A population that could be harmed by this app are business owners, brands, designers, and artists. Unauthorized use of branded logos and images could damage a brand's identity and reputation if they are associated with low-quality services. Similarly, if artistic work is used without permission, graphic designers and artists may lose potential revenue from licensing or selling their designs. These entities have the rights to pursue legal actions, which lead to costly lawsuits for everyone involved including the developers of the mobile business card application, hurting the product and lowering public interest in the app. As a result, app developers and other users might also be harmed in the process. Additionally, Intellectual Property theft could result in confusion among consumers/users of the app, who may mistake scams/frauds for legitimate service providers. Individuals looking to showcase their design skills with a customized business card may be also harmed if the customizability of the business cards is limited.

Another population that could be harmed are students and job-seekers, or just anyone attending networking events. If there are integrity issues with the data shared through the app, such as incorrect academic achievements or misleading/false professional information, it could harm their credibility and opportunities. Additionally, if a business card is accidentally sent to the wrong person, then that recipient will hold personal information about the sender that the sender cannot retract. They also have to trust that the recipient will not pass along or sell their information. There is also a high security risk with storing confidential information such as full names, emails, phone numbers, etc. If there were to be a data leak from the app it could harm all users by letting their personal information be exposed and stolen. Another thing to consider is that networking events can gather people from all over the globe. This means that the app would have to adhere to international data regulations, such as the GDPR, if they are holding personal data from citizens of different countries. If not, the founders could be penalized for that. A misuse of NFC, Bluetooth, or a spoofed QR code can also pose a security risk. For example, when sharing files through NFC or Bluetooth, it is difficult to verify what the shared file is before the recipient agrees to receive the file. As a result, people might accidentally be receiving malware or inappropriate content disguised as a business card in the app.

Individuals with limited internet access face potential exclusion from the digital networking opportunities offered by the app. In areas or among demographics where reliable internet connectivity is a challenge, these individuals may find it difficult to use the app, hindering their ability to engage in professional networking.

Elderly users who may not be familiar with or comfortable using digital tools, and users with visual impairments or other differing abilities that limit the use of the technology may face exclusion from the digital networking opportunities offered by the app, as well as being placed at a further disadvantage in terms of networking ability in situations where the application is the primary form of business-card networking such as at events, conferences, trade shows, and meetings. Users who have difficulty using the application may also become more vulnerable in these situations to those using the app with malicious intent (see above), or may be more likely

to fall victim to unauthorized use of branding and logos due to being uninformed or unaware of the risk.