**Incident handler's journal**

**Instructions**

| **Date:** December 28, 2022 | **Entry: 3** | | |
| --- | --- | --- | --- |
| Description: | An unauthorized individual accessed the personal and financial data of 50,000 customers. The estimated financial impact is $100,000. The incident has been resolved after a thorough investigation. | | |
| Tool(s) used | List any cybersecurity tools that were used. | | |
| The 5 W's | * **Who** caused the incident?   By an indivual who sent email from external source   * **What** happened?   individual was able to gain unauthorized access to customer personal  identifiable information (PII) and financial information.   * **When** did the incident occur?   Decmeber22-28th,2022   * **Where** did the incident happen?   Online   * **Why** did the incident happen?   Because of vulnerability in the Web | | |
| Additional notes | The company implemented regular vulnerability scans and penetration testing along with access control mechanism | | |