



F-Secure Corp

Cybersecurity mobile app foundation for AT&T

F-Secure Corp. (HEL:FSECURE) operates in the cybersecurity space, providing solutions that protect consumers from threats such as identity theft, fraud, and data breaches.

Overview & Challenge

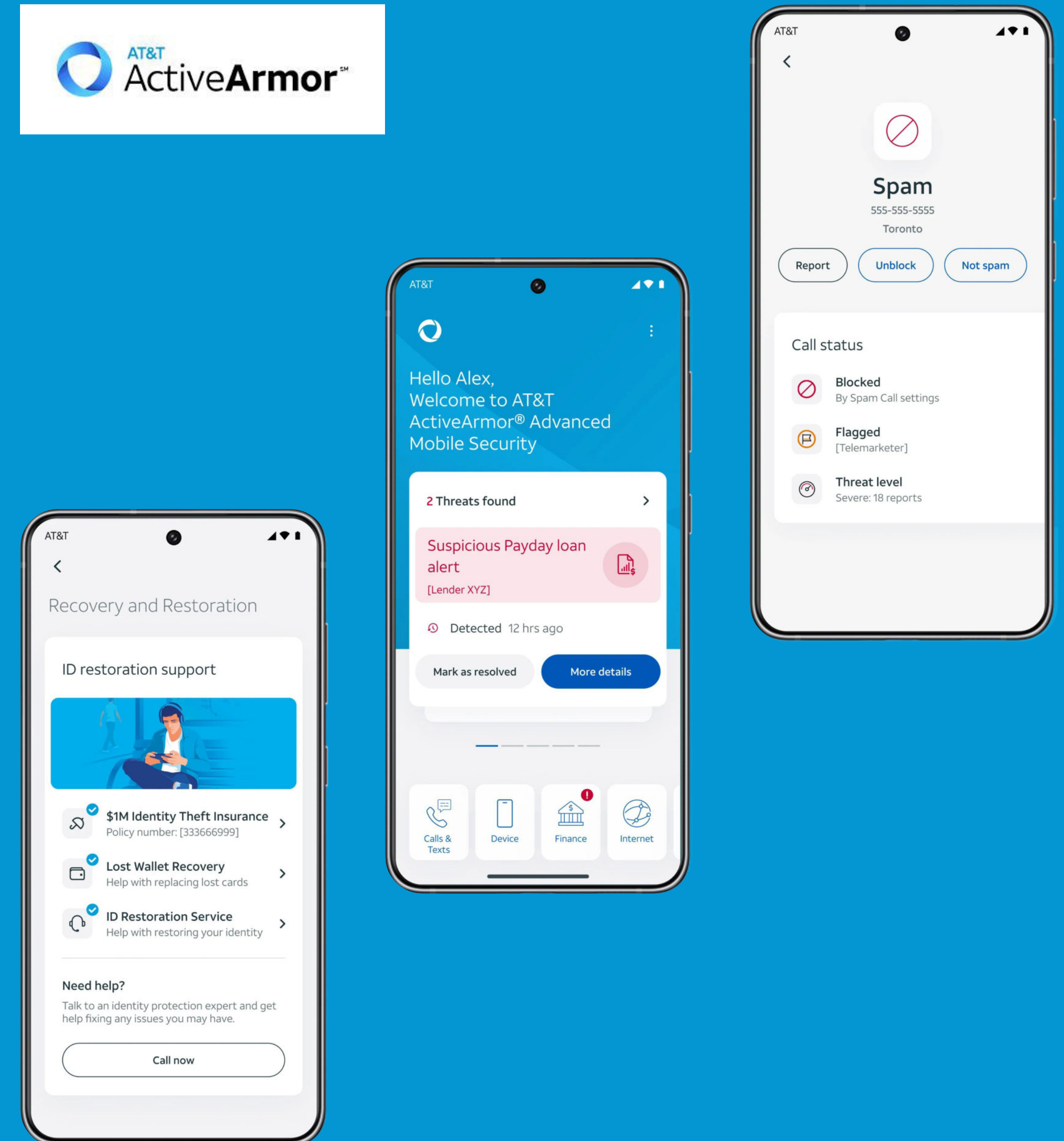
Overview

In 2023, F-Secure concluded the acquisition of LookoutLife, a US B2C unit part of Lookout, specializing in B2B solutions.

LookoutLife was working on a new (0→1) cybersecurity mobile app for **AT&T**'s customers following an established partnership.

I joined the LookoutLife product team to lead UX strategy and research efforts.

This case study focuses on a multi-phase research program that explored how consumers understand and respond to digital security risks; and how those insights shaped product direction.



Challenge

Consumers face increasing digital threats, yet many existing security tools often fail to support them at critical moments. From early exploration, we identified gaps:

- Users receive alerts, but struggle to interpret and act on them
- Users have a security breach, but don't know how to rectify the issue

Key challenges included:

- Unclear understanding of user priorities in digital security
- Limited visibility into how users interpret threats
- Lack of validated insights across global markets
- Uncertainty around what product experience would provide real value

This created a strategic question: *Which problems are critical enough to justify building a product around?*

Additional Context

For context, this project explored the viability of a consumer digital security mobile app by translating research insights into a validated product concept. In a nutshell, the project scope covered:

- Exploratory research
- Concept development
- Usability validation
- Iterative refinement

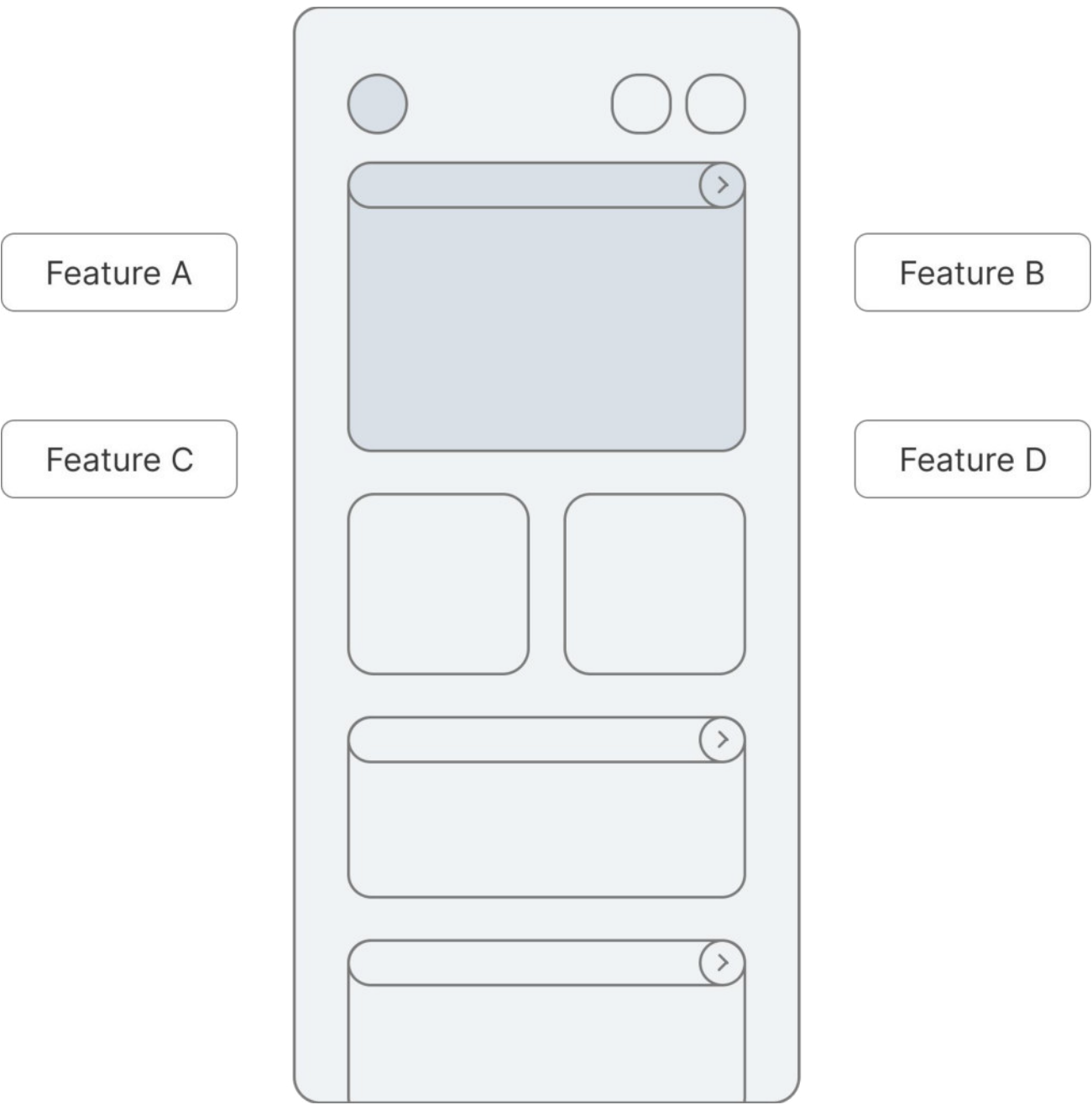
The outcome was a high-fidelity, user-validated concept that defined key features and flows based on user needs.

The final deliverables and evaluative insights were utilized by AT&T as a foundation to build **AT&T ActiveArmor®**, a mobile security app powered by F-Secure's proprietary technology.

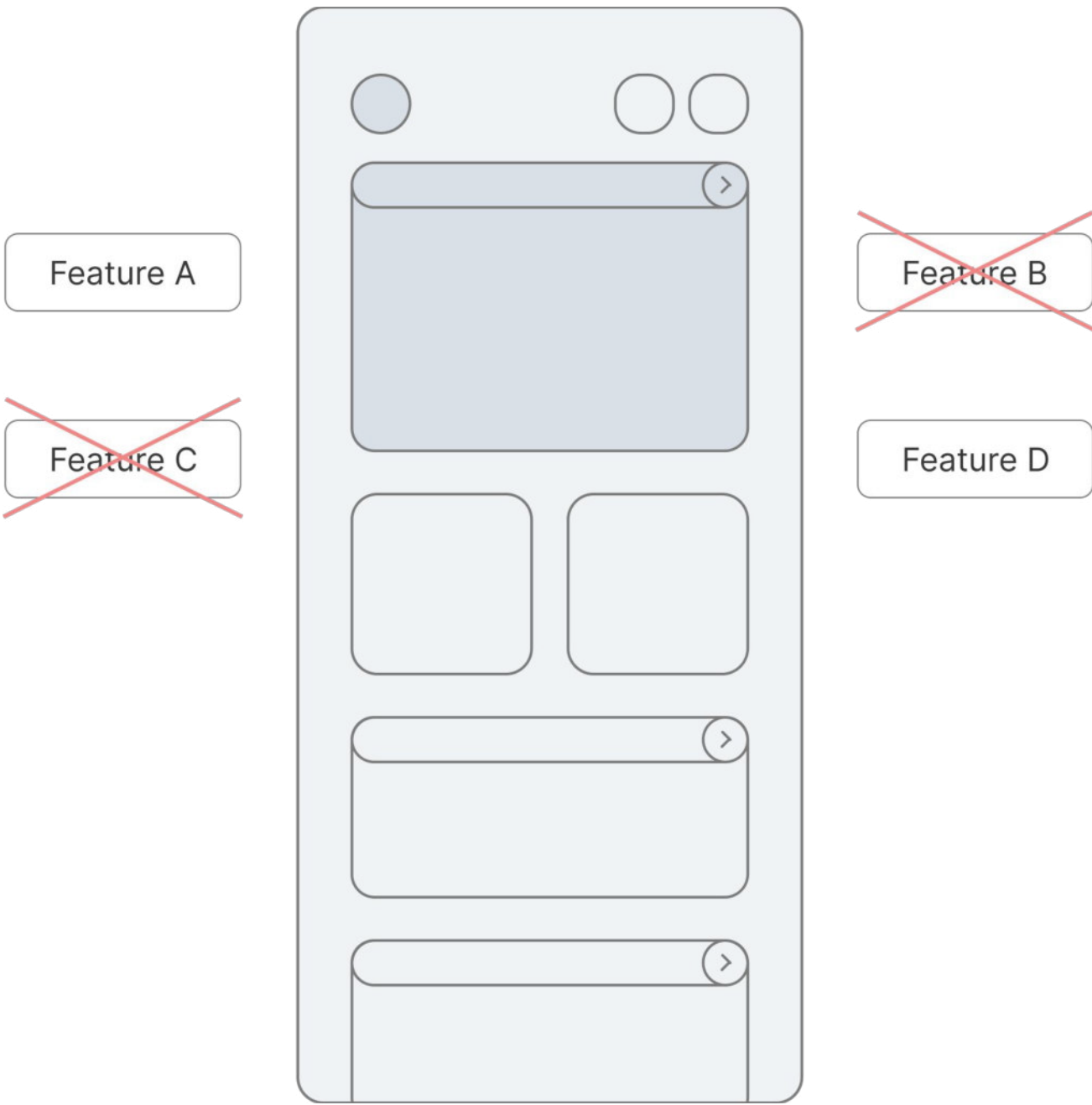
Additional Context (cont.)

The process, in a nutshell

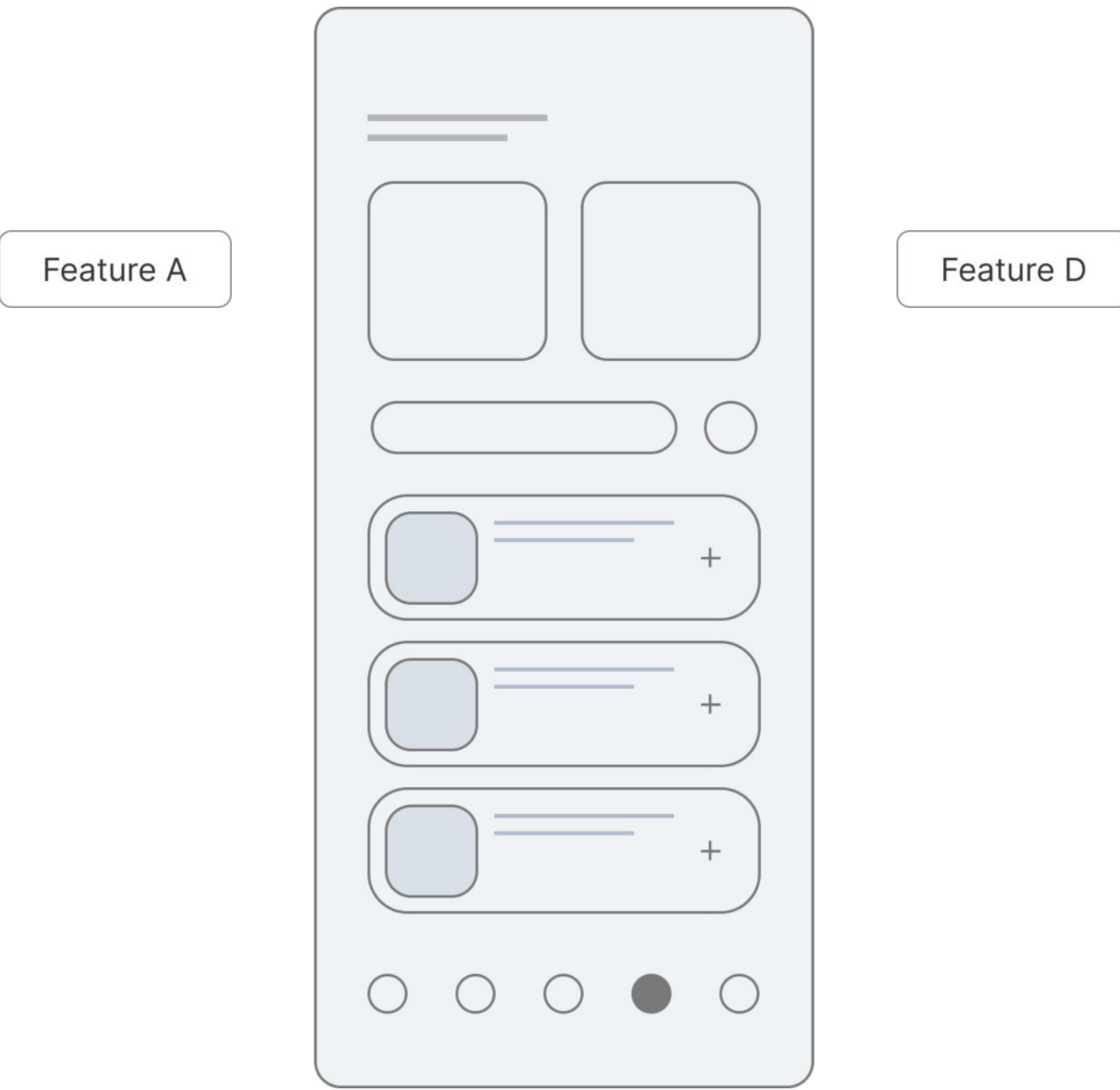
First, we built a hi-fidelity prototype based on research insights to establish UX and design strategy.



Next, I validate the concept among participants to determine what works well and what doesn't.



Lastly, our research / validation insights plus design structure were used by AT&T as a foundation to build their application.



Responsibilities

- Defining research strategy and roadmap
- Designing and executing qualitative and quantitative studies
- Synthesizing cross-method insights
- Translating findings into product and design recommendations
- Influencing product direction and experience design

Collaboration

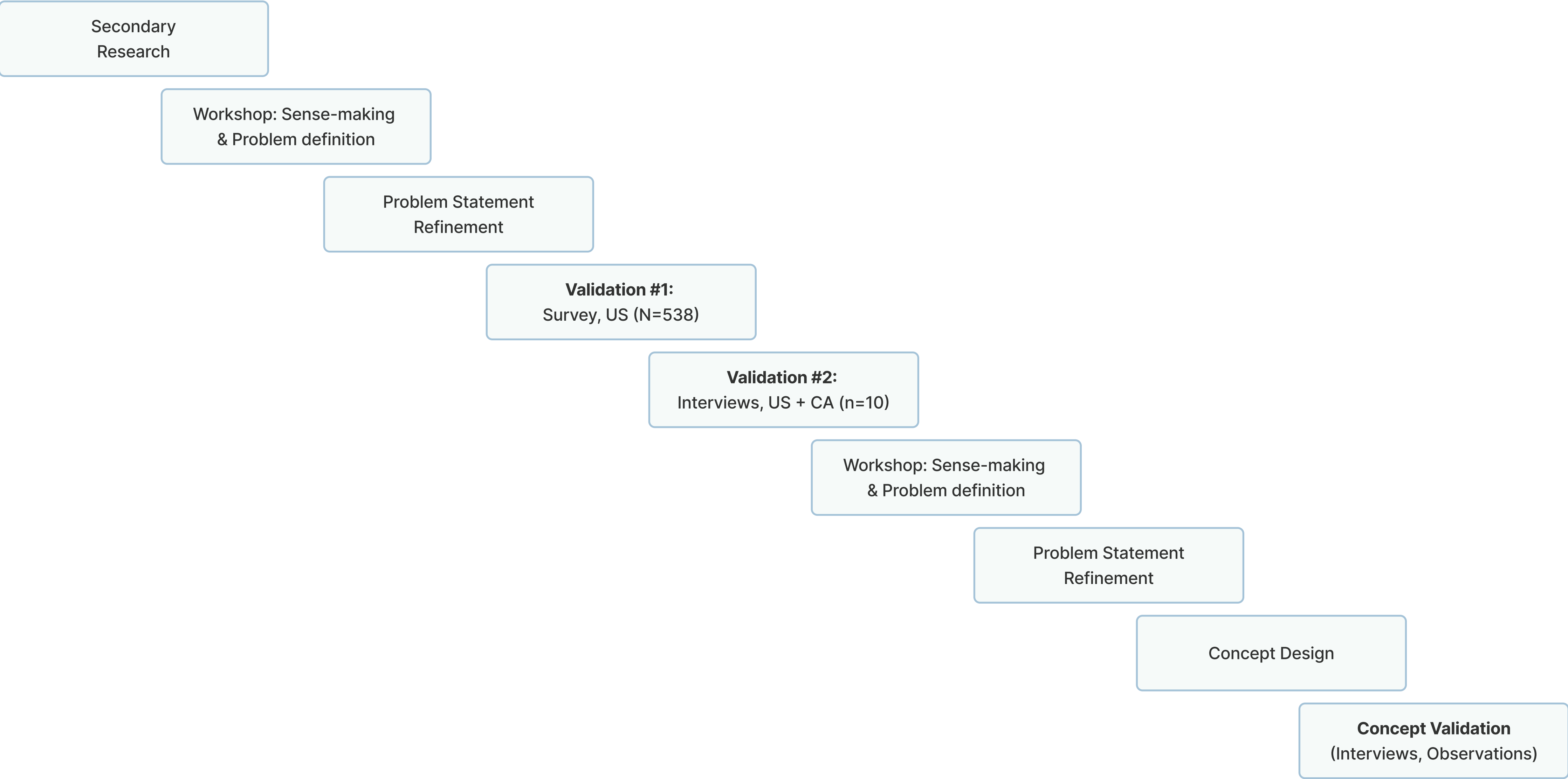
- Research Lead
- Product Designer
- Product Manager
- Project Manager
- Growth Manager

Key Impact

4.5 / 5 stars out of 80k reviews,
— *Apple App Store*

4.3 / 5 stars out of 86k reviews,
— *Google Play Store*

Research Map



Discovery Phase

Survey Studies & Interviews

In prior years, a large nationwide (US) survey was conducted via Forrester and Cint, accumulating 538 respondents. Subsequently, interviews with 10 consumers from the US and Canada were also conducted to collect qualitative insights.

Objectives

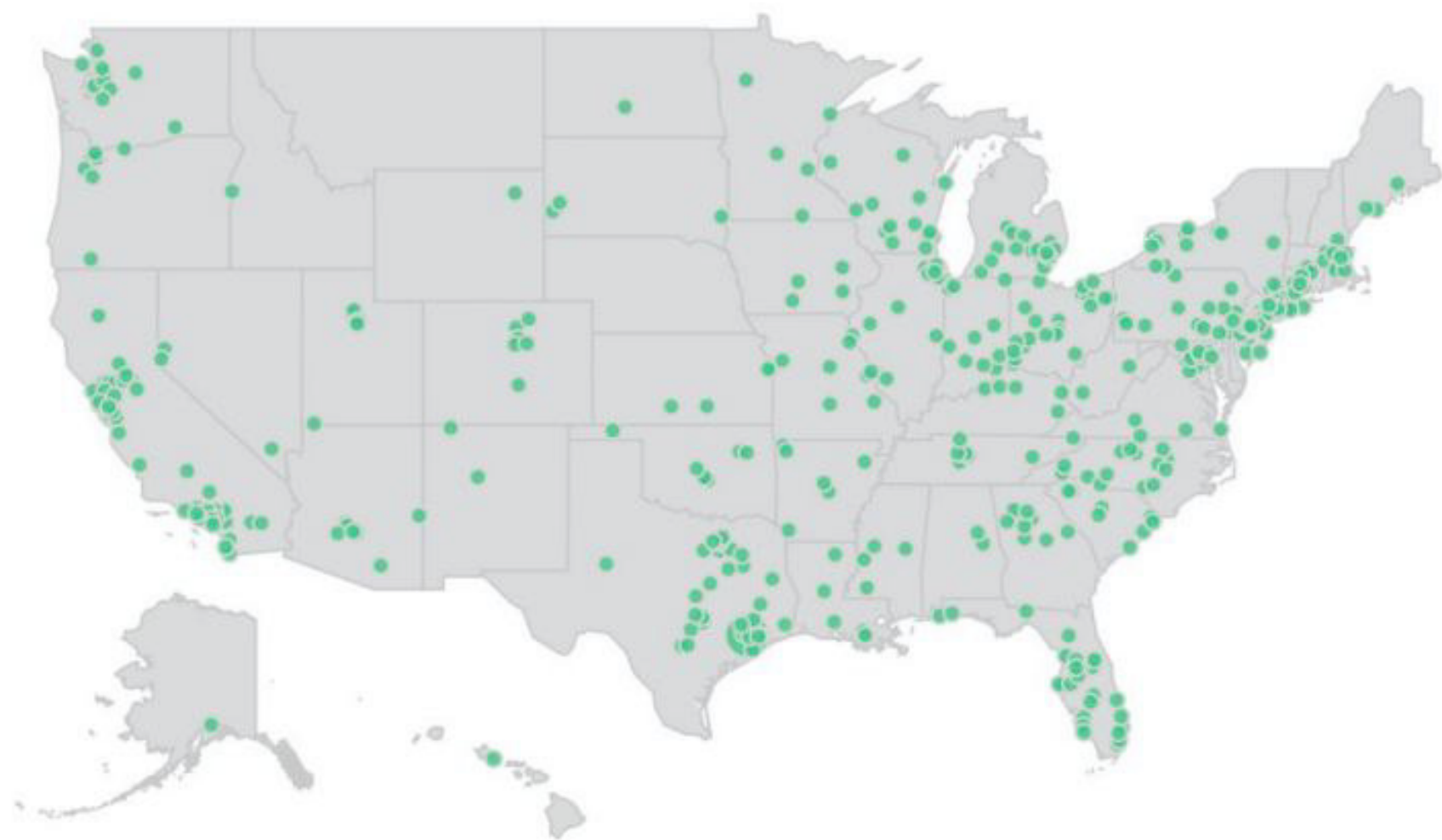
- To discover means to transform consumer business strategies, consumer and define competitive advantage
- To identify consumer needs from cybersecurity solutions (problem identification)
- To identify growth drivers

A summary of research and findings are elaborated in subsequent pages.

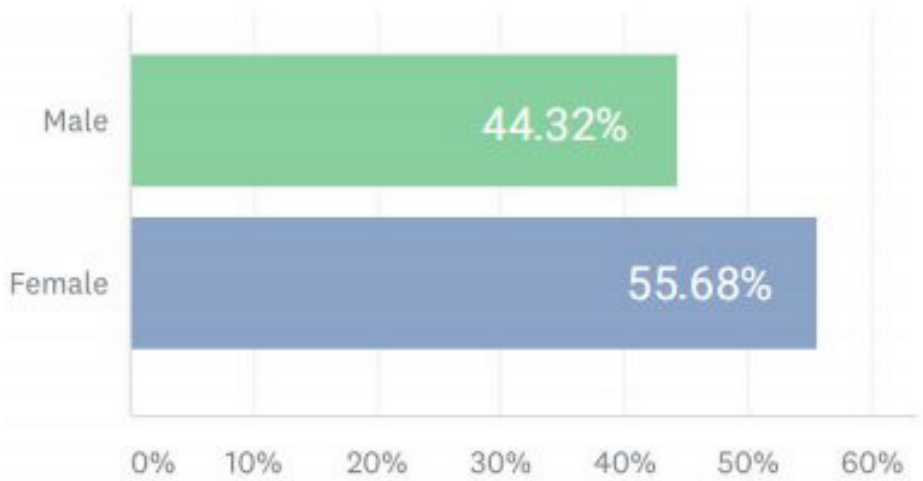
Survey Respondents Demographics (N=538)

DEMOGRAPHICS OVERVIEW

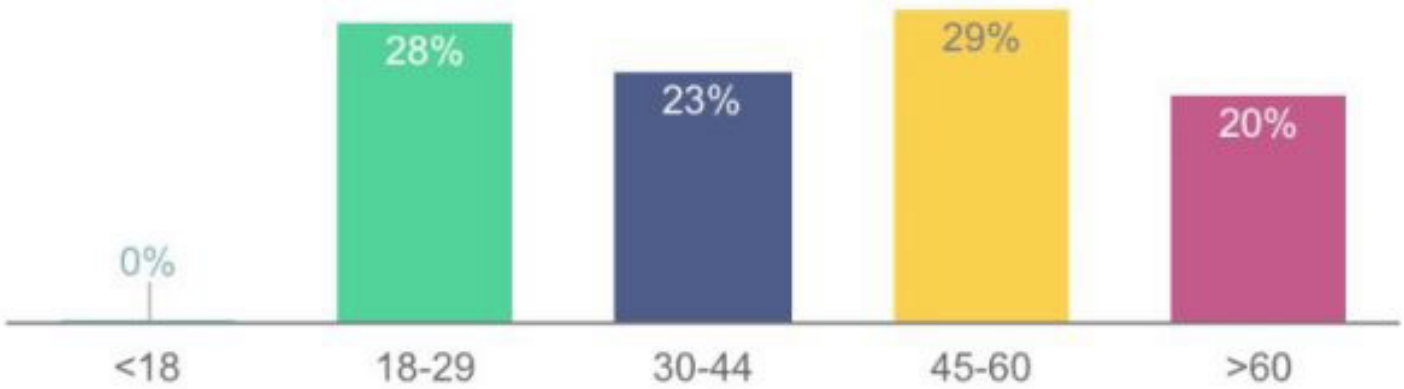
Country: United States (USA) - SurveyMonkey
Region: All Regions



Gender: All Genders
Gender Balancing: Census



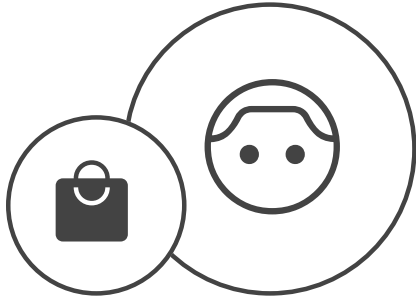
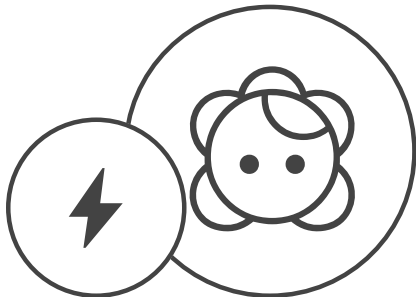
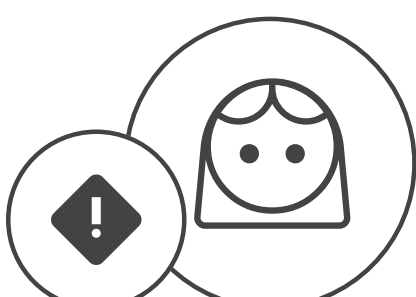
Age: 18 - 99
Age Balancing: Basic Census



Do you have children?



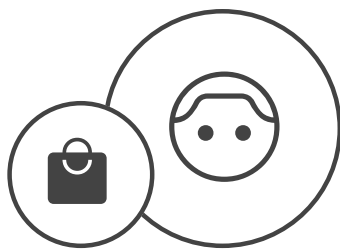
Personas & Profile types

Willing to share personal info		Conditional Consumerists (CC)	Young and tech savvy users consciously concerned about their privacy, but are comfortable sharing their personal information with companies so long they get a benefit or value.
		Reckless Rebels (RR)	Represent the largest share of consumers aged 18-24. They share personal data and take little to no precautions to protect their privacy.
Share personal info only when required		Data-Savvy Digitals (DSD)	Highly privacy aware and protective of their personal information. They use tools to protect data. Generally willing to share personal data only when required for a specific product or service.
Not willing to share personal info		Nervous Unawares (NU)	Concerned about digital privacy, and unaware how to protect themselves. They are least tech savvy and least aware of data harvesting practices.
		Sceptics Protectionists (SP)	Well informed and concerned about privacy. Nothing will motivate them to share personal information especially in social media.

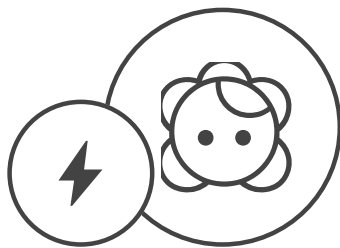
Survey Respondents Overview (N=538)

RESPONDENTS PERSONAS

Willing to share personal info



Conditional Consumerists (CC)



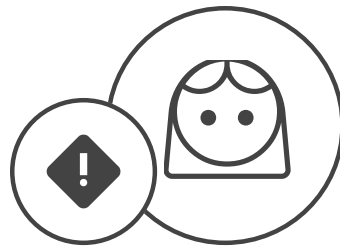
Reckless Rebels (RR)

Share personal info only when required



Data-Savvy Digitals (DSD)

Not willing to share personal info

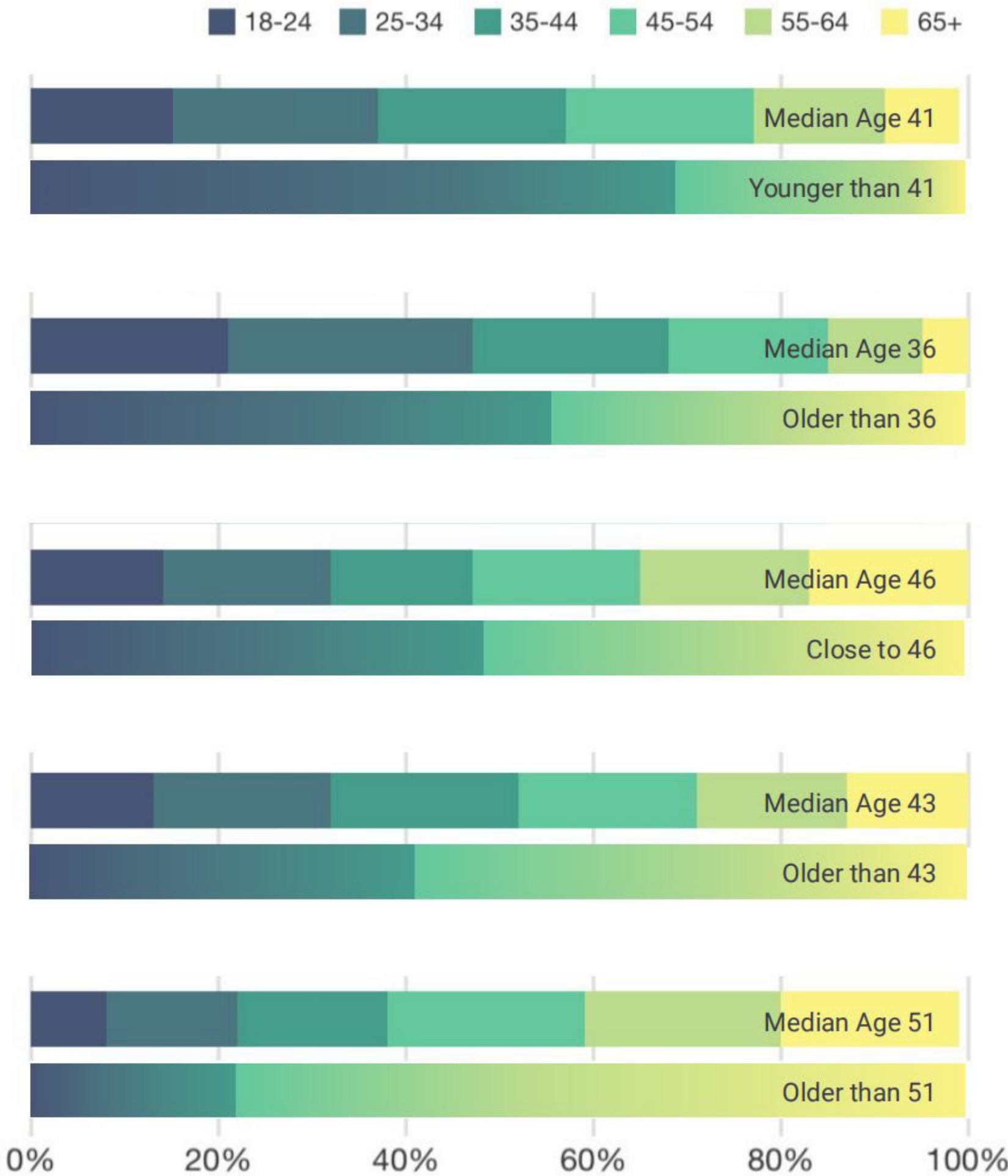


Nervous Unawares (NU)

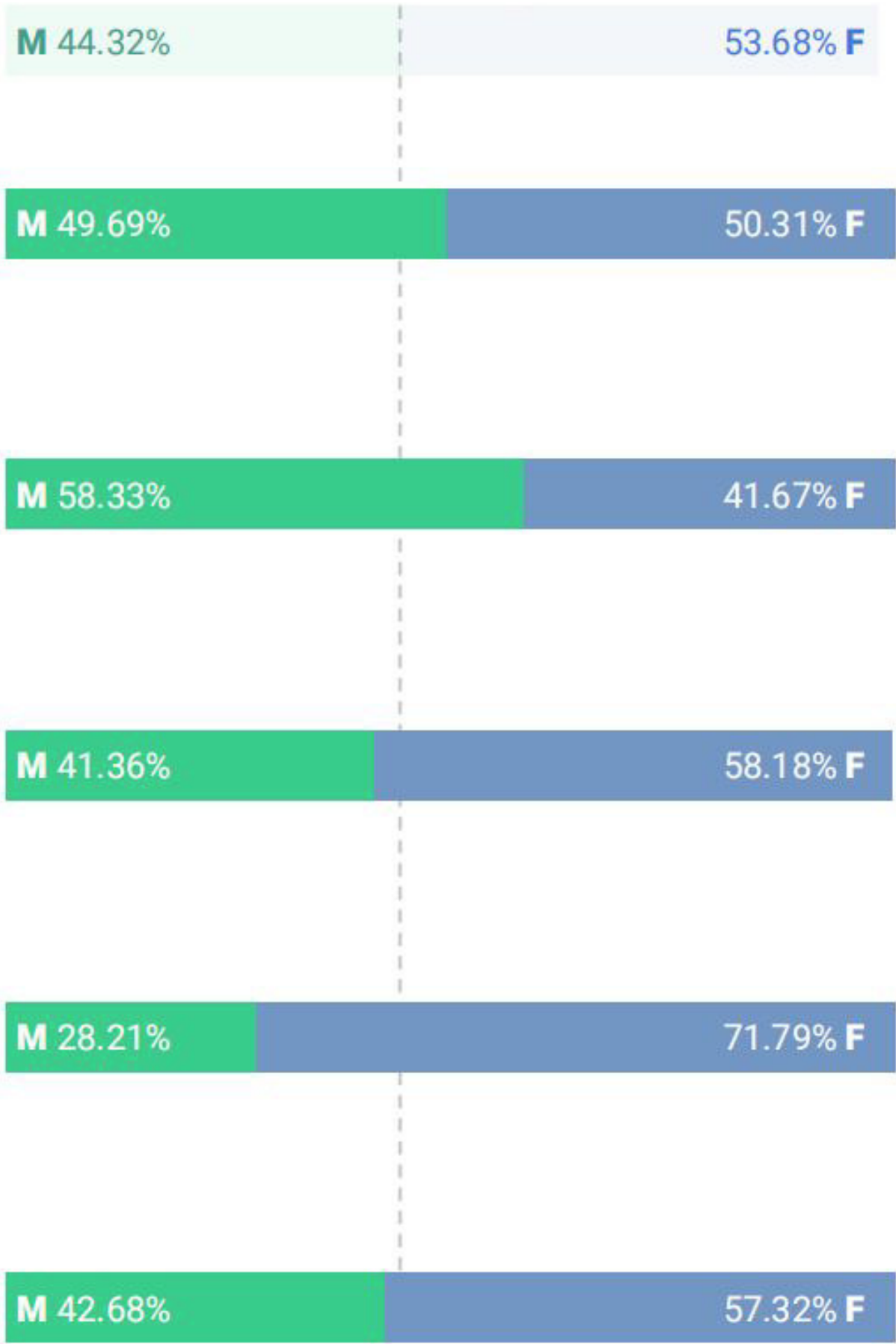


Sceptics Protectionists (SP)

BY AGE

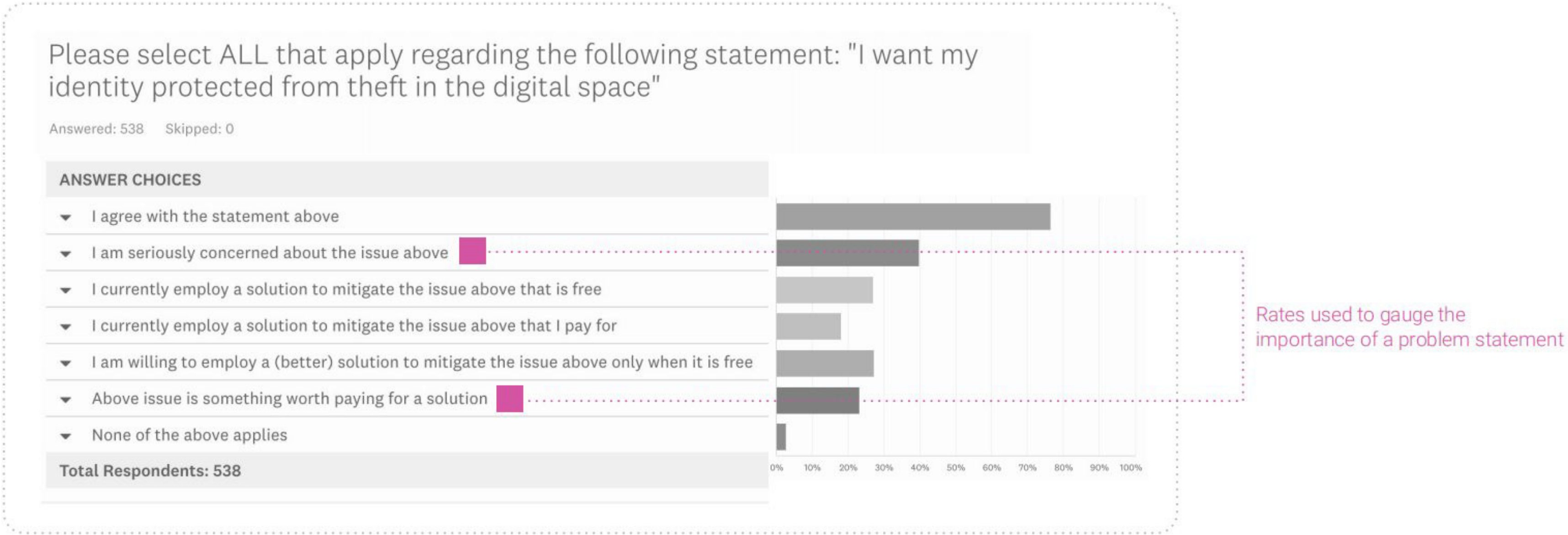


BY GENDER RATIO



Survey Format

Numerous questions pertaining to security topics were included in the survey. Participants were enabled to provide answers via choices established in the following diagram:



Summary of Findings

Rnk	Problem Statement	
1	"I want my financial transactions protected end-to-end"	Privacy
2	"I want my identity protected from theft in the digital space"	Identity
3	"I want to know if there is information about myself being used by companies without me being aware"	Privacy
4	"I want spam calls, spam SMS' and/or spam emails to stop"	
5	"I want my retail transactions protected end-to-end"	
6	"I don't want my browsing information shared with third-party companies for their use"	
7	"I want control over how my personal information is being used by companies, the government or other entities"	
8	"I don't want to feel like myself or my activities is being tracked online" (examples include getting unsolicited recommendations or advertisements)	
9	"I want to know if apps I've downloaded are collecting more data/information on me than necessary"	
10	"I want to protect all digital devices in my household, including IoT devices, routers, etc."	Household

First top voted statement:

"I want my financial transactions protected end-to-end" got the highest vote for "I am seriously concerned"

(46.65% of respondents. Avg is 34.99%).

Second top voted statement:

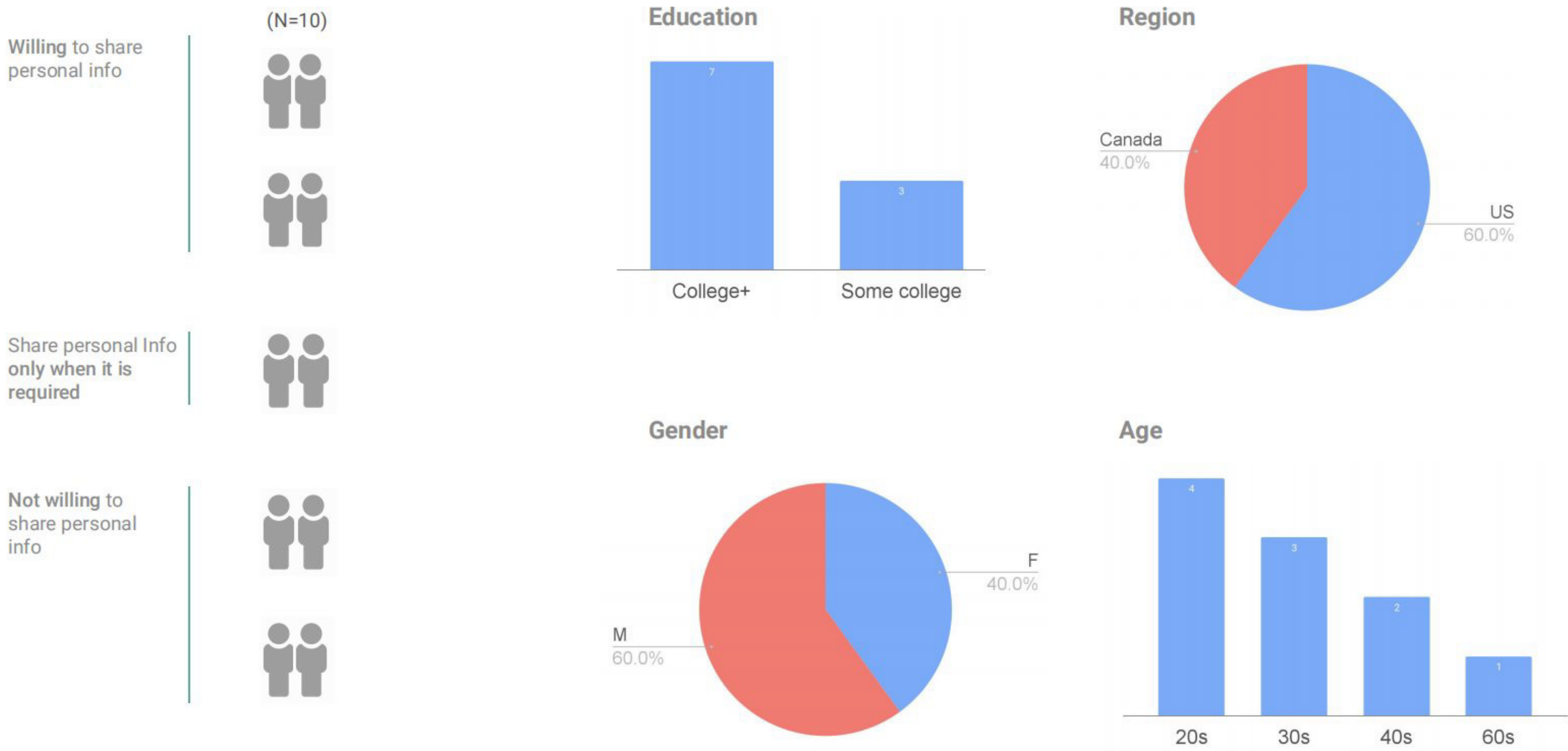
"I want my identity protected from theft in the digital space" got the highest vote for "

(23.23% of respondents. Avg is 12.40%)

Qualitative Research (n=10)

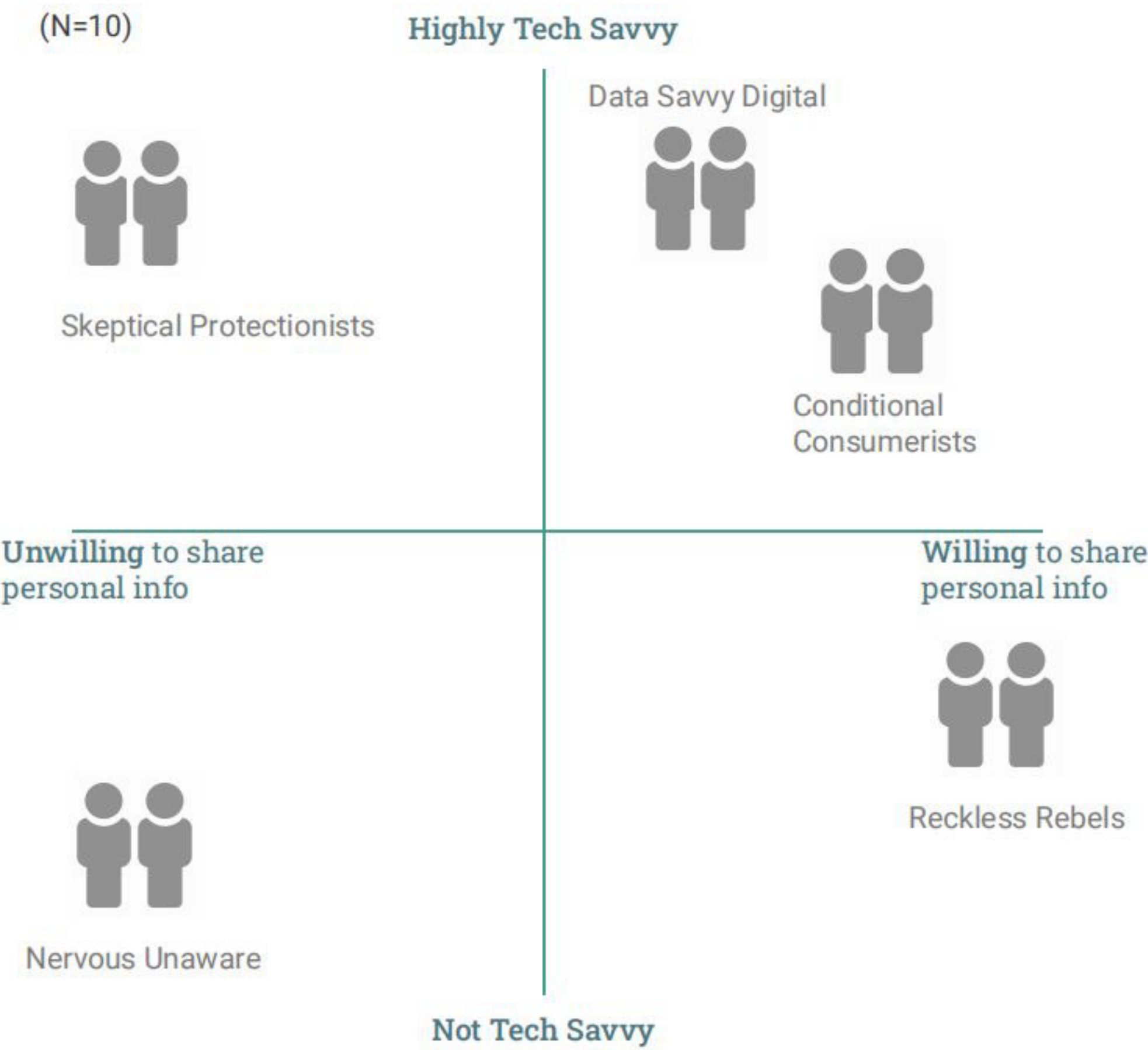
To understand consumer needs, a qualitative research was conducted among 10 participants from the **US** 🇺🇸 and **Canada** 🇨🇦

DEMOGRAPHICS OVERVIEW



User Research Map

Ten participants who took part in the survey study were recruited to expand on their needs.



LEGEND

Conditional Consumerists (CC)	Young and tech savvy users consciously concerned about their privacy, but are comfortable sharing their personal information with companies so long they get a benefit or value.
Reckless Rebels (RR)	Represent the largest share of consumers aged 18-24. They share personal data and take little to no precautions to protect their privacy.
Data-Savvy Digitals (DSD)	Highly privacy aware and protective of their personal information. They use tools to protect data. Generally willing to share personal data only when required for a specific product or service.
Nervous Unawares (NU)	Concerned about digital privacy, and unaware how to protect themselves. They are least tech savvy and least aware of data harvesting practices.
Sceptics Protectionists (SP)	Well informed and concerned about privacy. Nothing will motivate them to share personal information especially in social media.

Interview Structure

Qualitative research aimed at better understanding consumers' needs.

1. Setup/Intro

- Intro, goals for the session
- User background, use of cybersecurity applications, online behavior

2. Today's digital security and privacy problems

- Users' point-of-view (PoV) on their digital life
- Users' perception of their digital security, level of risks, and concerns

3. Today's digital security and privacy solutions

- User's approach to mitigating online security risks/concerns
- Gaps in solutions they use

4. Problem Statement Exercise

- User's response to key problem areas

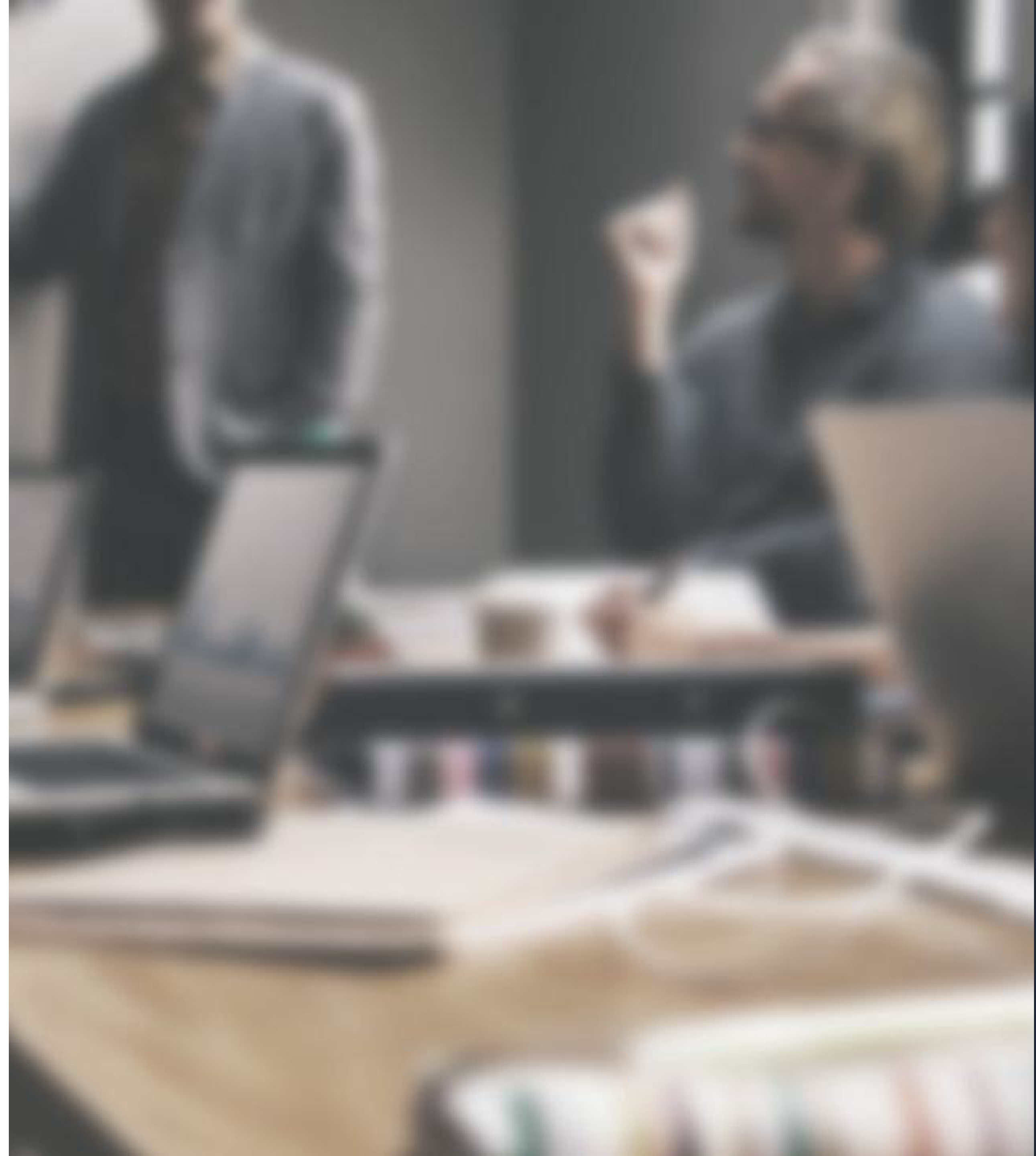
Task 1: Ranking the top 3 problem areas from the survey

Task 2: Discussing 'ideal solution' with users based on established themes

Task 3: Price test (not disclosed in this document)

5. Future vision

- Participants' view on the ideal digital security solutions for the near future



Summary of Findings

The top 5 important problem statements were:

1. I want my financial transactions protected end-to-end.
2. I want my retail transactions protected end-to-end.
3. I want my identity protected from theft in the digital space.
4. I want spam calls, spam SMS' and/or spam emails to stop.
5. I want to protect all digital devices in my household, including IoT devices, routers, etc.

Ideal Solution Theme 1:

“HELP ME MAKE SMART DECISIONS”

People want to be informed of any risk before signing up, giving information, or making transactions about the website/service they're about to interact with — Are they asking for too much personal information? Do these websites have a good reputation? etc.

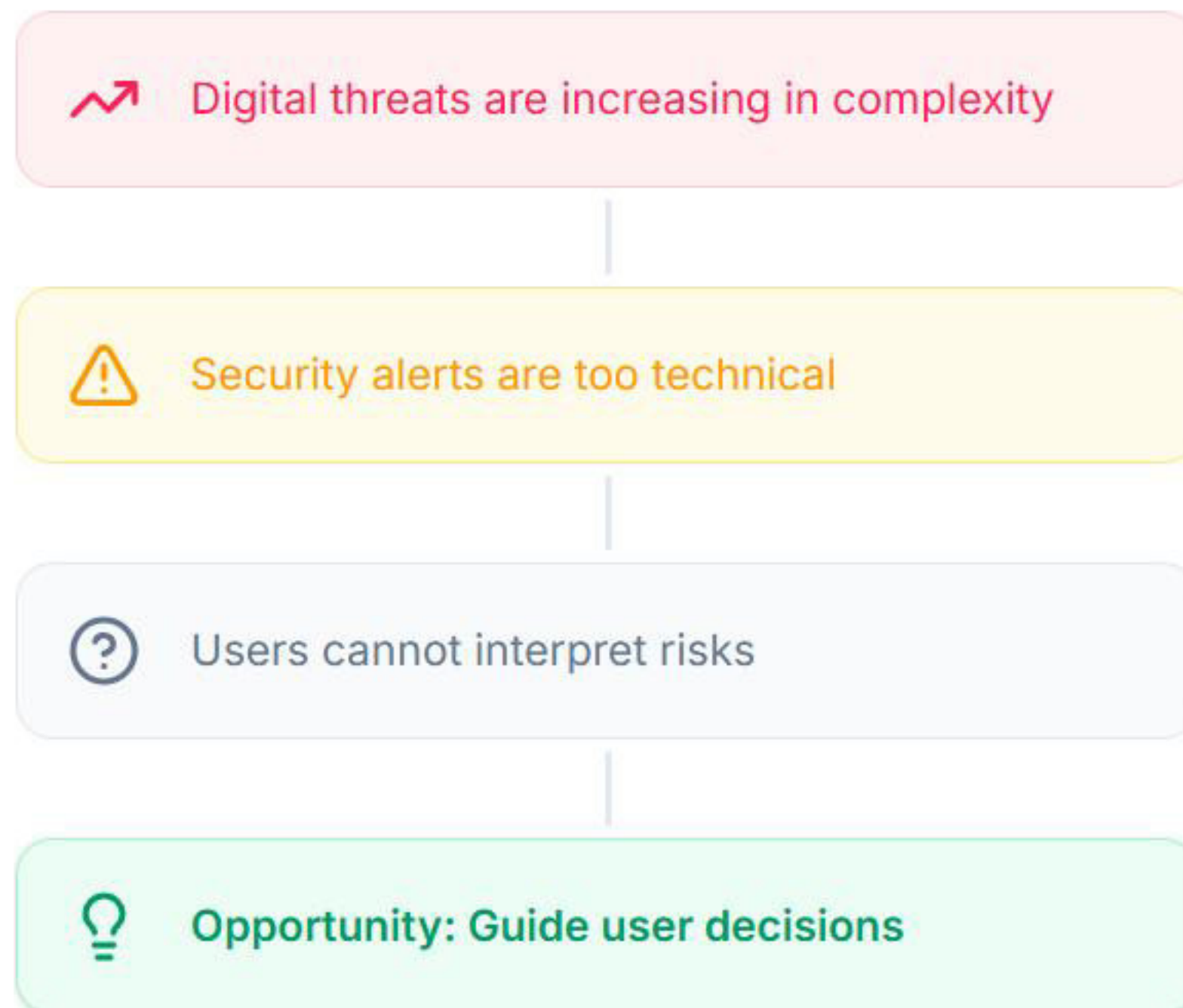
Ideal Solution Theme 2:

“GIVE ME A SINGLE-PANE VIEW & CONTROL OF MY DIGITAL INFO”

In regards to their accounts and transactions, people want a central dashboard view of status and activity — Where am I signed in? Who has my email address? What transactions were made under my digital identity? etc. Many wanted to be able to deny access/void any logins they didn't recognize or approve of from that dashboard

Strategic Product Question

Users deal with an array of difficulties when dealing with security threats:



Core take-away:

Consumers do not want just a feature-rich security tool; they want decision support and guidance when facing a digital risk

Opportunity Tree

Taking everything together, our north star is about building an application that boosts consumers’ confidence and control of their digital safety.



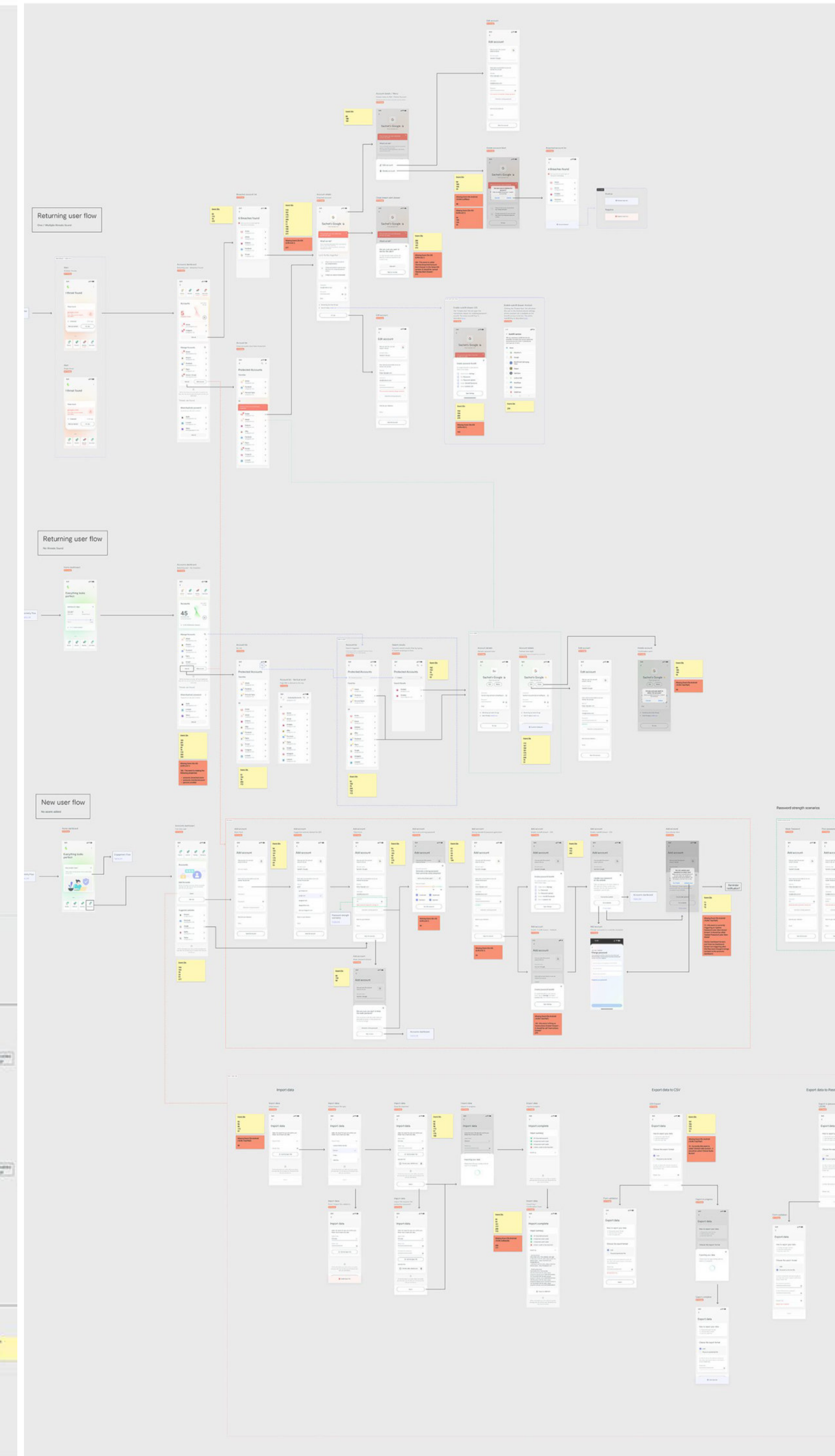
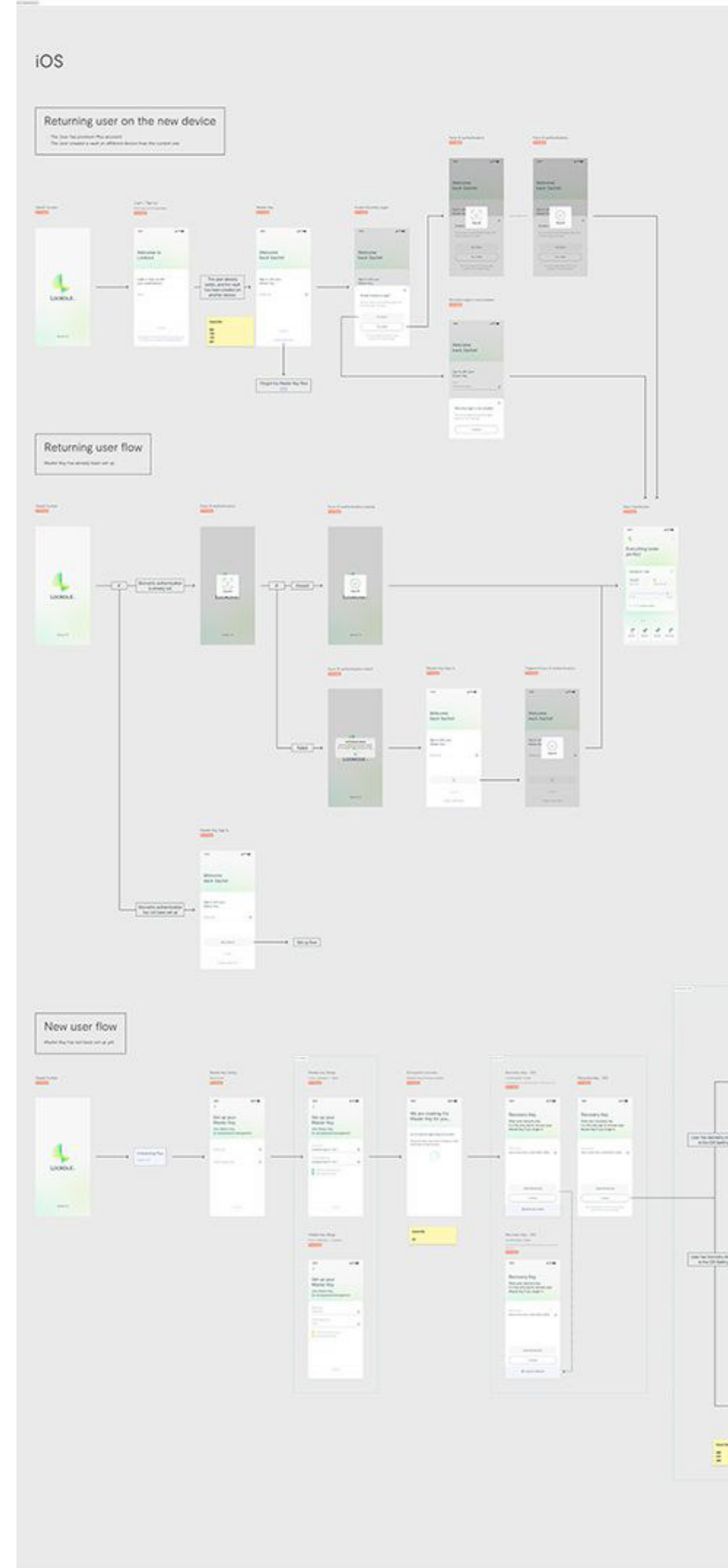
Concept & Exploration Phase

Concept Design

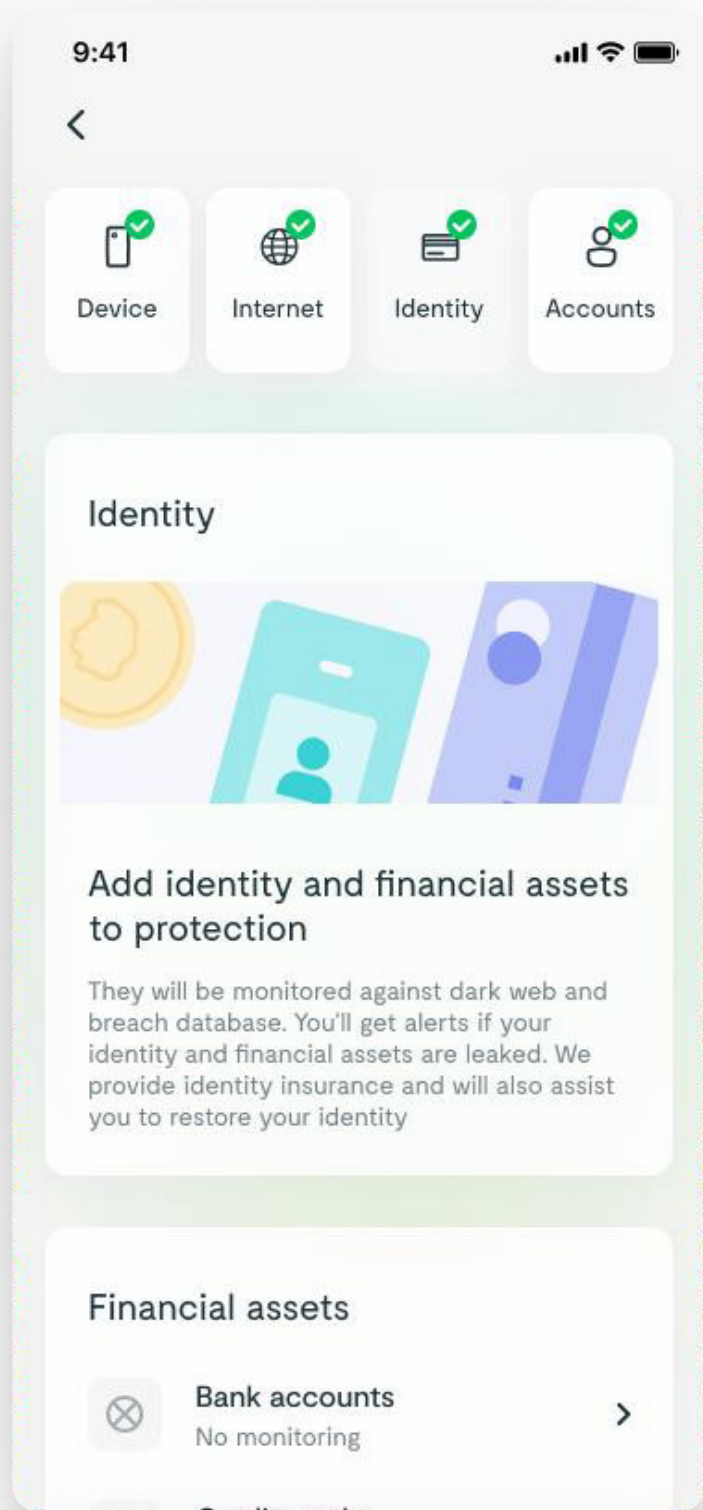
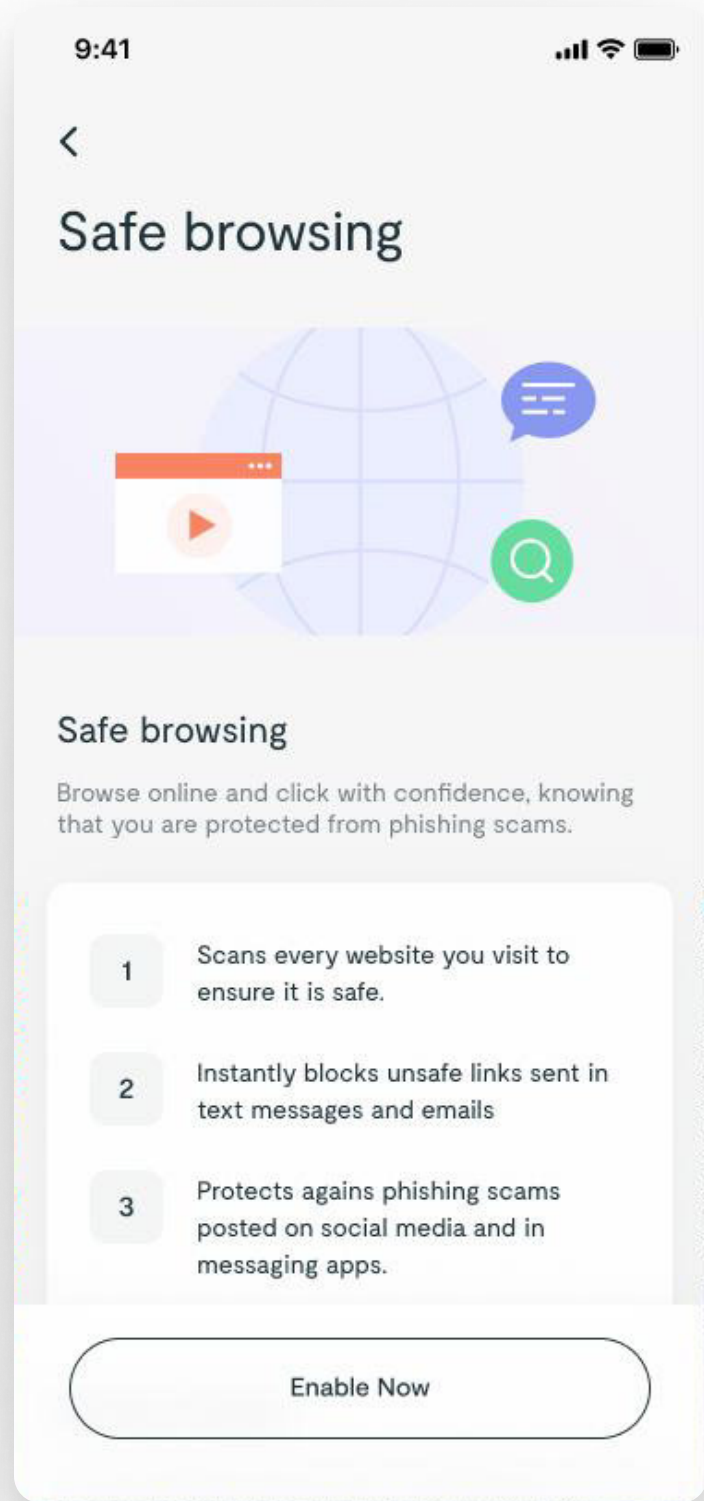
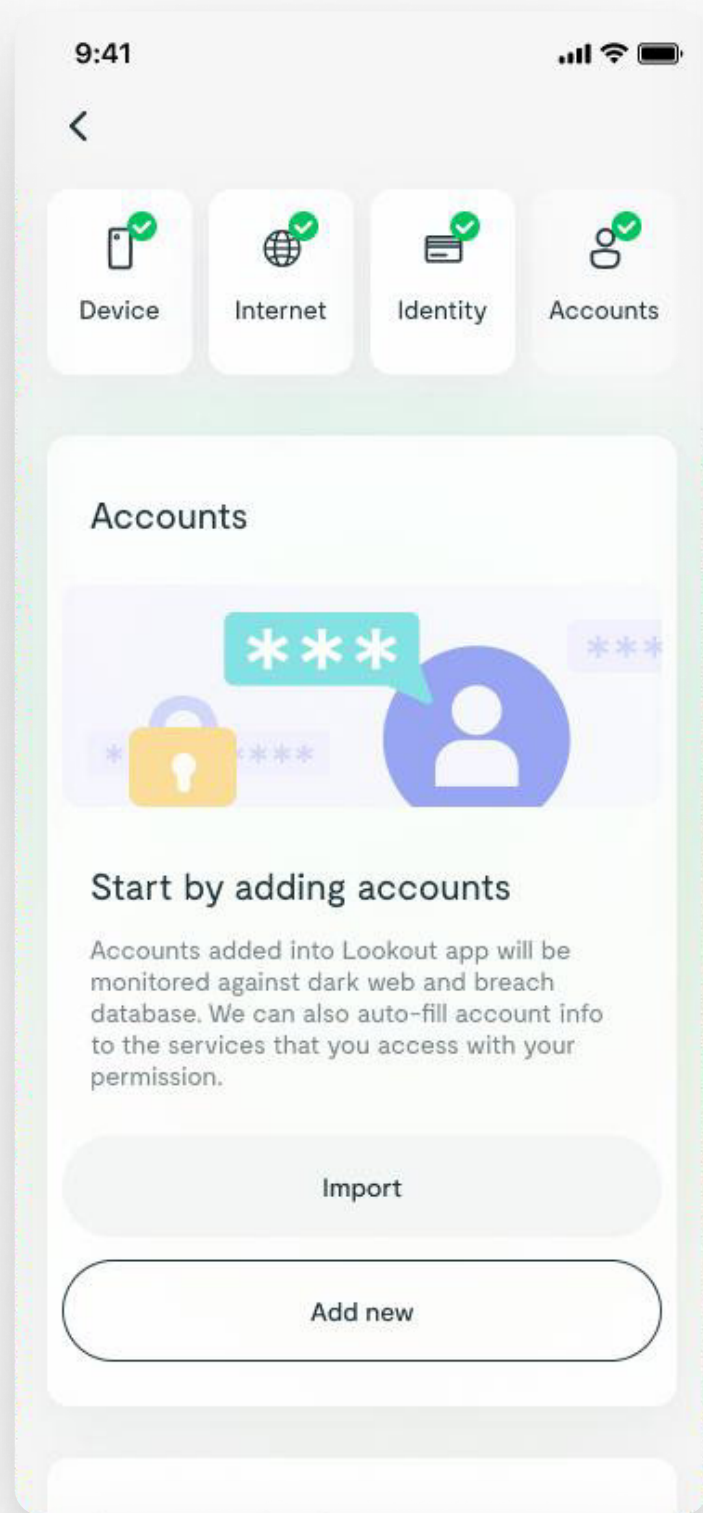
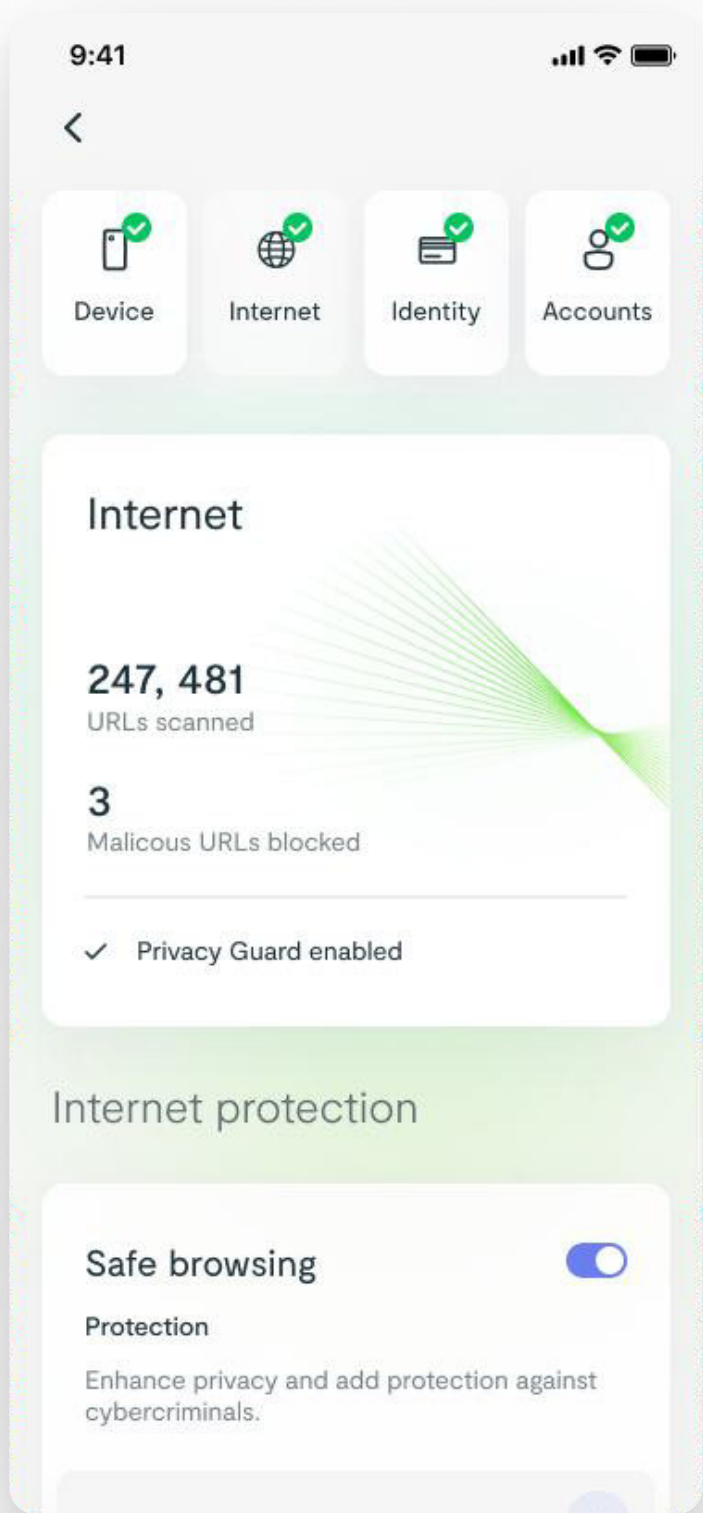
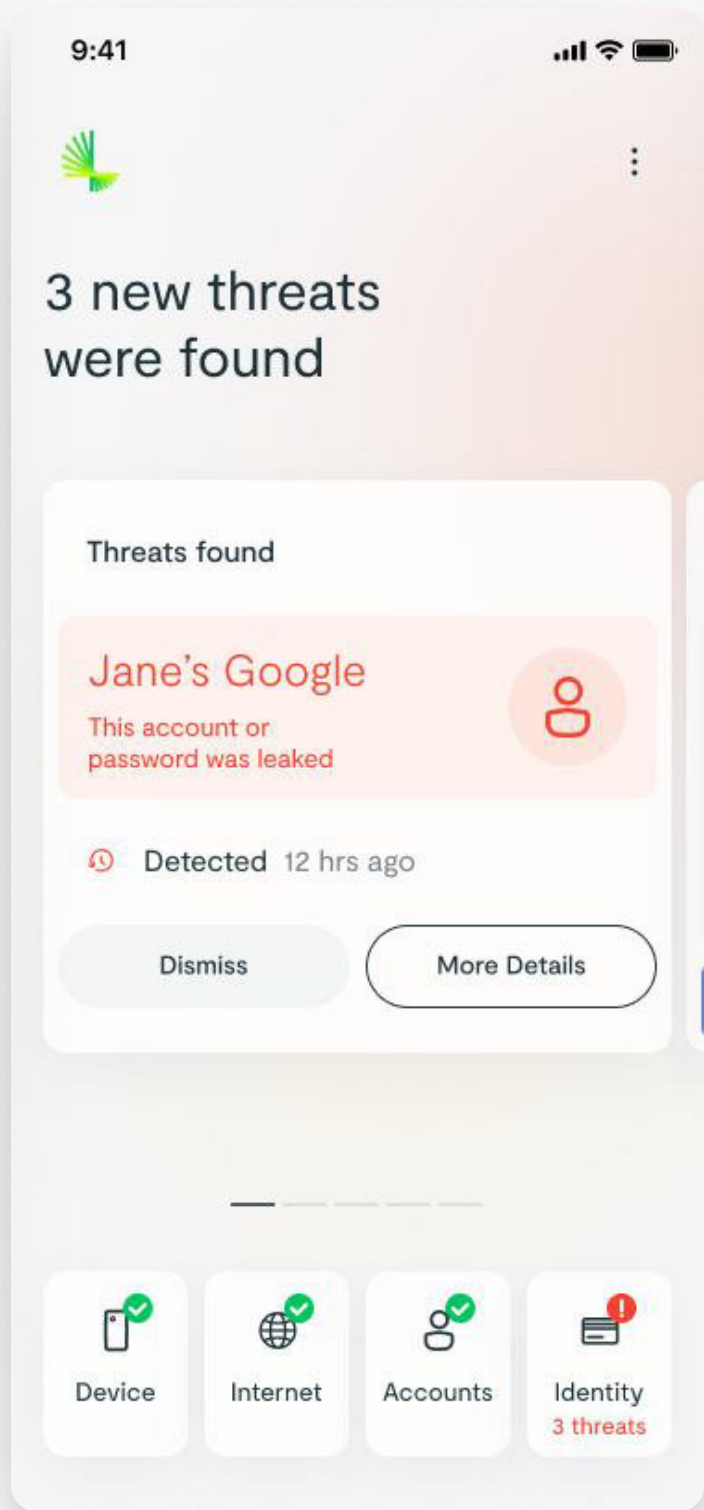
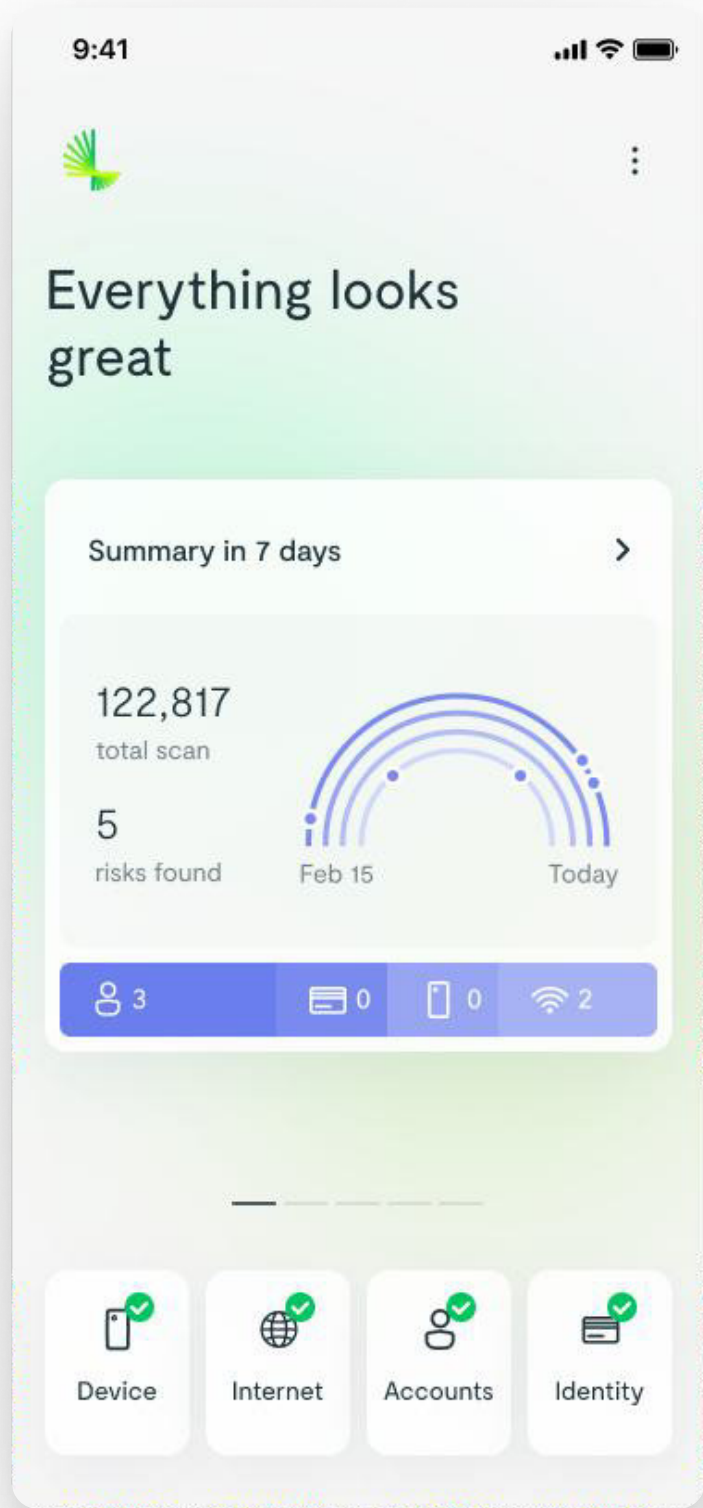
Following the research and synthesis phases, I partnered with a product designer to finalize a concept design. This phase involved cross-functional stakeholder alignment to ensure the concept addressed both user needs and business objectives.

Key areas of focus included:

- Onboarding experience
- Product growth strategy (i.e. gaining paid users)
- Information architecture
- Content design
- Feature definition
- Happy paths and edge cases



A few previews from the foundation app concept



Core Product Interaction flow



Evaluation Space

Evaluation

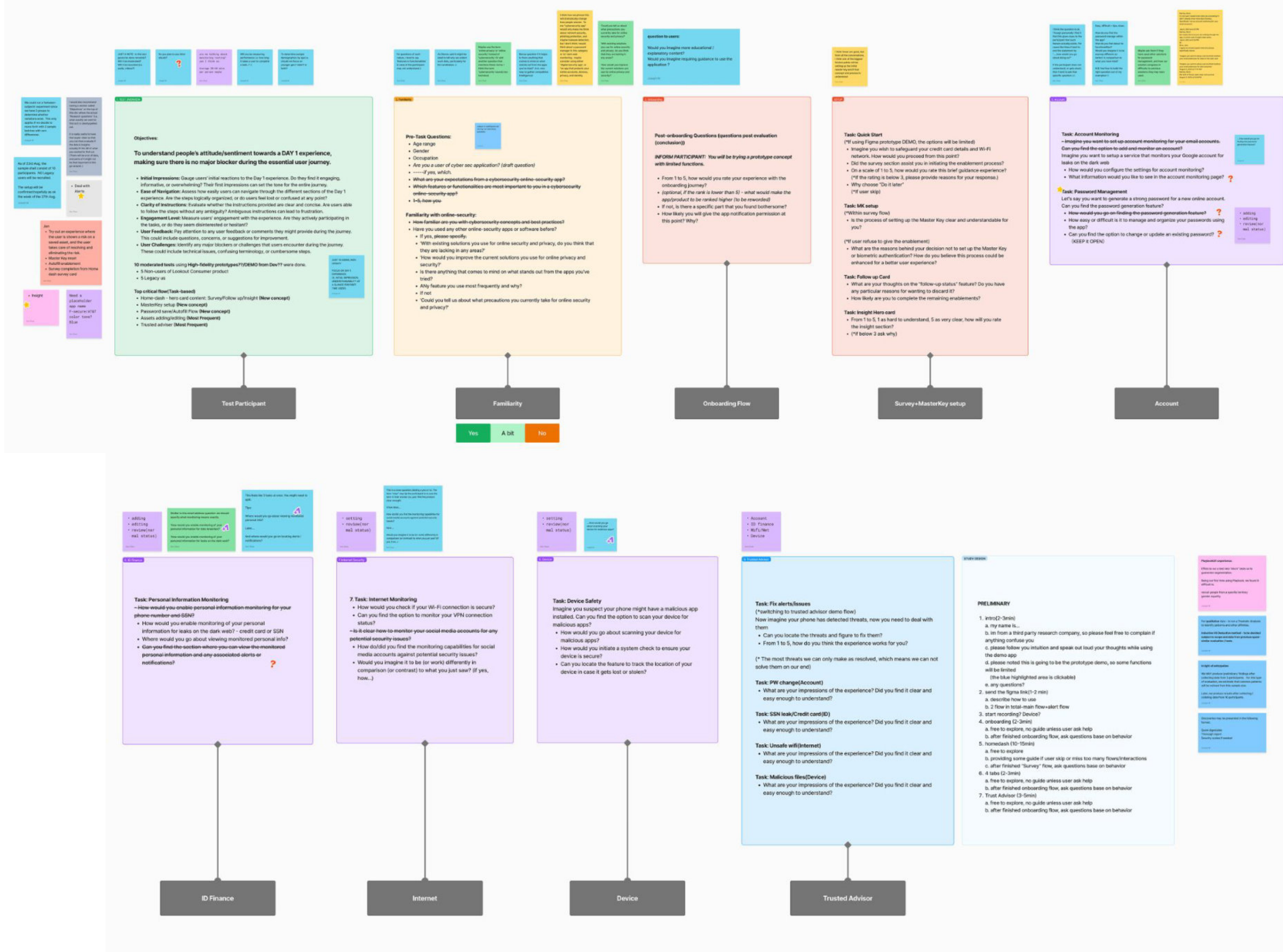
To validate the product concept, I conducted a remote moderated usability study over a two-week period using the **PlaybookUX** platform. Twelve participants (n=12), comprising 7 males plus 5 females with an age bracket of 20-45 years old were randomly selected.

Session structure:

- Study onboarding and contextual interview
- Prototype try-out with scenario-based tasks
- Post-session reflection

Participants were first introduced to the prototype and onboarding flow, then asked to complete realistic scenarios, such as: *“What would you do if your bank account was compromised and flagged by the app?”*

This approach allowed us to evaluate not only usability, but also decision-making behavior under simulated risk conditions.



Outcomes

Overall, participants responded positively to the product concept, particularly appreciating the guided onboarding experience and the clarity it provided when configuring the app.

One of the most valued features was the ***“Let’s fix this together”*** flow, a guided resolution experience designed to help users respond to security breaches.

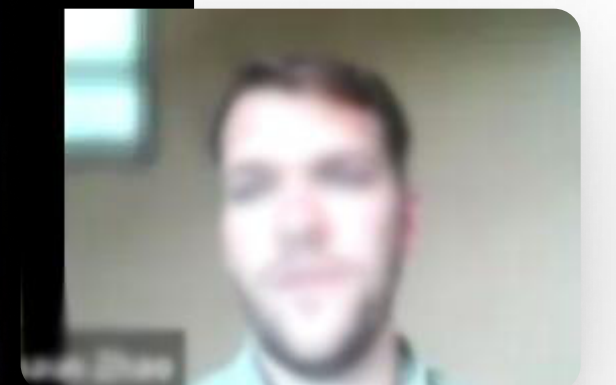
Participants reported that this feature increased their sense of safety and confidence, reinforcing the importance of actionable guidance in security contexts.

Key areas for improvement emerged around content clarity and hierarchy. Participants noted that certain terminology, messaging, and information structure required simplification to improve comprehension.

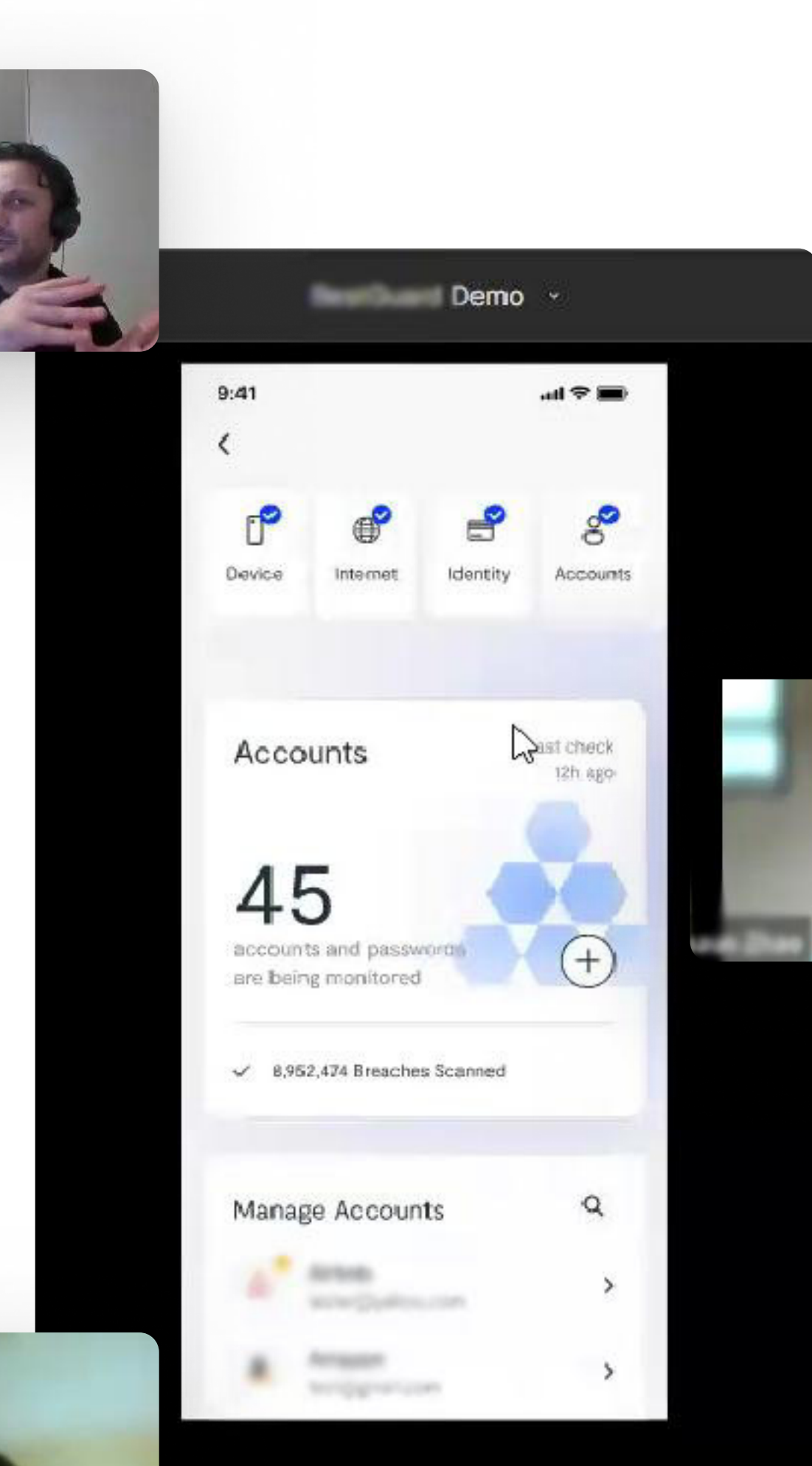
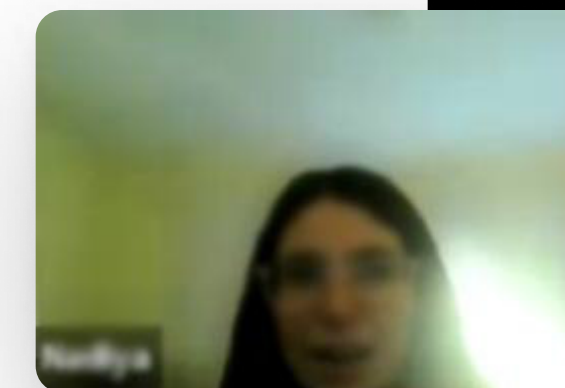
Moderator (me)



Moderator (PO)



Participant (US)



End of deck