access Control Lists).
4. Step 4: Recovery, If you are Casino LLC dba Larry Flynt's Lucky Lady Casino or a directly affected organization, validate that all unauthorized access paths have been closed and that exfiltrated data categories are mapped to all affected individuals. Confirm notification obligations are met for all applicable state jurisdictions. Monitor for downstream fraud indicators, identity theft reports, suspicious account openings, and establish a credit monitoring or identity protection program for affected individuals per standard breach response practice.
5. Step 5: Post-Incident, This breach exposes gaps in three control areas: incident detection latency (13-month gap indicates delayed identification), data minimization (breadth of exposed data categories suggests over-retention), and notification process readiness. Map remediation actions to NIST IR-6 (Incident Reporting), AU-11 (Audit Record Retention), and CIS 3.4 (Enforce Data Retention). Conduct a tabletop exercise focused on notification timeline obligations under multi-state breach notification laws.

Detection Guidance

No IOCs (IP addresses, domains, file hashes) have been publicly released for this incident based on available source material. For organizations assessing exposure to similar threats, focus detection on the techniques attributed to this incident pattern. For T1078 (Valid Accounts): review authentication logs for logons outside normal business hours, from unfamiliar geographic locations, or using service accounts in interactive sessions. For T1566 (Phishing): review email gateway logs for messages with suspicious attachments or links delivered to HR, payroll, or benefits personnel, roles likely to hold the data categories exposed here. For T1041 (Exfiltration): alert on large outbound data transfers from systems hosting PII or health insurance records, particularly to external IP ranges. Per NIST AU-6, audit records should be reviewed at a defined frequency for indications of inappropriate activity. Per NIST AU-3, ensure audit records capture what event occurred, when, where, the source, the outcome, and the identity of the subject, all required to reconstruct an exfiltration timeline. CIS 8.2 (Collect Audit Logs) should be validated across all systems storing SSNs, health insurance data, and government ID numbers.

Framework Mappings

MITRE-ATTACK

- **T1041** — Exfiltration Over C2 Channel
- **T1530** — Data from Cloud Storage
- **T1078** — Valid Accounts
- **T1566** — Phishing

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **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
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **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
T1041	Exfiltration Over C2 Channel	Exfiltration
T1530	Data from Cloud Storage	Collection
T1078	Valid Accounts	Defense-Evasion
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
Larry Flynt's Lucky Lady Casino Data Breach Lawsuit Investigation	https://www.claimdepot.com/investigations/larry-flynts-lucky-lady-c...	T3
[PDF] By providing this notice, Casino, LLC dba Larry Flynt's Lucky Lady ...	https://www.classaction.org/media/larry-flynts-lucky-lady-casino-da...	T3
[PDF] Casino, LLC dba Larry Flynt's Lucky Lady Casino	https://oag.ca.gov/system/files/Casino%2C%20LLC%20dba%20Larry%20Fly...	T1
Code of Conduct - Larry Flynt's Lucky Lady Casino	https://luckyladyla.com/about-us/code-of-conduct/	T3
Data Breach Notices | Attorney General - Maine.gov	https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a...	T1

Generated 2026-06-14 05:02 UTC by TJS Security Command Center