Appendix I

<u>Initial Client Interview Transcript</u>

Me: You are reusing passwords, so they probably just found your email password and then used it to access all your other accounts.

Mother: That's likely what happened; it's hard to remember every password, so I just used one.

Me: Was it a good one?

Mother: It wasn't a bad password. It could have been better if I didn't have to remember it.

Me: Trying to remember strong and unique passwords doesn't work well, Mom… That's a lot to remember.

Mother: Yes, I agree.

Me: Have you tried a password manager?

Mother: No, no, I have not.

Me: That probably is the best route to take. I want to look into it more because most password managers are online, and some have even been hacked recently. The ones that are offline are really complex, and I don't think that it's something you would be able to stick with using.

Mother: Well, what would I use then? What's wrong with the online ones? I don't want to write them down because someone can just take the list.

Me: They store your passwords in a central location on a server, which means they could be compromised. They also need an internet connection, which can be a problem. There can be third-party breaches as well, which I believe is what happened with LastPass.

Mother: Oh yes, that's not good. Having my passwords at work and on my laptop would be nice. How about a file on a USB?

Me: That's a good idea. How about I make you your own password manager? It would be a fun project, and you could be my client!

Mother: If you'd like to do that, I'd be more than happy to!

Me: I think the main focus should be to get rid of any stress that comes with managing your passwords.

Mother: Yes, and to prevent future attacks, of course.

Me: What I could do is have an encrypted file and an easy-to-use interface that retrieves the information for you. And then, you could add to it, and you would have the ability to generate random password strings that are extremely strong.

Mother: That sounds like exactly what I need. Are you sure you will be able to make it?

Me: It will be a fun challenge, and it'll be better than nothing, which is what you have right now. I think it would be a good idea to go over some requirements beforehand, though.

Mother: Sure, I really appreciate it. I'm still feeling overwhelmed and want to make sure something like that never happens again.

Me: Of course, Mom. That's why I'm here. Let's discuss what we want this password manager to do and what features we need.

Mother: Well, I want to feel secure. And I also want it to be easy to use. I'm not the most tech-savvy person out there.

Me: Absolutely. So let's start with security. I propose we have a master password that you will need to enter to access the password manager. We can also limit the number of attempts to enter the wrong password, so someone can't just keep guessing until they get in.

Mother: That sounds like a good idea. And what about the actual passwords for my accounts?

Me: Like I said before, we can generate strong, randomized passwords. And we can also set a renewal period for the passwords, so you'll get a reminder to update them.

Mother: That's perfect. And I also want to be able to see all of my accounts in one place and easily add or remove them.

Me: Not a problem. I can retrieve the account list from an XML file and display it in the main menu. And I can also make it so you can search for specific accounts.

Mother: That's great.

Me: And I'll also make sure that the data is secure and encrypted. I'll look into some encryption techniques.

Mother: I really appreciate this, and I can't wait to start using it. I do need a quick solution, so maybe give me an early version to use for a bit - that way, I can give you feedback on it as well.
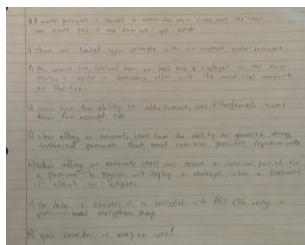
[Later] **Me:** Okay, I've drafted some success criteria. I'll talk with my CS teacher to get his approval as well.

Mother: I like it. Good idea to have the most used accounts at the top.

Me: Awesome! I'll get started and keep you updated on the development!