Threat Model:
Online Banking with
Oregon Community Credit Union

Money is secured.

For the customer the money is secured.

From anyone or anything that is not the customer or bank, the money is secured.

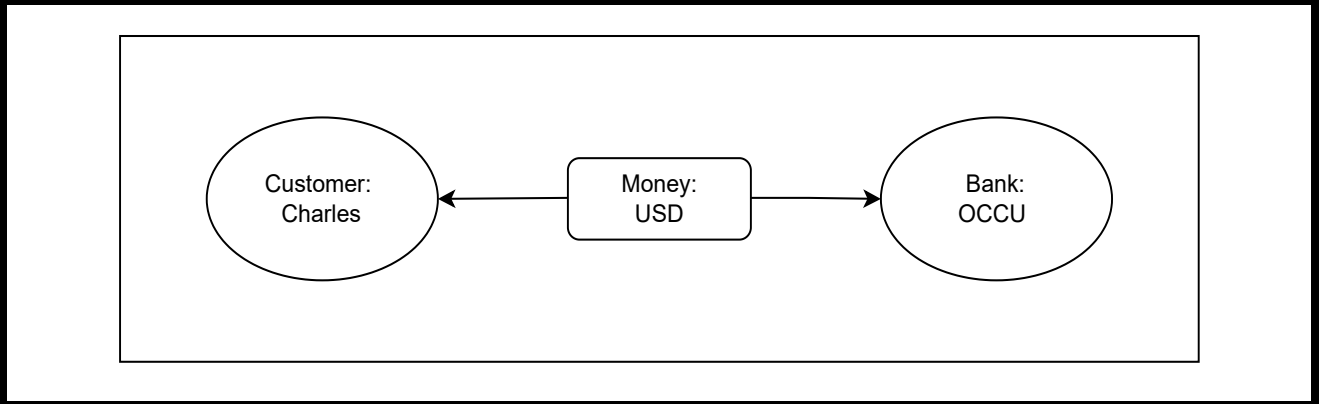
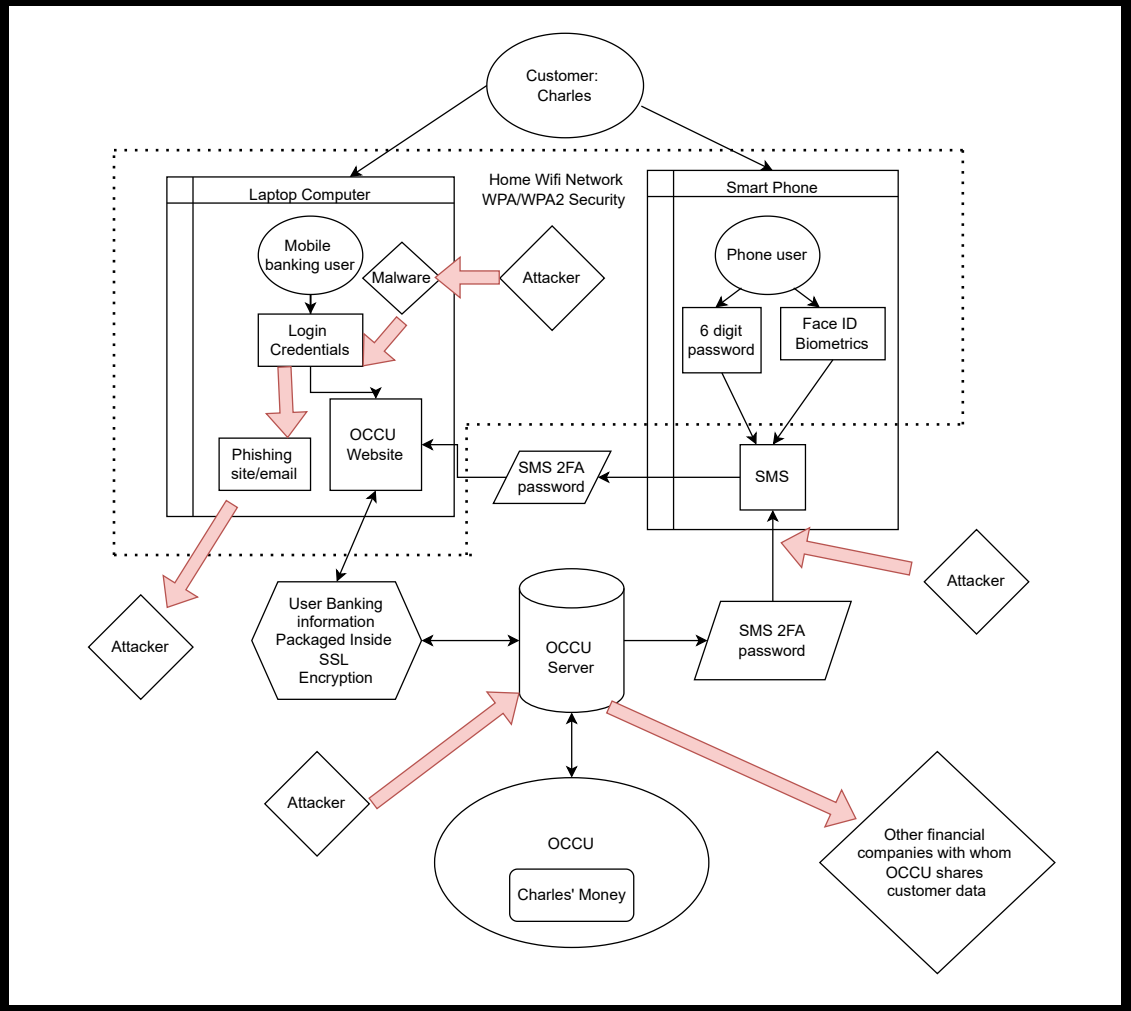


DIAGRAM: Signing in to OCCU website to access money



THREATS: what could go wrong?

- Someone gains access to my OCCU online banking account through my username, password, and 2FA code.
  - They could collect my OCCU username and password through a keylogger installed on my computer.
  - I could mistakenly enter my username and password on a phishing site.
  - 2FA via email, voicemail, or SMS could code could be intercepted.
- An attack on the OCCU data store provides access to my account number, which could be used to withdraw my funds.

LIMITATIONS

- Why are we *still* using SMS as a method of transmitting one-time passwords?
- Is my home wifi network secure? How many users have access it it?
  - WPA2 security is outdated
- OCCU shares my information “for joint marketing with other financial companies” (OCCU Privacy Policy)
  - With my personal and financial data freely shared across banks, if any of their security systems are compromised, my data is unprotected.

ADDRESSING LIMITATIONS

- Home network:
  - Upgrade router to WPA3
  - Limit network connection to only devices of residents
- SMS:
  - Create a ProtonMail email address used exclusively for receiving 2FA codes.
    - This would decrease my sensitive data being transmitted between devices.