Post-Incident Review

Unauthorized Access to Customer PII – 28 March 2025

Author: Lydiah Muigwa, Security Engineer
Date: July 30, 2025
Classification: Internal Use

1. Executive Summary

- **Scope**: 50,047 customer records (PII + truncated payment card) exfiltrated via forced-browse on `/receipt?orderId={}`.
- **Timeline**: First ransom email 22 Dec 15:13 PT; confirmed breach 28 Dec 19:20 PT; containment 28 Dec 20:41 PT.
- **Root Cause**: IDOR (CWE-639) on purchase-confirmation endpoint—no server-side authorization check.
- **Severity**: **CVSS 3.1: 7.5 (High)** - AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
- **Financial Impact**: $100k direct cost breakdown: $60k incident response, $25k customer protection, $15k compliance costs; no evidence of downstream fraud as of 30 Jan 2023.
- **Status**: **CLOSED** - Fixed (code + WAF), customers notified, credit monitoring deployed, lessons-learned shared.

2. Timeline (PT)

Date / Time	Event
22 Dec 15:13	Employee receives ransom email demanding $25k BTC; flagged as spam.
28 Dec 19:20	Second email arrives with sample data + $50k demand.
28 Dec 19:25	Security paged; on-call triages.
28 Dec 20:41	Vulnerable endpoint disabled.
29–30 Dec	Log analysis, patch development, WAF rule deployment, customer list finalized.
03 Jan	Public disclosure & customer communications sent.

3. Technical Findings

3.1 Attack Path

1. Attacker enumerated `orderId` sequentially (GET `/receipt?orderId=10000..15000`).
2. No authZ check → server returned full receipt page with PII.
3. Data scraped & exfiltrated; ransom demand followed.

3.2 Log Evidence

```
2022-12-28 19:21:03 GET /receipt?orderId=10001 200 127.0.0.1 42 ms 2022-12-28
19:21:04 GET /receipt?orderId=10002 200 127.0.0.1 38 ms ... 2022-12-28 19:45:12 GET
/receipt?orderId=15000 200 127.0.0.1 40 ms
```

Analysis: 4,999 requests in 24 min, 100% 200 OK responses, user-agent `python-requests/2.28.1`.

3.3 Regulatory Compliance Status

- **GDPR Article 33**: Breach notification submitted to supervisory authority within 72 hours
- **CCPA Section 1798.82**: Individual notifications sent within regulatory timeframe
- **PCI DSS**: Incident reported to acquiring bank and card brands
- **State Breach Laws**: Notifications sent to affected state attorneys general

4. Remediation & Customer Impact

Action	Owner	Status	Completion
Hot-patch to enforce `orderId` ownership check	Engineering	Complete	28 Dec 21:10
WAF rate-limit rule (100 req / 10 min / IP)	SecOps	Complete	28 Dec 21:30
Customer notification + credit monitoring	Communications	Complete	03 Jan
Incident retrospective & RCA documentation	Engineering	Complete	05 Jan

4.1 Lessons Learned

What Worked Well:

- Rapid escalation from employee to security team (5 minutes)
- Quick containment within 1 hour 21 minutes of detection
- Effective coordination between engineering, security, and legal teams
- Comprehensive log analysis capabilities enabled rapid scope determination

Areas for Improvement:

- Initial ransom email should have triggered security review, not spam classification
- Automated anomaly detection could have identified the attack in progress
- Authorization checks should be standard in all endpoint development
- Faster customer notification process needed (72 hours too long)

5. Action Items & Recommendations

Short-term (≤ 30 days)

- **Security Code Review**: Audit all customer-facing endpoints for similar IDOR patterns (Jira-1234) - *Engineering Lead*
- **Automated Testing**: Add mandatory unit tests for authorization on every new endpoint - *DevOps Team*
- **Employee Training**: Security awareness update on identifying extortion emails - *HR/Security*

Medium-term (≤ 90 days)

- **Centralized Authorization**: Deploy centralized authZ library; eliminate inline checks - *Platform Team*
- **Anomaly Detection**: Enable real-time monitoring for unusual access patterns on sensitive endpoints - *SecOps*
- **Incident Response**: Update playbooks to include immediate security review of extortion claims - *Security Team*

Long-term (≤ 180 days)

- **Penetration Testing**: Quarterly external pentest focused on business-logic flaws - *CISO Office*
- **Secure SDLC**: Update development checklist with mandatory threat modeling for PII access - *Engineering*
- **Zero Trust Architecture**: Implement zero-trust principles for all internal applications - *Infrastructure Team*

6. Financial Impact Breakdown

Cost Category	Amount	Description
Incident Response	$60,000	Forensic investigation, legal consultation, emergency engineering resources
Customer Protection	$25,000	Credit monitoring services for 50,047 affected customers (12 months)
Compliance & Regulatory	$15,000	Legal fees, notification costs, potential regulatory fines
Total Direct Costs	**$100,000**	Quantified impact as of report date
Potential Indirect Costs	TBD	Customer churn, reputation impact, business disruption (under assessment)

7. Appendices

A. Raw access logs (secure drive link: internal-security-drive/incident-2022-001/logs/)
B. Patch implementation details (GitHub PR #5678)
C. Customer communication templates (internal-comms/breach-notification-templates/)
D. Regulatory filing confirmations (legal-docs/compliance-filings-2022/)
E. WAF rule configuration (security-configs/waf-rules-v2.1.yaml)

Document Control:
Classification: Internal Use Only
Version: 1.0 Final