# **Data Breach Investigation Report**

## **Company Name: ABC SecureBank**

### **Date of Report: 15/08/2024**

### **Prepared By: Sravanthi Chitla**

**Objective:** Investigation of a Data Breach on a Renowned

Website.

## **Executive Summary**

On 15/08/2024, ABC SecureBank discovered a data breach during a routine security audit. The breach potentially exposed sensitive customer information, including names, account numbers, and transaction history. This report outlines the investigation conducted to determine the cause and scope of the breach, the forensic analysis performed, and the strategies developed for data recovery, regulatory compliance, communication, and post-incident review.

## **Incident Analysis**

### **Breach Discovery**

**Date of Discovery:** 15/08/2024

**Method of Discovery:** The breach was identified during a routine security audit conducted by the internal IT security team. Anomalies were detected in the network traffic, indicating unauthorised access to customer data.

### **Point of Entry**

**Analysis:** The investigation revealed that the point of entry was an unsecured API endpoint that was exploited by attackers to gain access to the customer database. The attackers used SQL injection techniques to bypass authentication and extract sensitive data.

### **Extent of Breach**

* **Affected Systems:** The breach primarily affected the customer account management system. Other systems, including transaction processing and internal communications, were not compromised.
* **Timeframe:** The breach is estimated to have occurred over a period of 14 days, from1/08/2024 to 15/08/2024.

## **Forensic Analysis**

### **Digital Forensics**

**Malware Investigation:** A thorough forensic analysis of the affected systems revealed no evidence of malware. However, logs indicated repeated unauthorised access attempts from an external IP address, correlating with the timeframe of the breach.

**Suspicious Activities:** Analysis of server logs showed abnormal activity, including multiple failed login attempts and unusual SQL queries that were executed against the customer database.

### **Evidence Collection**

**Collected Data:** The following evidence was collected for further analysis:

Server logs showing unauthorised access attempts.

Database logs indicating SQL injection attempts.

Network traffic logs highlighting the data exfiltration process.

**Preservation:** All collected evidence was securely stored to maintain integrity for potential legal proceedings.

## **Data Recovery**

### **1. Exposed Data**

**Type of Data:** The breach potentially exposed customer account information, including:

Customer names

Account numbers

Transaction history

**Quantity:** Approximately 50,000 customer records were identified as potentially exposed.

### **2. Data Recovery and Containment**

**Containment Strategy:** The unsecured API endpoint was immediately disabled, and additional security measures were implemented to prevent further access. Affected databases were isolated, and backups were restored to mitigate the impact.

**Recovery Plan:** A comprehensive review of the database was conducted to ensure data integrity. Affected customers' account numbers were reissued, and enhanced monitoring was implemented.

## **Regulatory Compliance**

### **1. Legal Considerations**

**Regulatory Requirements:** ABC SecureBank is subject to stringent financial regulations, including the General Data Protection Regulation (GDPR) and the Gramm-Leach-Bliley Act (GLBA). Compliance with these regulations requires timely reporting of data breaches and protection of customer privacy.

### **2. Reporting Obligations**

**Regulatory Bodies:** The breach was reported to the following regulatory bodies:

[Insert Relevant Financial Authority]

[Insert Data Protection Authority]

**Timeline:** The breach was reported within 72 hours of discovery, in compliance with GDPR requirements.

## **Communication and Notification**

### **1. Affected Customers**

**Notification Strategy:** Affected customers were notified via email and postal mail, informing them of the breach, the nature of the exposed data, and steps being taken to protect their accounts.

**Support:** A dedicated hotline and website were established to provide customers with information and assistance.

### **2. Stakeholders and Public**

**Internal Communication:** Key stakeholders, including executives and board members, were briefed on the breach and the ongoing investigation.

**Public Communication:** A press release was issued to address the breach, emphasising the steps being taken to protect customer data and enhance security measures.

## **Post-Incident Review**

### **1. Security Weaknesses**

**Identified Weaknesses:** The review identified several weaknesses in ABC SecureBank's security posture, including:

Unsecured API endpoints

Inadequate input validation and sanitization

Lack of real-time intrusion detection and prevention systems

### **2. Recommendations**

**Immediate Actions:**

Secure all API endpoints with proper authentication and encryption.

Implement real-time monitoring and alerting for suspicious activities.

Conduct regular penetration testing to identify vulnerabilities.

**Long-term Actions:**

Enhance employee training on cybersecurity best practices.

Review and update incident response procedures.

Invest in advanced threat detection technologies.

## **Conclusion**

The data breach at ABC SecureBank was a significant incident that exposed sensitive customer information. However, through prompt detection, thorough investigation, and swift containment measures, the impact was minimised. This incident underscores the importance of maintaining a robust security posture and being prepared to respond effectively to potential breaches. The recommendations provided in this report will help strengthen ABC SecureBank's defences against future threats.