Name **Date Submitted:**

Course and Section:

CASE STUDY

IT 412 – PLATFORM TECHNOLOGIES

Case Scenario #1: Organized Breach of Certain GCash Accounts

The Cybercrime Investigation and Coordinating Center (CICC) said on Monday, November 11, that it is investigating the possibility of an "organized breach of certain GCash accounts." The suspected breach is being seen as a possible cause for unauthorized fund transfers reported over the weekend. The CICC's Inter-Agency Response Center hotline has received 21 complaints so far involving alleged unauthorized fund transfers. Among those claiming to have lost money is the comedian Pokwang, who claimed that she lost P85,000 from her GCash account.

GCash, as one of the leading mobile payment platforms in the Philippines, in the past few months had a significant security breach that compromised the data of millions of users. This incident began when several users reported suspicious transactions, such as unauthorized fund transfers and fraudulent purchases. It was confirmed that the breach is the result of a highly sophisticated phishing efforts targeting users through their personal email and SMS, and deceiving them into providing login credentials. Once accessed, the attackers exploited flaws in the platform's authentication mechanism to bypass certain security processes, allowing them to make transactions without notifying users immediately.

Following the attack, GCash conducted an emergency downtime to resolve the vulnerability, however the approach was criticized for a lack of communication and openness, resulting in a loss of confidence among its clients. GCash claims to have strengthened its security by improving two-factor authentication (2FA) and investing in user education on phishing. Despite these precautions, there are still worries regarding the platform's general security architecture and the vulnerability of users' financial information.

Your Task:

As part of academic analysis, your task is to understand the breach and evaluate the vulnerabilities in the platform's security. You will analyze the security protocols implemented by GCash, evaluate the risks linked to these platforms, and suggest additional enhancements for platform durability.

Guide Questions for Case Analysis:

1. In what ways does multi-factor authentication (MFA) strengthen security on services such as GCash, and what further enhancements could be implemented to reduce phishing attacks more efficiently?
2. What possible vulnerabilities in GCash's authentication system might have enabled attackers to circumvent specific security measures? In what ways can these vulnerabilities be strengthened?
3. What are the essential principles of secure platform architecture that GCash ought to adhere to in order to reduce vulnerabilities? Explain how these principles are relevant to the mobile payment platform.
4. What are the consequences of poor communication with users after a security breach, and what best practices can GCash use for incident response communication?
5. Based on this scenario, offer a technique that GCash might employ to regain and restore user trust in the platform following a big breach.