FINAL INCIDENT REPORT

Executive Summary:

On December 28, 2022, at 7:20 p.m. PT, our organization encountered a security breach resulting in unauthorized access to customer personal identifiable information (PII) and financial data. Approximately 50,000 customer records were compromised, with an estimated direct cost impact of $100,000 and potential revenue loss. The incident has been fully investigated and resolved.

Timeline:

December 22, 2022, 3:13 p.m. PT: An employee received an email from an external source claiming to have stolen customer data, requesting a $25,000 cryptocurrency payment. The email was dismissed as spam and deleted.

December 28, 2022: The same employee received another email from the same source, now demanding $50,000 and providing a sample of the stolen data.

On the same day, the security team was alerted, initiating an investigation between December 28 and December 31, 2022.

Investigation:

The security team identified the root cause as a vulnerability in the e-commerce web application, enabling a forced browsing attack. Attackers accessed customer transaction data by manipulating order numbers in URL strings of purchase confirmation pages. Thousands of purchase confirmation pages were compromised, leading to data exfiltration.

Response and Remediation:

The organization collaborated with public relations to notify affected customers and offered complimentary identity protection services. Analysis of web server logs revealed a spike in customer orders, pinpointing the source of the attack.

Recommendations:

To prevent future incidents, we propose:

- Regular vulnerability scans and penetration testing.
- Implementation of access control measures:
    - Utilization of allowlisting for specific URL access and automatic blocking of requests beyond defined parameters.
    - Authentication requirements for user access to content.