1 Executive Security Assessment Report

1.1 Overview of the Assessment

A comprehensive security assessment was conducted on the domain **ch-ca-s-udp1.fiservmobileapps.com**. The analysis was initiated on **April 28th at 18:00** and completed in a duration of **00h:05m:11s**. The assessment, identified by tracking ID **148b5e3eff97**, was performed using a Basic scan type. The evaluation focused on identifying High and Medium-risk issues, employing OWASP and OSCP methodologies to ensure a thorough examination of the web application and infrastructure.

1.2 Summary of Key Findings

The recent security assessment revealed no High, Medium, or Low-risk issues, with **three** informational findings. Notably, all scanned ports (**11** in total) were filtered, indicating robust perimeter security controls such as firewalls and IPS/IDS systems. This suggests a strong defense against unauthorized access and reconnaissance attempts. Additionally, the analysis confirmed that the infrastructure is dedicated, with no shared hosting risks detected, enhancing data isolation and security. The geographic distribution analysis showed all servers are located in the United States, with no presence in high-risk locations, minimizing geopolitical risks. These findings underscore a well-secured environment, though continued vigilance and manual verification are recommended to ensure ongoing protection.

1.3 Key Security Issues

Title	Risk
No High or Medium Risk Issues	N/A

1.4 Detailed Findings

1.4.1 Description

The security assessment did not identify any High or Medium-risk issues. The infrastructure demonstrated strong security measures, including filtered ports and dedicated hosting environments. These findings indicate effective implementation of security controls that mitigate potential threats and vulnerabilities.

1.4.2 Affected Assets

- Domain: **ch-ca-s-udp1.fiservmobileapps.com**
- Total Scanned Ports: **11** (All filtered)

1.4.3 Recommendations

While no High or Medium-risk issues were identified, it is recommended to maintain current security practices and continue regular security assessments. Implementing continuous monitoring and periodic manual verification can further enhance the security posture. Additionally, staying informed about emerging threats and updating security protocols accordingly will help in maintaining a resilient defense against potential cyber threats.

1.5 General Recommendation

To ensure ongoing protection and resilience against evolving threats, it is advised to conduct regular security assessments and audits. Continuous monitoring of network traffic and system activities should be implemented to detect anomalies promptly. Furthermore, fostering a culture of security awareness among employees can significantly contribute to minimizing human-related risks.