**Assignment - 1 The Problem**

**School of professional studies**

[**Masters Research Project - 07 (Spring 2025)**](https://canvas.slu.edu/courses/70893)

**Professor: Dr.** [**Annamaria Szakonyi**](https://canvas.slu.edu/courses/70893/users/1379)

**Due Date: January 28th, 2025**



**Team 6**

**Group Members:**

**Amith Pitta**

**Lila Venkata Sairam Rayala**

**Mohanram Shrinivasan**

**Sai Ganesh Rao Patike Eranna**

* **Samyuktha Rani Pulagam**

**Problem Statement: Ally Financial Inc. Enhancing Security and Customer Trust**

One of the top providers of financial services, Ally Financial Inc. provides investment products, mortgages, auto loans, and banking. In order to achieve client needs, the company offers trusted, user-friendly online platforms and maintains a high priority on protecting customer data. Customers depend on Ally to protect the details of their finances, therefore offering secure services is necessary for establishing trust and maintaining pleasure. Interestingly, the usage of phone numbers as a required second factor for multi-factor authentication (MFA) has pushed Ally to be faced with rising concern. Because of issues including spoofing, phishing, and SIM-swapping, this mode of operation is recognized as unsecure. Consumers think it's out of date, which makes them doubt Ally's security system as a whole and makes some of them think about cutting off their accounts (Ally Financial, n.d.).

Security threats occur when phone numbers are used for authentication because hackers are able to figure out how to get into client accounts without authorization (DiNardi G, 2023). Customers may worry about fraud or identity theft and feel insecure if sensitive financial information is misused. They may become worried of using Ally's services as a result of this and lose faith in the system. Improving security techniques is crucial to protecting consumer data as online threats keep growing. To prevent unwanted access and safeguard client accounts, identity verification should be strengthened, fraud detection should be improved, and security responses should be fast (Martinez J, 2024).

As the first step to increase security, we are creating a Time-Based One-Time Password (TOTP) mechanism to address this issue. By generating short term security codes, TOTP lowers risks associated with utilizing phone numbers for verification and makes authentication safer. But this is just the first step. To improve account security, we would like to implement Push-Based authentication, biometric authentication, and AI-powered fraud detection in the future. In order to protect from future online threats, we also want to implement risk-based authentication and highly advanced security solutions. Customers will feel more confident knowing that their information is secure due to these upgrades, which will encourage the development of an effective, reliable, and secure future financial system (Arent B, 2024).

**References**

Ally Financial. (n.d.). *Banking, investing, home Loans & Auto Finance | Ally*. <https://www.ally.com/>

DiNardi, G. (2023, August 11). *What can hackers do with your phone number?* <https://www.aura.com/learn/what-can-hackers-do-with-your-phone-number>

Martinez, J. (2024, September 30). *11 common authentication vulnerabilities you need to know. StrongDM*. <https://www.strongdm.com/blog/authentication-vulnerabilities>

Arent, B. (2024, August 1). *What is Time-Based One-Time Password & How it Works*. Teleport. <https://goteleport.com/learn/totp-time-based-one-time-password/>