### **Team Deliverable C**

Introduction

The objective of this deliverable is to define a list of prioritized design criteria, do technical/user benchmarking, and determine target specifications that can be used in the development of the final solution.

**List of User Needs (taken from Team Deliverable IB):**

1. Detect SIM swap (if UEID and SIM do not match)
2. Implement an alert mechanism to notify the enterprise of a detected swap
3. Have administrative access to accept SIM swap(s)
4. Locate UE and SIM swap
5. Have the ability to reduce network/device bandwidth

**This week’s tasks:**

1. Technical benchmarking (2 days)

* Nava

In charge of researching similar products that already satisfy interpreted client needs.

1. User benchmarking (Wednesday, Thursday; 2 days)

* Abby

In charge of obtaining user perceptions of similar products

1. Target specifications (Tuesday, Wednesday, Thursday; 3 days)

* Neyssa

In charge of obtaining design specifications with ideal measurable design criteria

1. Reflection on client meeting (Saturday; 1 day)

* Gill

In charge of going over the document and writing the reflection on how the client meeting impacted the development of the design criteria and specifications at the end of the document

1. Update the Trello board (Saturday; 1 day)

* Aadi

In charge of updating the Trello board with updates on task responsibilities, task durations and missing tasks

# User Benchmarking

McAfee Security: Privacy & VPN

* Customer rating: 4.6 stars
  + 12k reviews
  + #75 in Utilities on Apple Store
* “Can you make it so it scans every hour or make it so you can set every time it scans and then send a notification saying the scan detected something or not”
* “Why do you have to pay for more services? I don’t think it’s worth paying”
* “Want to get any information you have to enter a code from an email…. just plain sucks”
* “Subscription price is high”
* “Unreliable”
* “Untrustworthy”
* “This app keeps me from connecting to cellular data”
* “Blocked internet completely”

Google Authenticator

* Customer rating: 4.8 stars
  + 89k reviews
  + #7 in Utilities on Apple Store
* “Is consistent”
* “Wish it had an apple watch function”
* “Extremely safe guard”
* Trouble with backing up and using it on new phones
* “Simple”
* Set up takes a while
* “Love the way everything is integrated”
* “Simple, quick and straightforward”

Microsoft Authenticator

* Customer rating: 4.7 stars
  + 69k reviews
  + #3 in Productivity on Apple Store
* “Microsoft offers no support”
* “Abusively strict”
* “Switched phones and it basically logged me out of everything”
* School IT services had to help reset it multiple times
* Red notification badge on icon won’t go away
* “Backup feature is a lifesaver”

Truecaller: Caller ID & Block

* Customer rating: 4.3 stars
  + 19k reviews
  + #44 in Utilities on Apple Store
* “AI assistant never worked at all… no one ever communicated back to me”
* “Fools people into subscribing for a membership by telling them that it is a free trial”
* “Doesn’t stop any spam calls”

## Summary

The benchmark analysis of these applications reveals a variety of strengths and weaknesses across the board. McAfee Security struggles with perceived value and reliability, while Google Authenticator stands out for its consistent performance and user satisfaction. Microsoft Authenticator presents support and usability challenges but is well-received for its backup feature. Truecaller faces significant criticism regarding its spam-blocking capabilities and subscription practices.

## Recommendations

* Improve scan frequency
* Reduce subscription value
* Improve reliability
* Consistency in performance
* Improve customer support
* Address device transition issues
* Improving spam detection

# Technical Benchmarking

**Rough notes on existing applications**

* NOTE: We will be using Shabodi’s APIs and cannot alter them. However, comparisons are made to existing APIs as a method of seeing what additional features can be integrated into the code that we will be responsible for.
* [Microsoft Authenticator](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-authenticator-app)
* User needs seen in this program: detection of login, alert mechanism, administrative access to accept/deny requests
* Microsoft using two-factor authentication and an OTP prompt sent directly to a user’s phone
  + Passkeys are made available for BYOD (bring your own device) and MDM (mobile device management)
* Passkey generation
  + On iOS → Secure Enclave
  + On Android → Secure Element or Trusted Execution Environment (TEE)
* Takes place of login on devices for users who have enabled Authenticator
  + Ie. you will see a prompt to authenticate with an OTP instead of re-entry of your password
* The mobile app installed on a device will alert a user of a login
* [AMBER Alert XML Draft Standard](https://amberalert.ojp.gov/sites/g/files/xyckuh201/files/media/document/xmlstandards.pdf)
* User needs seen in this program: alert mechanism, interoperability, network/enterprise programming
* Current technology range of the program:
  + Satellite, wireless, web, e-mail, etc.
* Enterprise benefit → responds to both vertical (takeover) and horizontal (acquisition) integration
* Allows both legacy and developing network systems to cooperate with the program
* Public → use available to solutions, public, and government
* XML → eXtensible Markup Language based on SGML and W3C (not a programming language)
  + Describes information and defines its processing
  + Uses HTML-esque tags and attributes
  + Interpretation of data is left to the application unlike in HTML where tags and attributes are defined
  + Allows web-based apps to share information regardless of the language (ie. Java, C++, etc.) → vendor-neutral
* Configures to more than one device type
  + Websites, phones, etc.
* Works under constraints → ie. alerts must be for children, not adults
* [AWARE Biometrics Program](https://www.aware.com/resource/combating-sim-card-fraud-with-biometrics/)
* User needs seen in this program: detection of login, alert mechanism, locating login
* Use biometric verification in place of an OTP or two-factor authentication
  + Face, voice, irises, etc. with use of a camera/microphone or other pre-approved input device
  + Using modern liveness detection to avoid pre-recorded information.

## Summary and Recommendations

Based on a technical comparison of similar and pre-existing products, the integration of an alert mechanism, secure login detection, and biometric authentication would be beneficial for Shabodi's SIM detection software. Using device-specific security features like iOS's Secure Enclave and Android's Trusted Execution Environment (TEE) could enhance passkey generation and secure user authentication and slowly move away from two-factor authentication. Interoperability should also be prioritized to ensure seamless integration across various networks and device types with a focus of use on a 5G network.

# Target Specifications

Reduction of bandwidth during sim swap/fraud

* Bandwidth speeds of lower than 25 Mbps to reduce data loss on the network.

<https://lightyear.ai/blogs/internet-speed-vs-bandwidth>

Authentication

* Strength : High level of confidence in the identity of the user (we want to remove two-factor authentication but keep the security aspect.)
* Usability : authentication methods are user-friendly

Price

* Free for enterprises to use

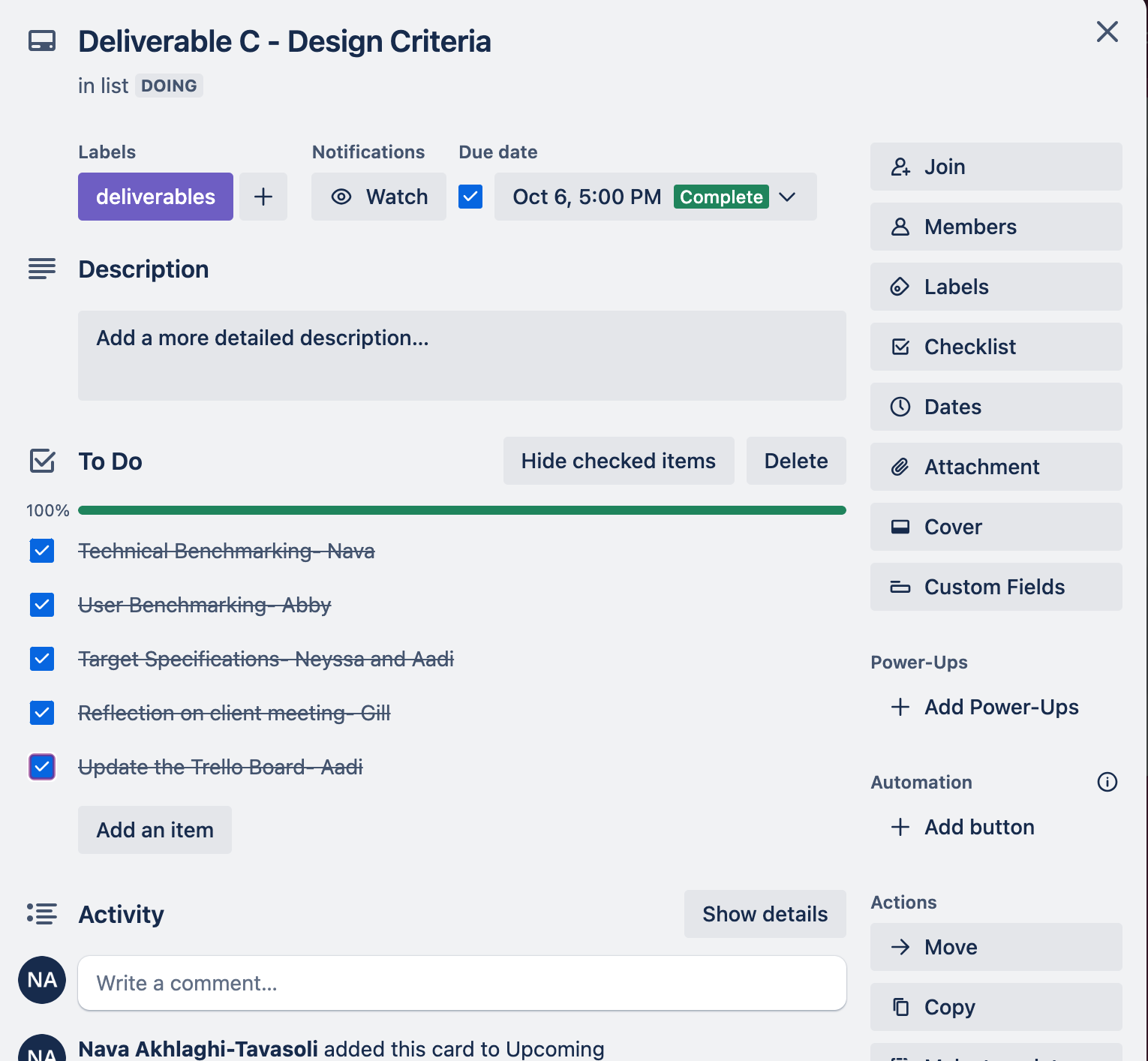
Application accessibility

* Responsive design: adapts to different screen sizes and orientations
* Shabodi has mentioned that they are not as focused on the UX aspect of the project, so less emphasis can be placed on it

Alert mechanism

* Understandability : Text is clear, alerts are easy to understand.
* Accessibility : Reader-friendly text, sufficient contrast between the background and text, alerts are navigable by keyboard.
* Actionability : provide clear instructions on which actions the reader should take in response to the alert. Ideally Reducing network bandwidth so that new devices cannot be added to the network and further preventing huge data loss or allowing the sim swap if it was approved.
* Clarity : Provides clear and concise language on information on the location of the sim swap and
* User notifications : app alert on swap/fraud location, device information, and user history.

# Updates to the Trello Board



# 

# 

# 

# 

# 

# Reflection

The client meeting with Shabodi clarified the project’s direction. The project requirements and their relative importance were also properly established. The user needs (according to Shabodi) were defined, and translated into criteria, distinctly presenting the main constraints. In deliverable B, we had established several unknown factors which were later clarified through interaction with Shabodi. For example, the following point was put forward and elucidated: one goal would be to get rid of or at least mitigate the use of OTP (one time passwords) and two-factor authentication. The meeting revealed a stronger preference for functionality over an aesthetic user interface (UI). A strong focus was to be put on connectivity to their network able users to communicate their APIs.The client also expressed a need for a flexible and scalable design, mainly working with technical enterprises on a business-to-business level and less individual users. Operation on a 5G network would be prioritized for this project given the connected nature of the application.

# Conclusion

As the development of our SIM Swap detection system for Shabodi begins, our priority will be to focus on using what we have analyzed based on user and technical benchmarking in accordance with their listed needs in order to develop a functional application. We will consider the APIs that they already have available and make sure that our code is functional with them. The UI/UX aspect of the program will be less of a priority given Shabodi’s primary focus is on functionality in 5G networks, connectivity, and reducing network bandwidth during potential SIM fraud events. Over time, and as the programming portion of the development begins for this project, our team will refer to this Deliverable in order to ensure that our priorities remain aligned with Shabodi’s needs based on what we have listed in this document so that our product meets their expectations.