**CSC318: The Design of Interactive Computational Media**

**Securing Privacy and Preventing Scams during Online Purchases**

**TA: Ken (Studio D)**

**A REPORT**

**by**

**Team Vulcan**

Aayush Bhan (aayush.bhan@mail.utoronto.ca)

Asma Mohammed (asma.mohammed@mail.utoronto.ca)

Madhav Kanna Thenappan (madhav.thenappan@mail.utoronto.ca)

Mugdha Banthwan (mugdha.banthwan@mail.utoronto.ca)

Sahil Handa (sahil.handa@mail.utoronto.ca)

Stephen Lim (alfonsusstephen.lim@mail.utoronto.ca)

UNIVERSITY OF TORONTO

OCTOBER 2023

**TABLE OF CONTENTS**

1. Chapter 1: Introduction 3

1. Introduction 3

2. Motivation 4

3. Stakeholders 5

a. Primary Stakeholders

b. Secondary Stakeholders

1. Chapter 2: Field Studies 6

I. Data Gathering Technique 1: Interviews 6

II. Data Gathering Technique 2: Questionnaires 10

III. Key Findings 11

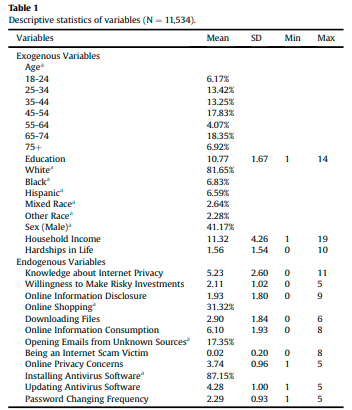
1. Chapter 3: Experience Map 14
2. Chapter 4: Job Stories 17
3. Chapter 5: Design Requirements 19
4. Appendices 21

# 

# CHAPTER 1: GENERAL PROBLEM

# 

## INTRODUCTION

Over the years, online shopping has become very popular due to the variety of goods, convenience, and different types of delivery options it offers. We saw a surge in online sales and purchases during the Covid-19 pandemic. However, as much as it has eased our lives; it also has certain drawbacks. One of the most important drawbacks is the risk of fraud and scams. In table[[1]](#footnote-0) mentioned below for a sample size of 11,534, 18.35% of people are between the ages of 65-74 affected the most by these scams, where 31.32% of the scams come from online shopping.

*In this study, we aim to find ways to prevent and reduce online purchase scams and their effects on our stakeholders. We also want to find ways to guarantee online privacy for them.*

## MOTIVATION

There has been a steady increase in the number of online purchase scams over the years. According to ABC news, Americans lost $10.3 billion to internet scams in 2022, especially, the elderly lost $3.1 billion to internet scams in 2022, the most of any age group.[[2]](#footnote-1) These commonly take place in the form of phishing emails, impersonation calls, fake deliveries, etc. Not only do scams lead to revenue loss for institutions and customers, but they also affect people’s mental health. Scams often result in financial losses, which can lead to significant financial stress. The worry over repaying debts or regaining financial stability can contribute to mental health problems such as insomnia and overall anxiety. This can lead to trust issues in online shopping, as individuals believe they are making legitimate purchases. Discovering that they have been deceived can lead to feelings of betrayal. To mitigate the impact of scams on financial losses and mental health, it's important to take preventive measures, such as staying informed about common scams, being cautious about sharing personal information and reporting scams to relevant authorities.

Our process to arrive at the problem statement is described in our mind map. We first tried to understand online scams by dividing them into different parts by talking about impacts, types of scams, causes and their effects on the victims(e.g. losing money due to fraudulent transactions).

Scams can lead to feelings of anxiety, stress, and anger leading victims to develop a lack of trust in online shopping and e-commerce platforms, which in turn causes mental health issues. This can lead to victims may face legal actions, investigations, or disputes to resolve the scam.

Hence, we decided to focus on securing privacy and taking steps to avoid falling for scams in the first place.

## STAKEHOLDERS

### Primary Stakeholders

We will be focusing on people who spend a considerable time shopping online in the working age group (16 - 60 years).

PERSONA:

### Secondary Stakeholders

We will be focusing on Financial Institutions and e-commerce companies.

# CHAPTER 2:

# FIELD STUDIES

## DATA GATHERING TECHNIQUE 1: INTERVIEWS

### Primary Stakeholder

**1.1 Scammed Individual**

Understanding the thoughts, feelings and emotions of the primary stakeholder, the scammed individual, is really important because it provides the research team with qualitative information in a first-person point of view, which can be used to better understand the motivations behind the scammed individual’s actions and responses. This is best facilitated by a semi-structured interview, which allows the individual to capture relevant information, regardless of questions.

We found an individual, who had been scammed via phone call, through the team’s personal network, and conducted a one-on-one semi-structured online interview with them. The individual is a 20-year-old university student who was also new to Canada and wasn’t familiar with the practices used by banks with respect to the sharing of sensitive personal financial data when they got scammed.

This interview was focused on addressing questions regarding the methods used by the scammer to scam the scammed individual and what they feel could have been done to prevent scamming, as a result allowing us to complete the incomplete POV statements 1 and 5(referenced in Appendix).

An online meeting time was coordinated with the list of questions being explored, and the protocol and consent form(referenced in the appendix) were shared with the scammed individual prior to the interview. Once the meeting started, the participant shared the signed consent form, and we started discussing the questions with the responses being recorded. This was done to create a transcript of the discussion for better documentation of research data. This was done prior to the questionnaire being sent out so the insights gathered would help create a questionnaire to answer pertinent unanswered questions.

### Secondary Stakeholder

#### 2.1. Fintech

Fintech companies are usually the “middleman” between a consumer that makes a transaction and banks that facilitate that transaction. Companies can range from services that provide shopping solutions to retailers such as Shopify and Strip or huge e-commerce retailers such as Amazon. In a way, fintech companies provide us with a third-person point of view due to the nature of their workings and play an important role in protecting users from scams and frauds. Hence, we used our connections within the industry to find someone willing to be interviewed. We determined that an interview would be the best data-gathering method to tackle this because it provides us with information about the inner workings of fintech companies. We determined this will help us answer our incomplete POV statements 3 and 4. We wanted to know what fintech companies are doing to tackle fraudulent online shopping transactions made by scammers. In addition, we wanted to know what responsibilities fintech companies have in ensuring online shoppers have a safe and easy experience when making an online transaction via their platforms.

Our interviewee is a software engineer working for a Toronto-based fintech company in their transactions department. We identified them to be a good source to interview because of their 5+ years of experience working in the industry which indicated their knowledge in the inner workings of the company. We familiarize them with our research, the content of our questions, and why we think they might be a good candidate for answering them. After they agreed to an interview, we ensured that they got a protocol form and a consent form (both referenced in the Appendix) administered to them. The interview consisted of 11 questions and was mostly structured with an opportunity to ask follow-up questions when they arise. We felt the need to create mostly structured open-ended questions because we wanted to get a clear understanding of the technicality and inner workings of how fintech companies tackle scams. However, we also ensured to ask if there was anything else they would like to add before we finished the interview. This allowed us to catch anything we had not previously thought of asking as well as any personal experiences and insights coming from someone within the industry.

#### 2.2. Banker

To gather quality data, the team opted for one-on-one interviews, where the team can gather intimate and detailed responses to formulate many key insights. Our interviewee was a banker in the fraud department who specializes in rectifying scam requests. This individual was selected due to their expertise in dealing with scam cases, providing us with valuable insights into the resolution process and trends in scam requests. The interviewee was given a protocol form (referenced in the Appendix) where the style and significance of the interview were outlined. Furthermore, we decided to conduct interviews first to gather key details that can be implemented in our questionnaire (2nd method) to probe for more key insights. The interview was semi-structured and was an opportunity to gather information on the individual experiences.

Utilizing the team’s network, we were able to contact and have a 30-minute conversation. The team notified the individual about the premise of the conversation as well as administered the consent form to the interviewee beforehand. Then, the team compiled a list of questions that could be asked, however, there was an emphasis on allowing the interviewee to answer questions out of the scope of the questions. This semi-structured interview style enabled the team to get a broad sense of the problem statement at hand and then use this information to dive deep into other probing methods. For example, many questions formulated by the team targeted the idea of how scams are executed, but the interviewee gave insights about where and why these scams happened(incomplete statement 4). This style of interviewing allowed the team to gain a multidimensional understanding of the problem that would have been overlooked if the interview style had been well structured. Gaining these insights allowed our questionnaires to be more effective.

**The Perspective of a Banker:** Interviews with the banker revealed the complexity of the situation from the side of those tasked with rectifying scam requests (incomplete statement 5). The constantly shifting landscape of scam tactics challenges these professionals to adapt and remain vigilant. Understanding their perspective is vital for improving prevention and response strategies.

## DATA GATHERING TECHNIQUE 2: QUESTIONNAIRES

We chose to use questionnaires in order to reach out to a larger and more diverse audience. They remove the time and regional constraints on the number of individuals we can connect with. We wanted to be as inclusive as possible. People with disabilities may find it difficult or uncomfortable to sit through interviews or observations. Questionnaires might be an easier option for people with them, especially for people with speaking, hearing and executive dysfunction disabilities.

We created two questionnaires, one aimed at primary stakeholders and the other at secondary stakeholders using Google Forms. The questionnaires consisted of objective questions (e.g., Single-choice questions, MCQs, etc.) as well as subjective questions.

For the primary stakeholder's questionnaires, we used social media like Instagram and WhatsApp to spread the questionnaire. We also sent it to our personal contacts within the age group of 16-60.

For the secondary stakeholder questionnaires, we reached out to our connections who work with or know someone who works in either financial institutions or e-commerce companies.

For the primary stakeholders, we recruited individuals who shop online frequently and belong to the working age group (16 - 60 years). The first two sections of the form inform the participants about the aim of the study and ask for their consent. The rest of the sections consist of questions regarding their experiences with scams, the techniques they are aware of to protect themselves from scams and their awareness of the safeguards available to them [POV 1].

For secondary stakeholders, we recruited individuals who are associated with either financial institutions or e-commerce companies. The first two sections of the form inform the participants about the aim of the study and ask for their consent. The rest of the sections consist of questions regarding the support their institutions/companies offer the customers to protect them from scams and how frequent the problem is [POV 2].

* We first conducted the primary and secondary stakeholder interviews. We created the questionnaire after discussing the findings from those interviews. The methods were carried out in this order because we would be able to focus on the questions that are significant to the target audience. We also wanted our stakeholders to feel comfortable sharing their ideas and details. The interviews helped us realize what kind of questions would be appropriate to ask the stakeholders.

The order of our data-gathering methods helped us improve the quality of our questions

and the stakeholders’ participation experience.

## KEY FINDINGS

1. **Scam Waves:** Through an interview with our expert in the fraud department, we uncovered a significant trend in online scams. Scams tend to come in waves, where a large number of people are targeted by similar types of scams, with varying methods of execution. For instance, during one period, a wave of scams may focus on impersonating online retailers, while another wave may involve phishing attacks. This iterative pattern of scamming can confuse individuals who are not up to date with the latest scamming practices and fall victim to such scams.

***Significance:*** The discovery of scam waves and the constant evolution of scam tactics is significant for several reasons. First, the change in scams explains why many individuals fall victim to these scams. Scammers adapt their strategies to take advantage of vulnerabilities in people's awareness and understanding of current scam tactics.

1. **Confusion and Targeting:** The iterative nature of scam plans initiates mass confusion among victims, especially among frequent online shoppers. As online scams continue to evolve, they take on new forms and disguise themselves under different guises. These ever-changing tactics lead to a lack of awareness and preparedness among potential victims.

***Significance:*** The confusion experienced by individuals due to the iterative and constantly evolving scam tactics is significant because it highlights the psychological aspects of online scams. Scammers use tactics that prey on people's lack of awareness about current scams, leading to misplaced trust and ultimately victimization. Understanding this psychological component is crucial for devising effective prevention and awareness strategies.  
*Design Implications:* This finding underscores the need for user-friendly interfaces, educational resources, and awareness campaigns that are continuously updated to reflect the latest scam tactics. Designing user interfaces

1. **Personalized Scams:** Through our interview with primary stakeholders and questionnaire with primary and secondary stakeholders, we discovered that most scammers try to gain the trust of the victim by providing them with their personal details. This would occur as a result of a scammer obtaining an individual's phone number or email address and then their name and other relevant information. Then they would piece up the information together to create a convincing scam story that someone can easily fall for as obtained by our primary stakeholder interview. They try to pose as legitimate individuals or institutions and make the victim believe that they know them very well. Most of these scams are carried out in the form of calls. For e.g., Scammer A would call victim B and tell them that their name is B, they work as a teacher and live in Toronto. This would make B feel that since A knows their details, they must be legitimate individuals/institutions.

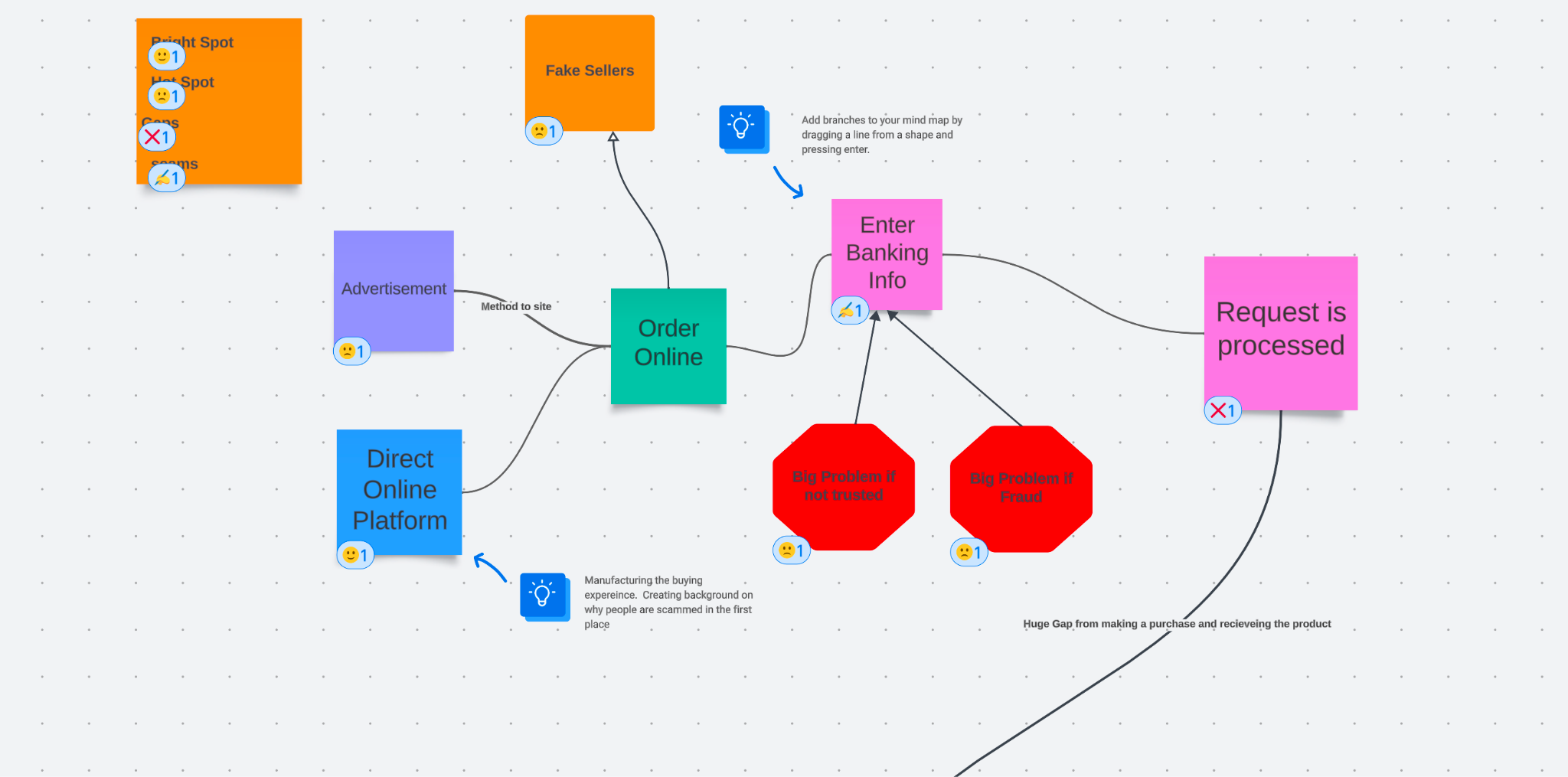
***Significance:*** This discovery is significant because it raises the question - “How do the scammers know our personal details so well?”. We reveal our personal details like name, phone no., email ID, etc., quite frequently and on various occasions. It has become so common for us that we do not pause to think about our privacy. We have become socially engineered to think that our personal information can easily be shared with others and has no right to protection or privacy.

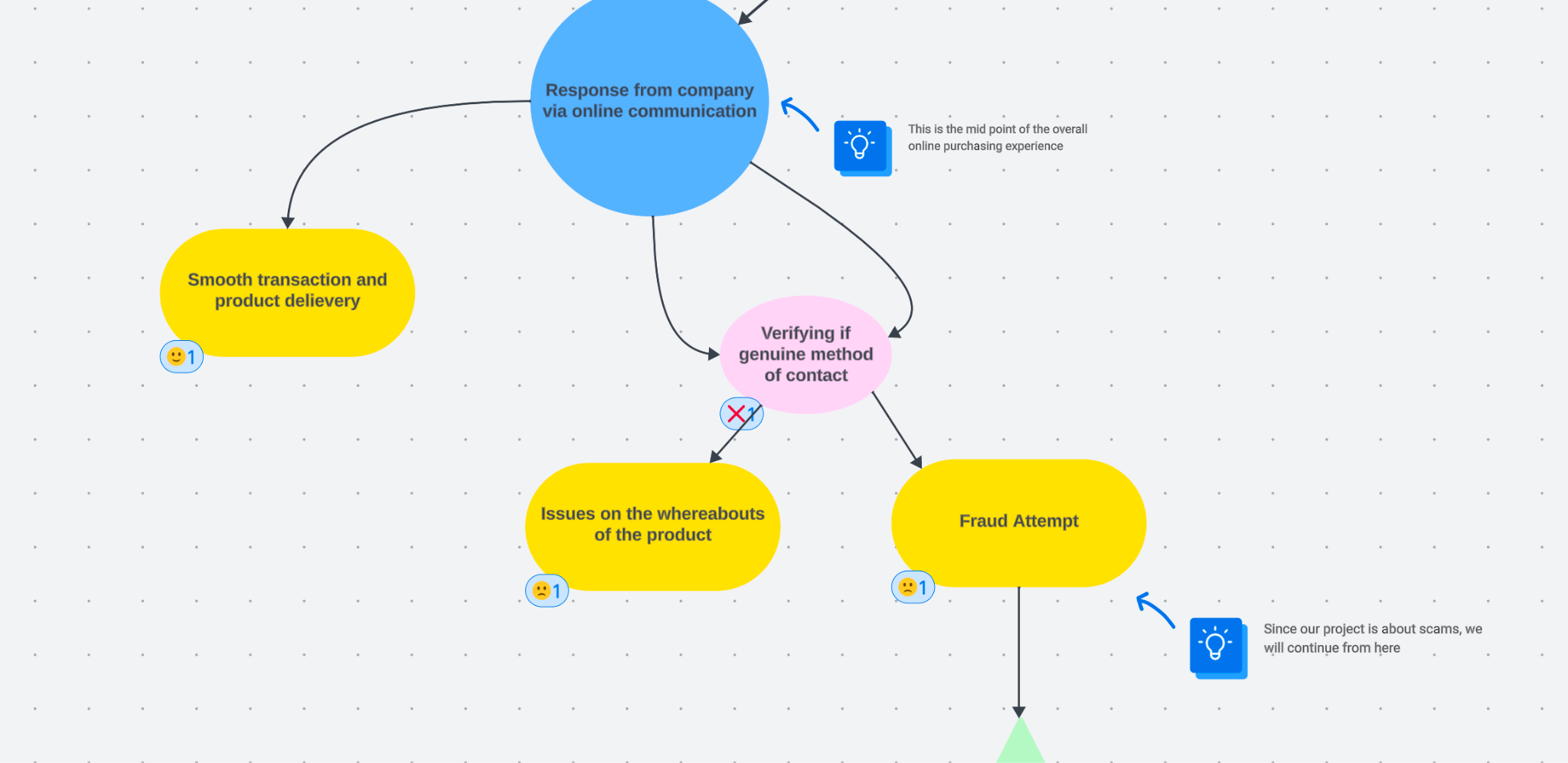
1. **Unawareness regarding available support and safeguards:** Through our interview with our primary stakeholders, we discovered that a majority of them are not aware or have little knowledge about their financial institution’s policies and the support they offer in the event of scams.

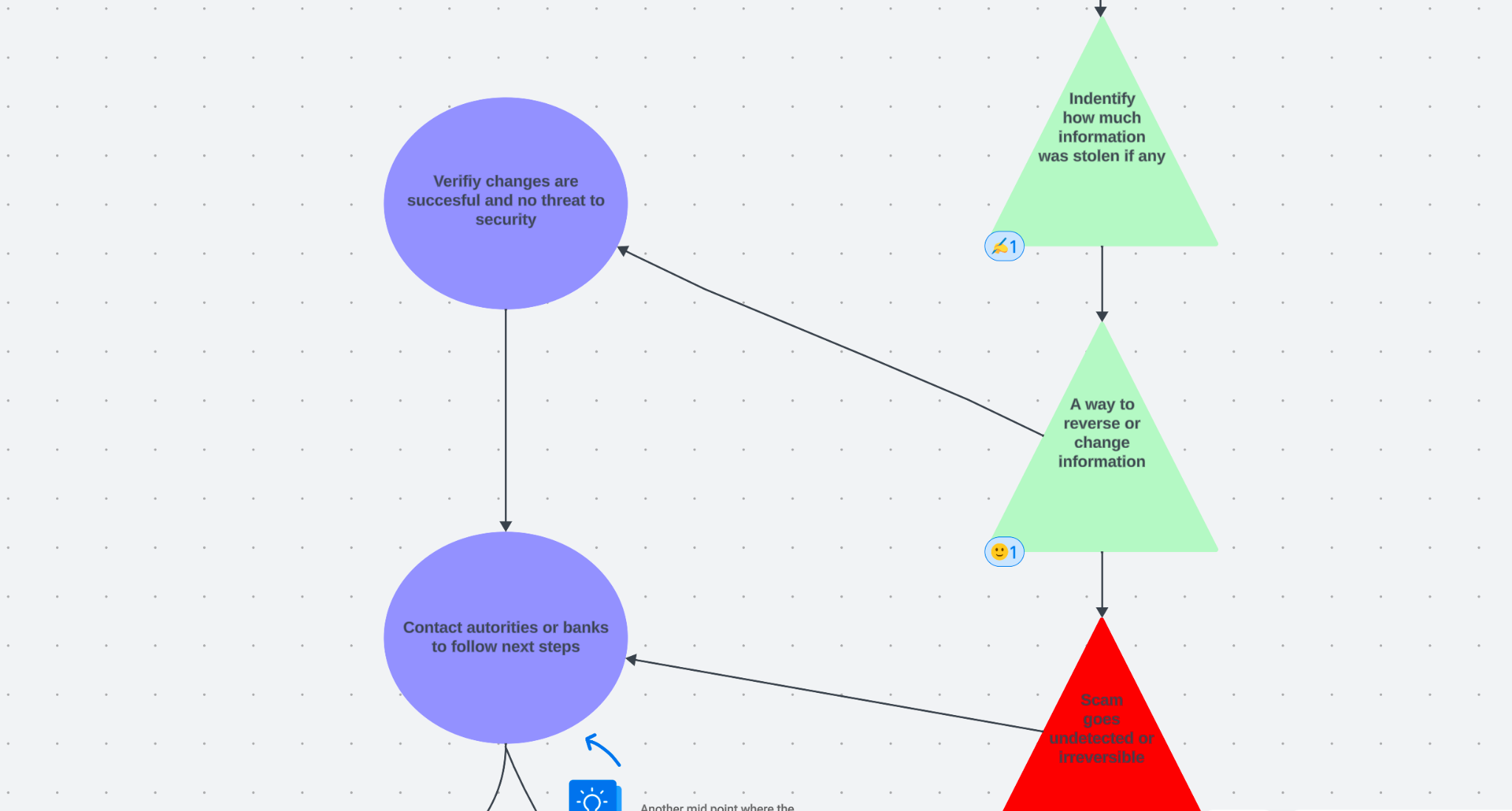
***Significance:*** This is a serious cause of concern as victims do not know what to do after they have been scammed or it is simply too late. They are affected both financially and psychologically as they feel helpless after losing their funds. This affects their trust in the financial institutions as well, which further affects the institutions’ brand image.

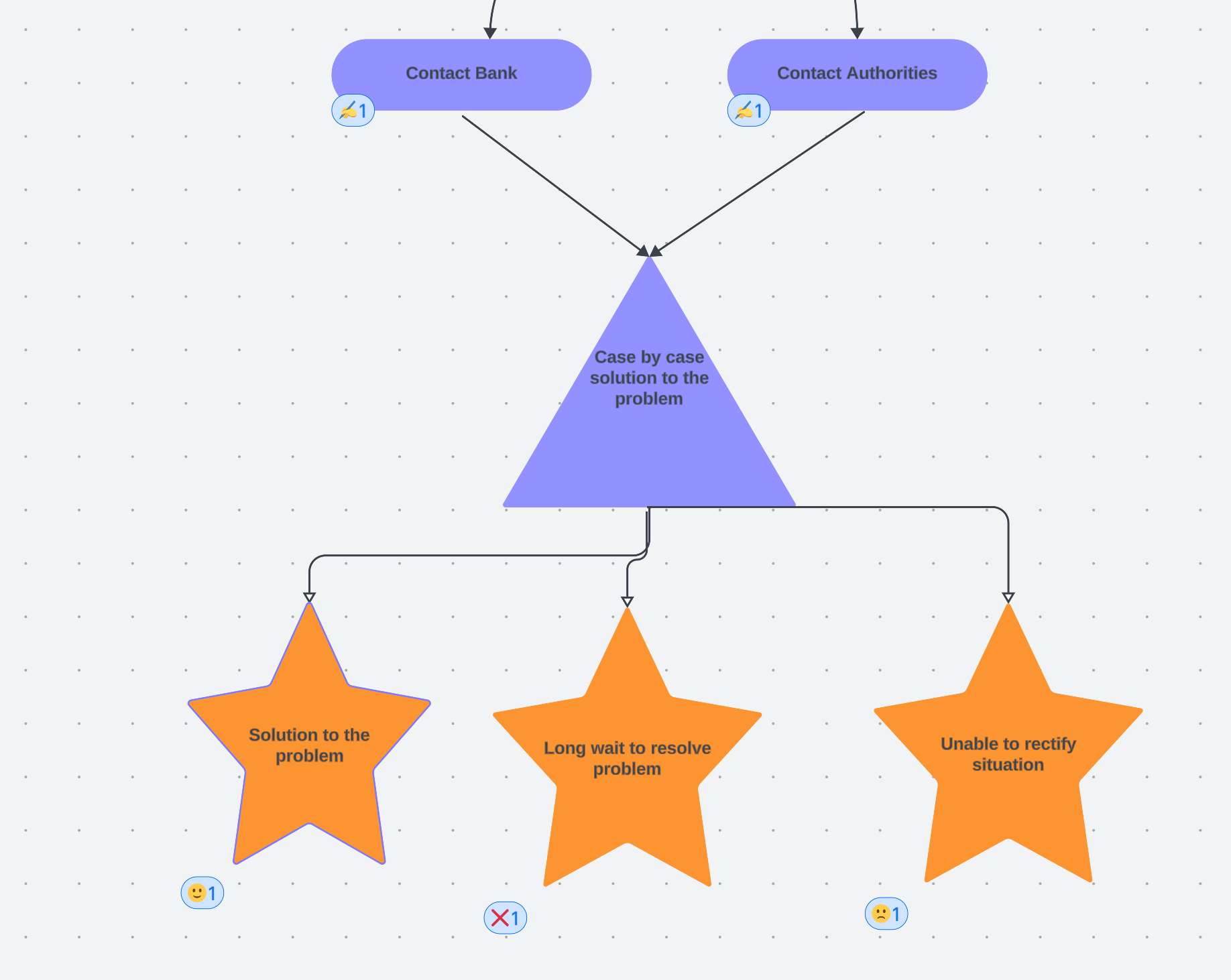
# CHAPTER 3:

# EXPERIENCE MAP

****

****

****



**Experience Map Link:** <https://lucid.app/lucidspark/9fd06abe-7e6d-4efb-8ddc-e5325dbe5910/edit?viewport_loc=-720%2C3857%2C2893%2C1648%2C0_0&invitationId=inv_cb7c13b3-87cb-477d-a9bc-bed427b8a2c>

# CHAPTER 4:

# JOB STORIES

## Job Story 1

When I am making an online purchase, I want to ensure that my credit card information is encrypted and secure, so I can feel safe putting in my information.

***Motivation and purpose:*** Ensuring that online platforms encrypt all personal and financial information of their customers is vital to maintaining a secure shopping experience. Consumers have the right to protect and hide their sensitive financial information and personal information from potential identity thieves and scammers.

## Job Story 2

When I am buying products online, I want to authenticate the seller, so I can buy genuine and good quality products.

***Motivation and purpose:*** Buyers should be able to verify whether the seller they are buying from actually exists or not. This reduces the odds of fake products and deliveries. E-commerce sites should be aware of the sellers and the advertisements that are allowed on their platforms.

## Job Story 3

When I receive a call/message from an unknown number, I want to be able to identify the caller/sender, so I can avoid impostors.

***Motivation and purpose:*** Unknown calls and texts can cause confusion. We want to ignore them as they might be from scammers but they could be from genuine sources as well. People should be able to identify and differentiate between the two so they can avoid scams and not miss important calls/messages.

## Job Story 4

When I am using multiple e-commerce platforms, I want to create strong and unique passwords for each, so I can reduce the risk of having my accounts hacked into.

***Motivation and purpose:*** While it is much easier to remember the same password and use it across multiple platforms, it is actually a very unsafe practice. It makes your account and identity prone to theft and fraudulent activity especially if an e-commerce platform gets cyber-attacked. Therefore, it is important that users take measures to protect themselves.

## Job Story 5

When I find a great deal (in the form of advertisements) on product prices, I want to inquire about the deal with the e-commerce company, so I can be sure that it is a safe investment.

***Motivation and purpose:*** Many times buyers see a very lucrative deal on a trustworthy site and buy the product. However, these ads might be from malicious sellers/hackers who just want to steal your information. Hence, it is important that the buyers are able to verify whether a sale or a deal visible on the e-commerce site is genuine or not.

# CHAPTER 5:

# DESIGN REQUIREMENTS

## Design Requirement 1:

Identify secure and legitimate phone numbers and email addresses and flag those that are fraudulent.

***Motivation and purpose:*** The identification of phone numbers and email addresses still heavily relies on users doing their own research. Hence, automatically identifying fraudulent phone numbers and email addresses makes it easier to avoid scam calls and emails from the very beginning. This saves users the hassle of manually checking whether a phone number or email address is legitimate or not.

## Design Requirement 2:

Keep people updated with the latest information about bank and e-commerce policies and any widespread scams that they should look out for.

***Motivation and purpose:*** Many vulnerable populations such as the elderly and newcomers are the most prone to scams. Therefore, we want to ensure these populations are protected by providing updated information about bank and e-commerce policies they wouldn’t otherwise know. In addition, keeping people alert to what kinds of scams are being used the most helps protect most people.

## Design Requirement 3:

Provide a psychological helpline for people who have been scammed and suffered big losses.

***Motivation and purpose:*** Most people who fall for scams find themselves in a lonely position with no one they can go to. A psychological help line would therefore provide people with a support system they wouldn’t otherwise have. Such a support system will help reduce negative emotions and prevent them from manifesting into something worse.

## Design Requirement 4:

Automatically detects a transaction scam and blocks it by alerting your banking institution.

***Motivation and purpose:*** Retrieving your money after a transaction scam is usually a long process. At times, there can also be no guarantee that you are going to get your money back. Instead of allowing a scam to occur in the first place, automatic detection of it will save users a lot of time and hassle.

## Design Requirement 5:

Verifies whether an e-commerce website is safe and legitimate to use or not by scanning for any fraudulent activity and user reviews.

***Motivation and purpose:*** Users usually need to manually check whether a website is safe and legitimate by searching for other people’s reviews. Even then there’s no guarantee that the website is 100% legitimate. Hence, verifying that a website is secure and legitimate allows users to feel safe while using the website.

# 

# 

# APPENDICES

1. **FIELD STUDY PROTOCOLS**
2. **Project** **Title**: Securing Privacy and Preventing Scams during Online Purchases
3. **Investigators**: Team Vulcan
4. **Purpose**: The purpose of our research is to understand how individuals fall victim to online scams to help us derive requirements for the design of novel interactive computational media that are intended to be useful to online shoppers. A brief description of our design problem is: Many users are sent scam or fraud inquiries through online sources. Millions fall victim to these online scams and millions of dollars are stolen. We want to find a solution and end online scams.
5. **Process to be followed**: We will brief the participants about the purpose of the study, explain the consent form to them, and ensure that they sign the consent form. We will then engage the participants in a 30-minute semi-structured interview. We will also, with their permission, make observations as follows: The insight provided on a phone interview will be used to make observations on what trends and patterns are followed by scam artists.
6. **Participant selection:** Participants will be chosen from their experience with dealing with fraud cases. They will be identified via personal network connections and selected according to their years of experience dealing with these types of problems. In general, they will be characterized by their occupation and work experience in any fraud department.
7. **Relationships**: The participants recruited for our study consist of family members, friends and professional connections.
8. **Risk and benefit:** There will be minimal risk to the participants, for example, that they feel that they have wasted their time. The only benefit will be to contribute to the education of the investigators. Participants are free to withdraw before or at any time during the study without the need to give any explanation.
9. **Consent details**: We will brief the participants about the purpose of the study, explain the attached consent form to them, and ensure that they consent to participate and sign the consent form (see section II of Appendices).
10. **Compensation**: Participants will receive no compensation.
11. **Confidentiality**: Information will be kept confidential by the investigators. Names or other identifying or identified information will not be kept with the data. The only other use will be to include excerpts or copies in the assignment submitted, but names and other identifying or identified information will not be submitted.

**II. CONSENT FORMS**

1. **For Interviews**

**Consent Form: Securing Privacy and Preventing Scams during Online Purchases**

I hereby consent to participate in a research study conducted by Team Vulcan for an assignment in University of Toronto Computer Science 318, *Design of Interactive Computational Media*.

I agree to participate in this study, the purpose of which is In this study, we aim to find ways to prevent and reduce online purchase scams and their effects on our stakeholders. We also want to find ways to secure online privacy for them.

I understand that

* The procedures to be used are interviews and questionnaires. We will give a brief explanation of the goal of the research. The participants will be asked to answer questions related to online shopping experiences, scams and safeguards available to them. The whole session will not be recorded. \*
* I will receive no compensation for my participation.
* I am free to withdraw before or at any time during the study without the need to give any explanation.
* All materials and results will be kept confidential, and, in particular, my name and any identifying information will not be associated with the data.

**PARTICIPANT**

Name (please print)

Signature

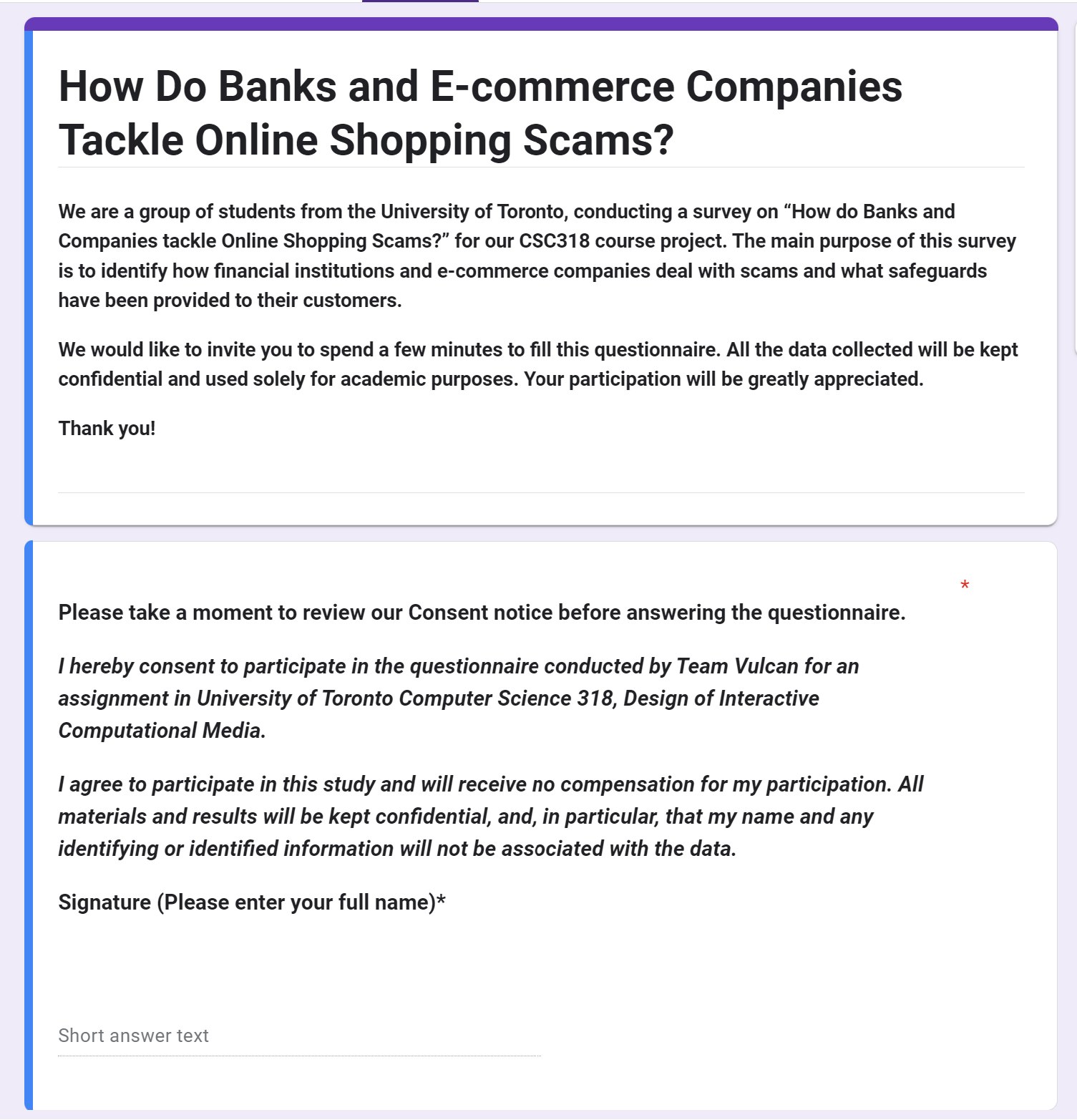
Date

**INVESTIGATOR(s)**

Name Signature

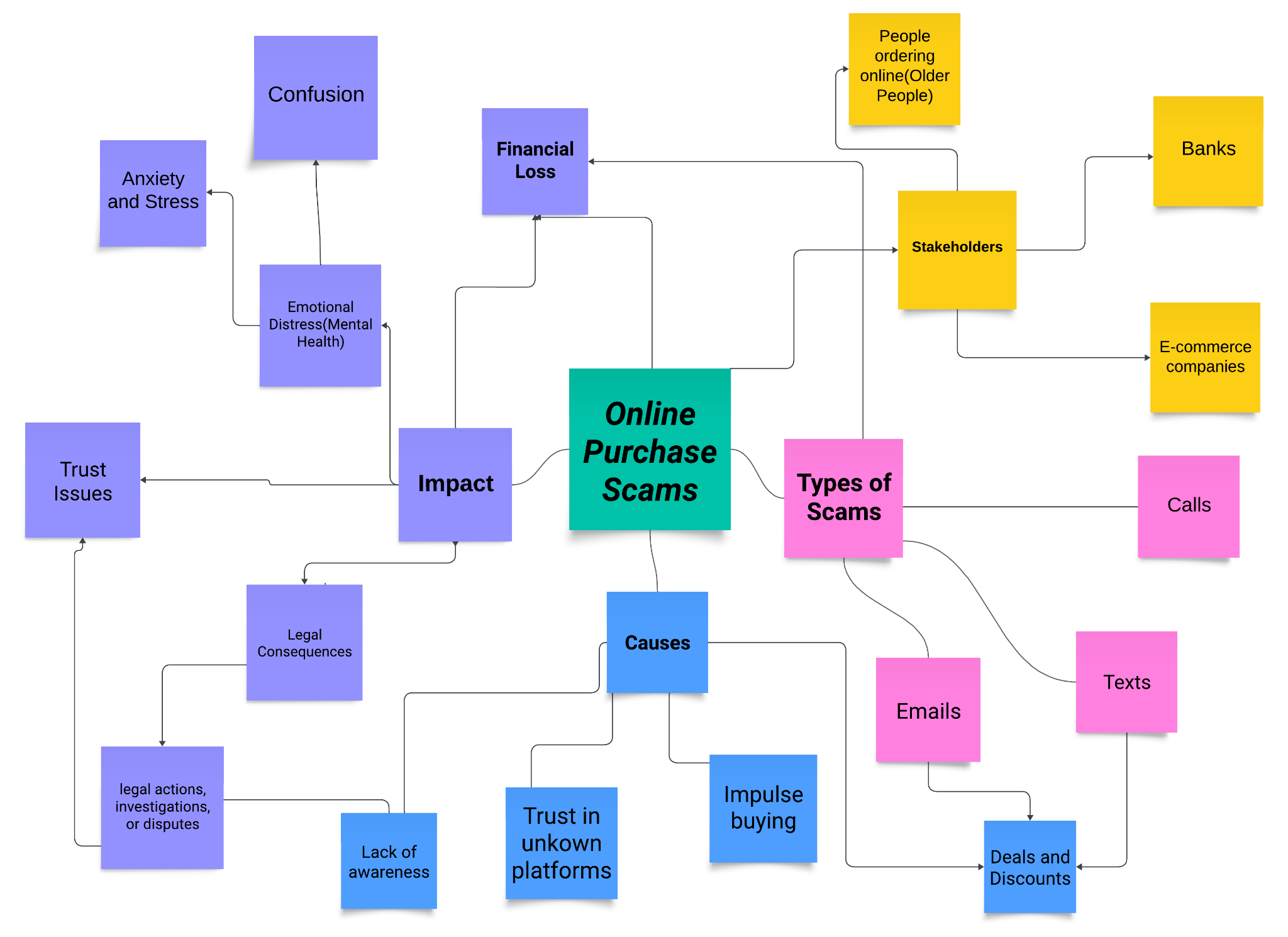
\*in the case of the primary stakeholder interview consent form, the last sentence of this clause is changed to “This whole session will be recorded”.

1. **For Questionnaires**



**III. DOCUMENTATION OF THE PROCESS**

**Mind Map**



**Complete POV statements**

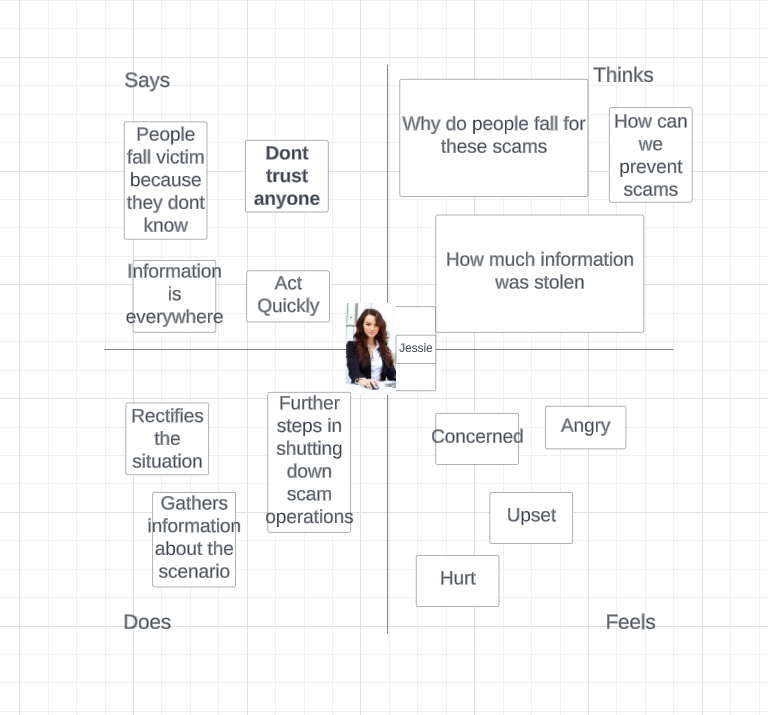
1. Shoppers need to be able to protect their information during online transactions so that their details are not misused later on.
2. E-commerce companies need to be able to authenticate their sellers so that customers are not deceived/scammed.
3. People need to be able to verify the website they are buying for a secure connection (HTTPS) so that the legitimacy of the website is ensured.
4. Customers need to exercise caution when encountering deals that are too good to be true and avoid impulsive purchases.
5. People need to ensure that the company contact is safe and legitimate so that no information can be stolen.
6. Everyone needs to learn about the most current type of scam so that they can be vigilant and prevent being scammed

**Incomplete POV statements**

1. Shoppers need to be able to identify scam calls and texts, because ??
2. Financial institutions need to ??, so that their customers are aware of the support available in case of scams.
3. Elders are commonly more prone to falling for scams, because ??
4. Scammers are able to easily find our personal information online, because ??
5. The victims need to ?? so that they don’t fall for these schemes again.

**Empathy maps**

**Primary Stakeholders**

**Secondary Stakeholders**

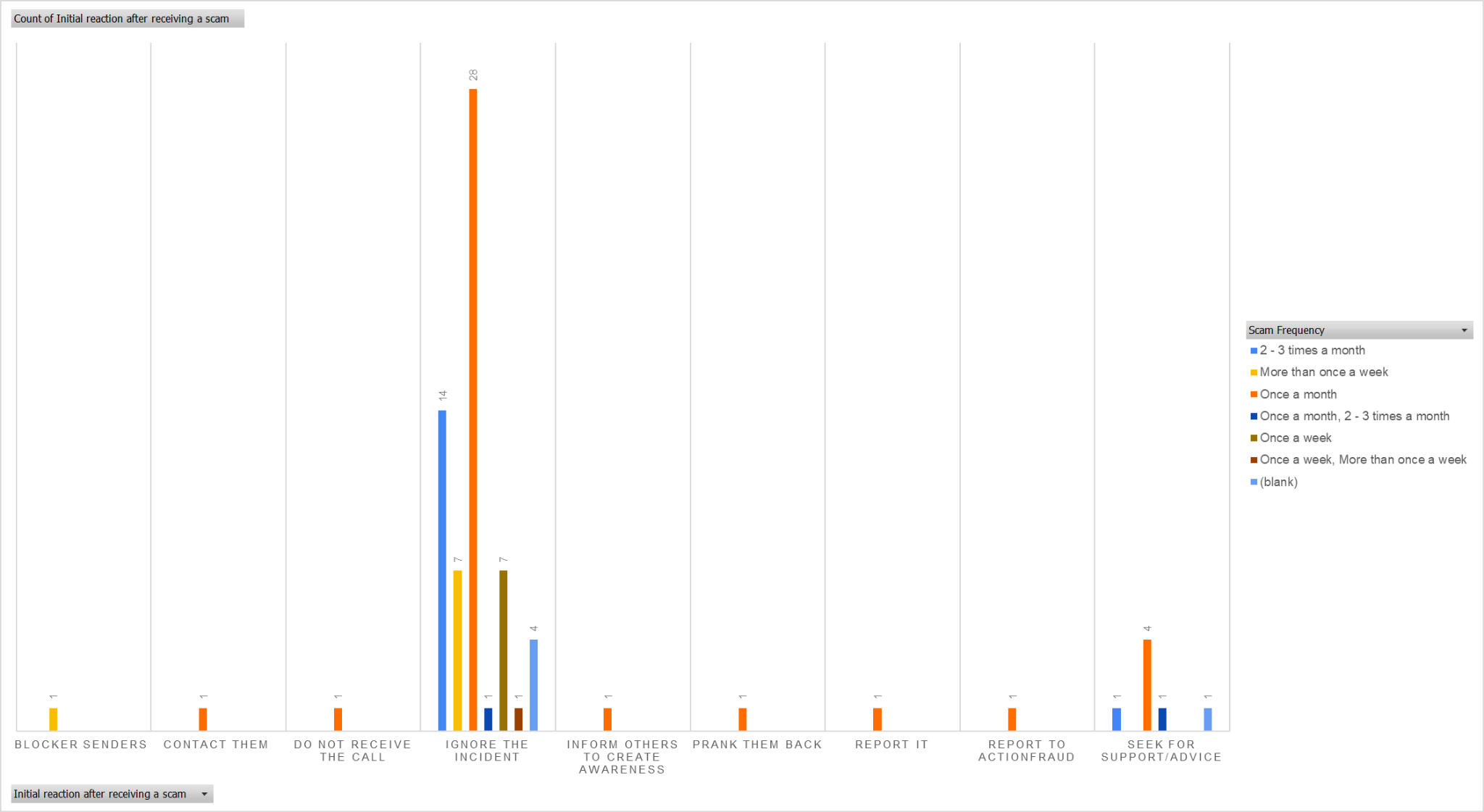
**Data Analysis documentation**

* **Relation between Type of Scams, Age, and Spending**

****

* From the graph, we can learn that people aged 16-30 are frequently targeted by scams either by text, call or email. We believe this is due to the technology proficiency this age group has as most of them are techno-savvy. Thus, as the scams occur through digital technology, they become the biggest target victims. The graph also indicates that bigger spending doesn’t necessarily mean you will be targeted more often by scammers.

**Figure 1.2. People’s Initial Reaction and The Frequency of Scam**

****

* From the graph, we can learn that more than 50% of the respondents ignored the incident but still experienced the scam more than once a month. This frequency tells us that ignoring the incident might not be enough to stop the attacks since our respondents are still being attacked after ignoring the text, email, or call. It might be better to not pick up the call, email or text.

**IV. RESEARCH INSTRUMENTS**

1. INTERVIEWS

**Primary Stakeholder:** Person that has been scammed

**Background Information:**

1. Can you briefly describe the online scam incident you encountered, without revealing any sensitive information?
2. What type of online platform were you using during the incident (e.g., online marketplace, social media, banking website)?
3. What methods did the scammer use to contact you?

**Experience during the Online Transaction:**

1. Can you walk me through the steps of the online transaction/activity you were attempting to perform?
2. Were there any specific difficulties or confusion you encountered during the process?
3. Did you notice any unusual or unexpected behaviour on the website or app you were using?

**Trust and Credibility:**

1. What factors influenced your trust in the website or seller involved in the transaction?

**Emotional Aspect:**

1. How did they capture your interest to make a transaction?
2. How did the incident make you feel emotionally (e.g., angry, embarrassed, anxious)?

**Suggestions for Improvement:**

1. In your opinion, what could the online platform or website have done differently to prevent this scam?

**Secondary Stakeholder: Person working in the FinTech Industry.**

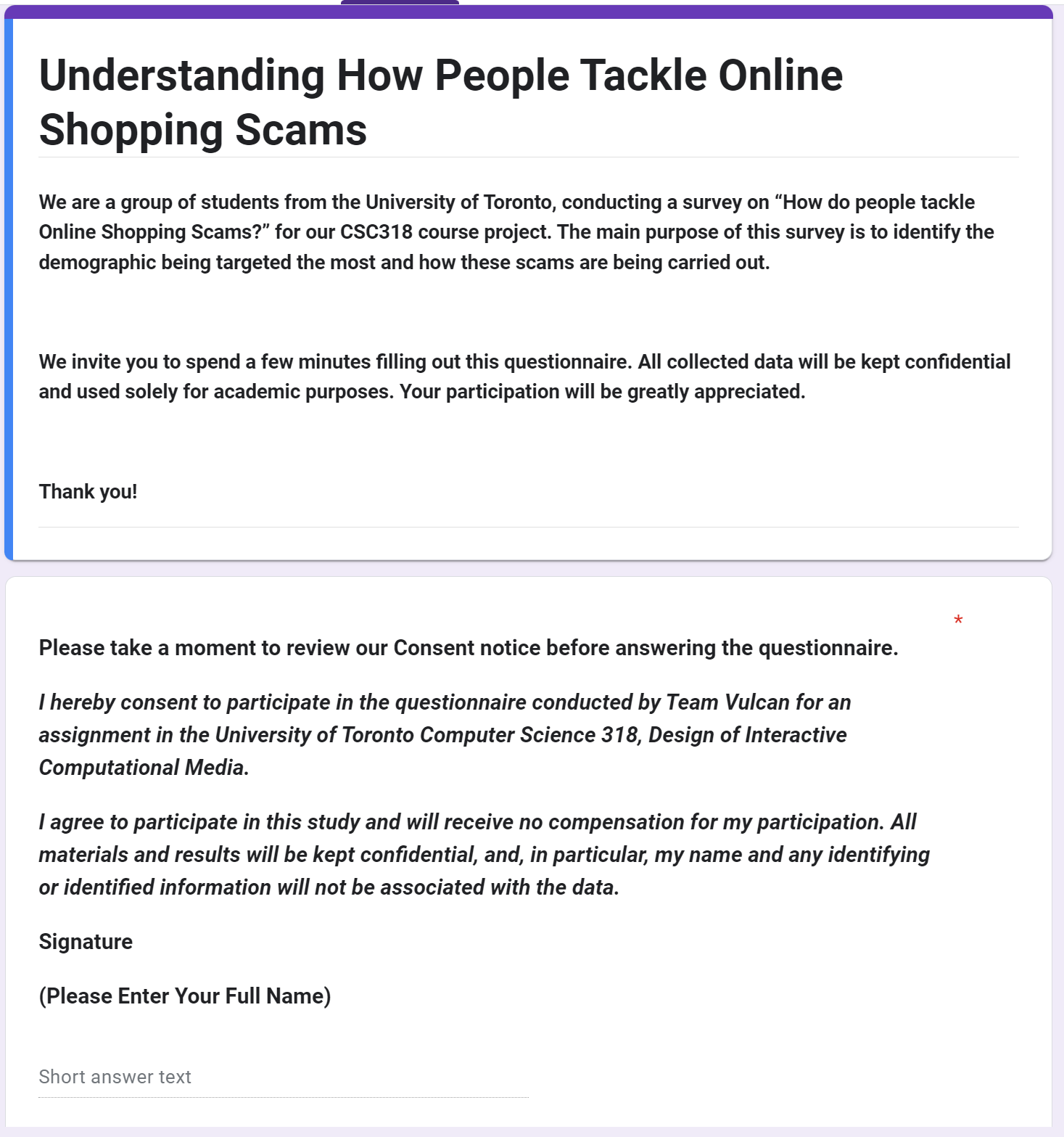
1. Through your work, what goes into ensuring a transaction is safe and credible?
2. What is the fintech industry doing to tackle scammers who are increasing by the day?
3. What advice do you have for people who receive fraudulent links and text messages?
4. How are you ensuring that people’s personal information is protected?
5. Why is it hard to tackle scammers despite all the security measures set up by the industry?
6. Please walk me through what it takes for someone to regain their money after a scam
7. What type of information is most prone to theft and how can one protect themselves from it?
8. Elderly people happen to be the most prone to scams and fraud, how can they protect themselves?
9. Are there any regulations that make it hard to tackle this issue?
10. How can regulating bodies help tackle this issue?
11. As someone who works in the industry, what measures are you taking to protect yourself?

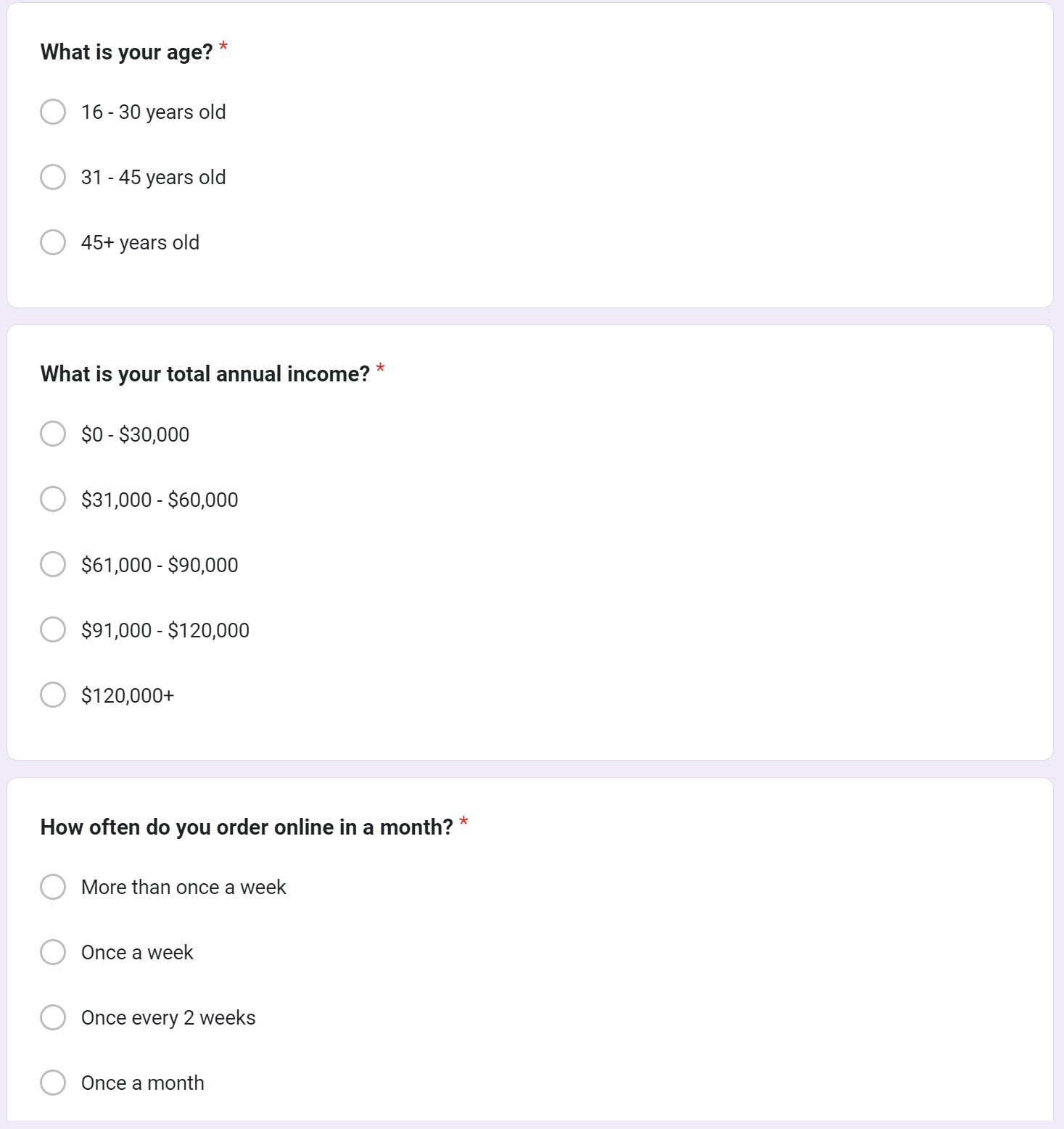
**Secondary Stakeholder: A person working in banking.**

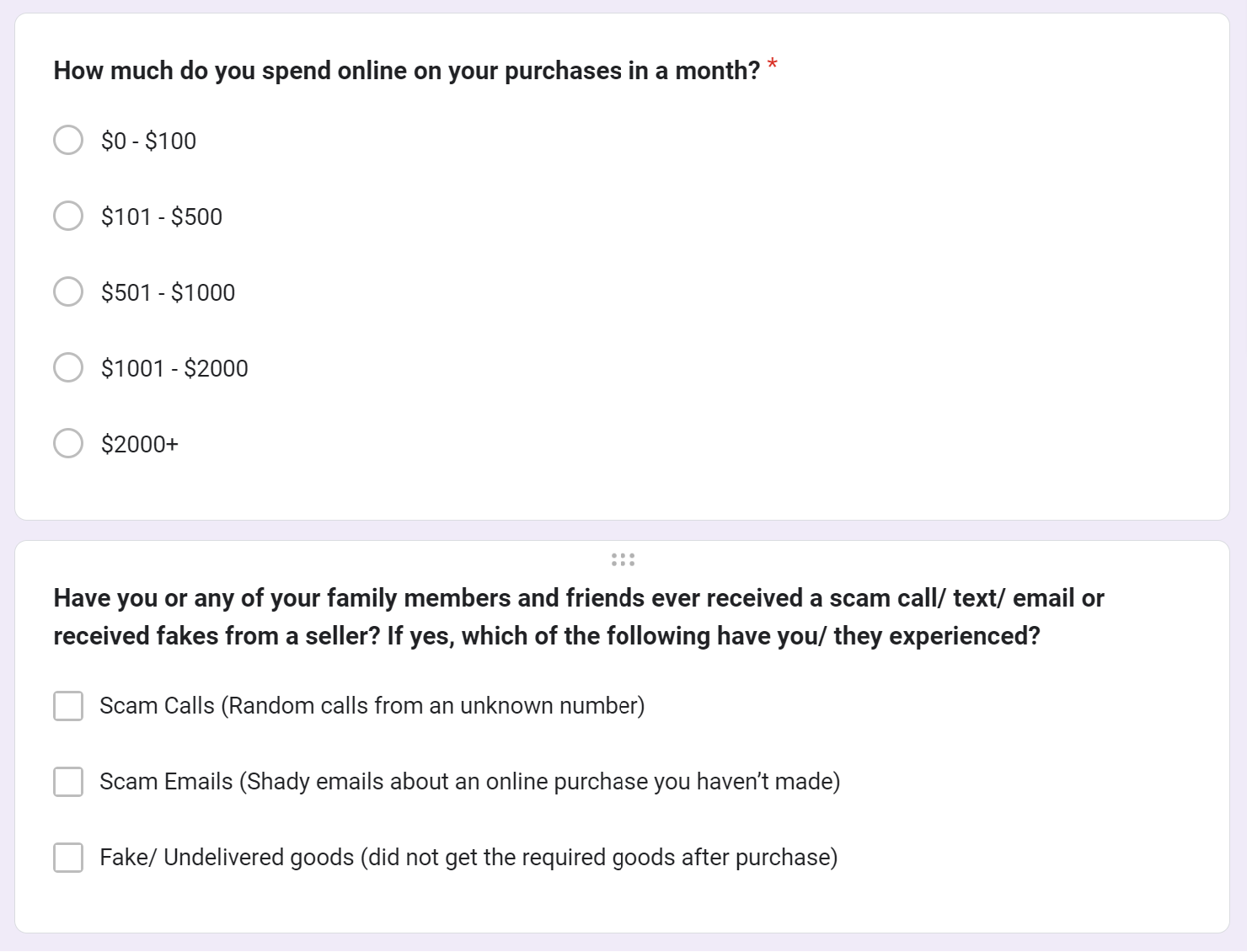
1. Through your work, what goes into ensuring a transaction is safe and credible?
2. What is the banking industry doing to tackle scammers who are increasing by the day?
3. What advice do you have for people who receive fraudulent links and text messages?
4. How are you ensuring that people’s personal information is protected?
5. Why is it hard to tackle scammers despite all the security measures set up by the industry?
6. Is there a way to reverse the effects of a scam?
7. Are there patterns when it comes to the method of scamming?
8. Please walk me through what it takes for someone to regain their money after a scam
9. What type of information is most prone to theft and how can one protect themselves from it?
10. As someone who works in the industry, what measures are you taking to protect yourself?

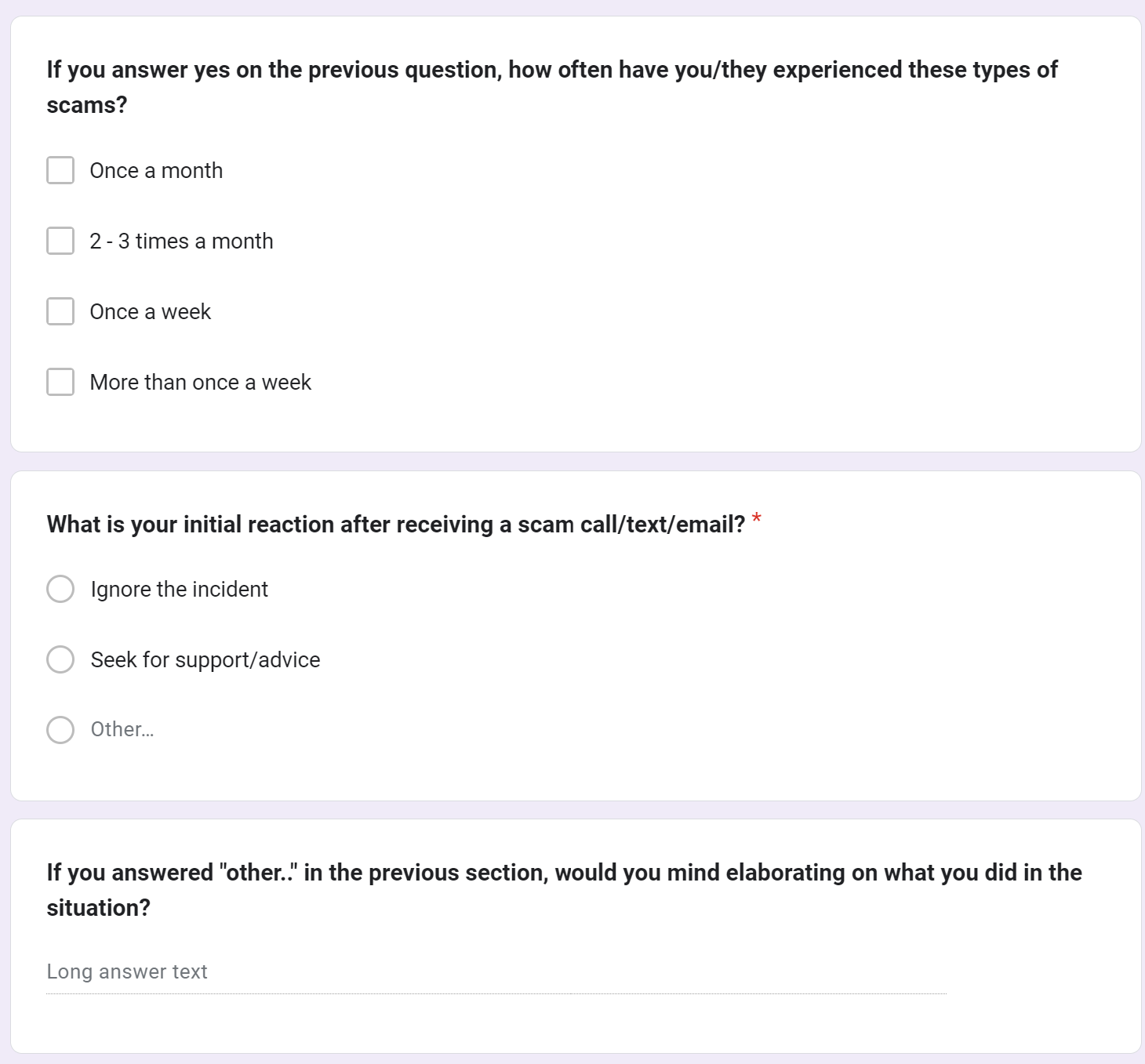
B. QUESTIONNAIRES

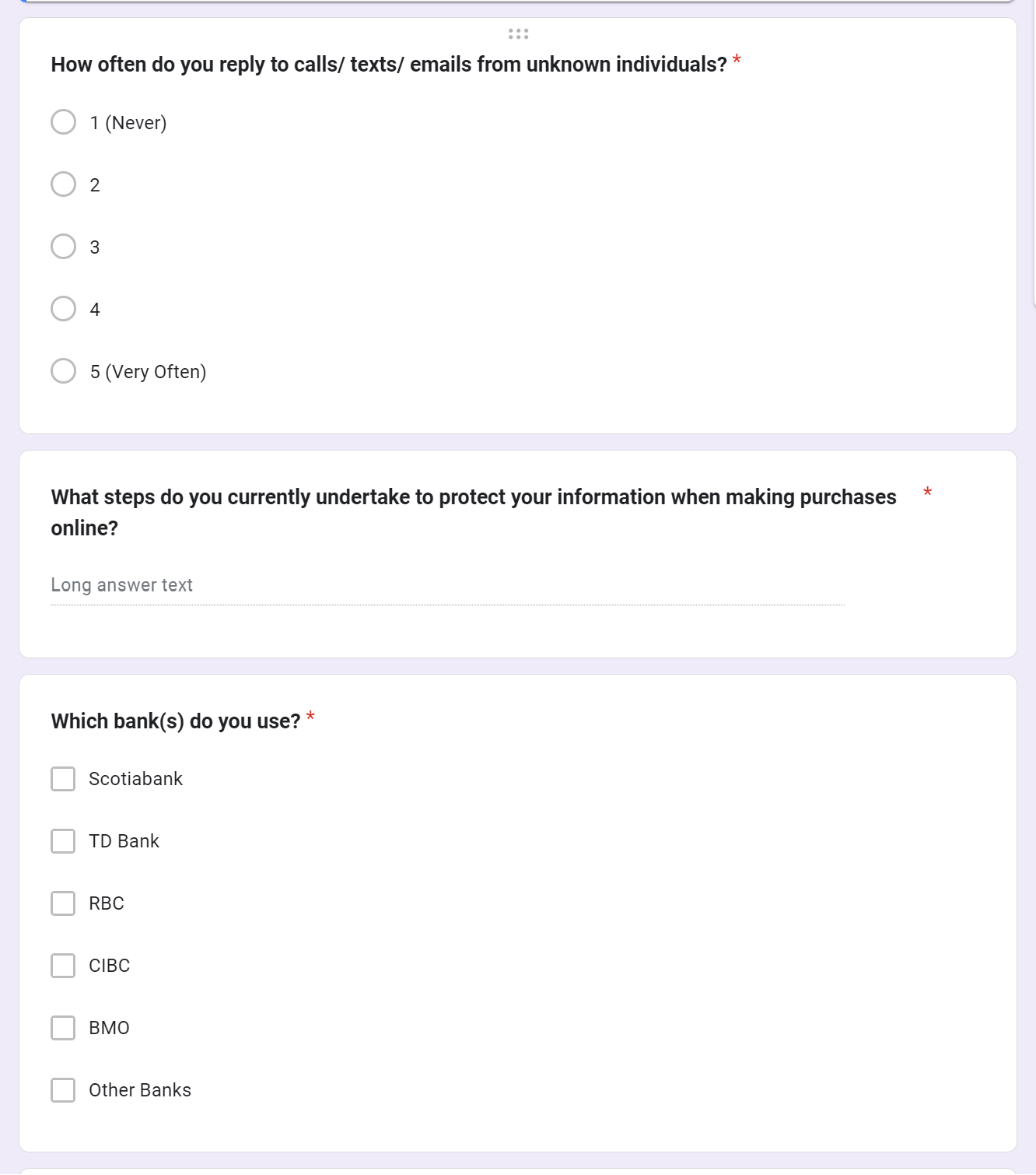
Figure 4.1. Primary Stakeholder Questionnaire Form



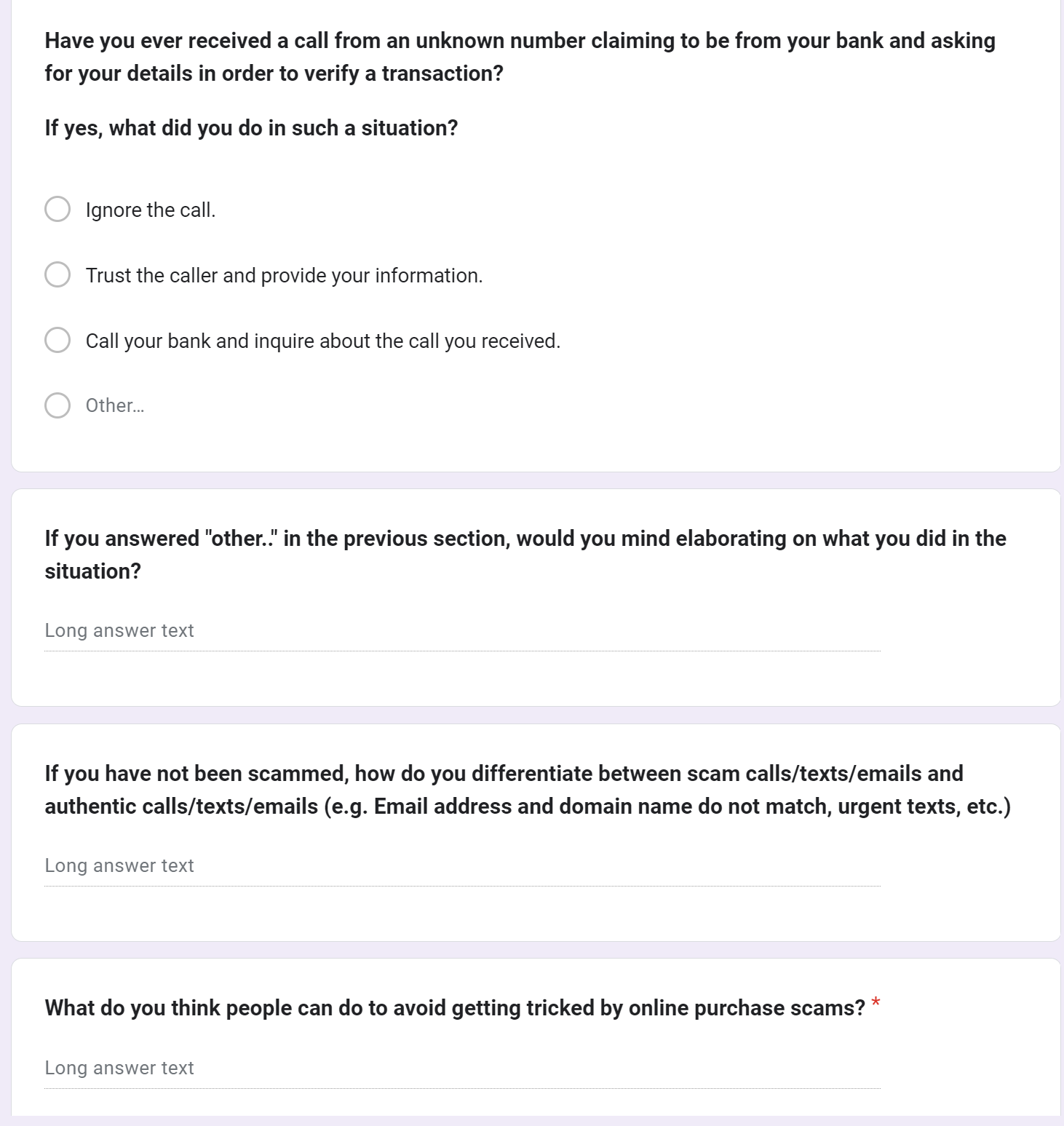








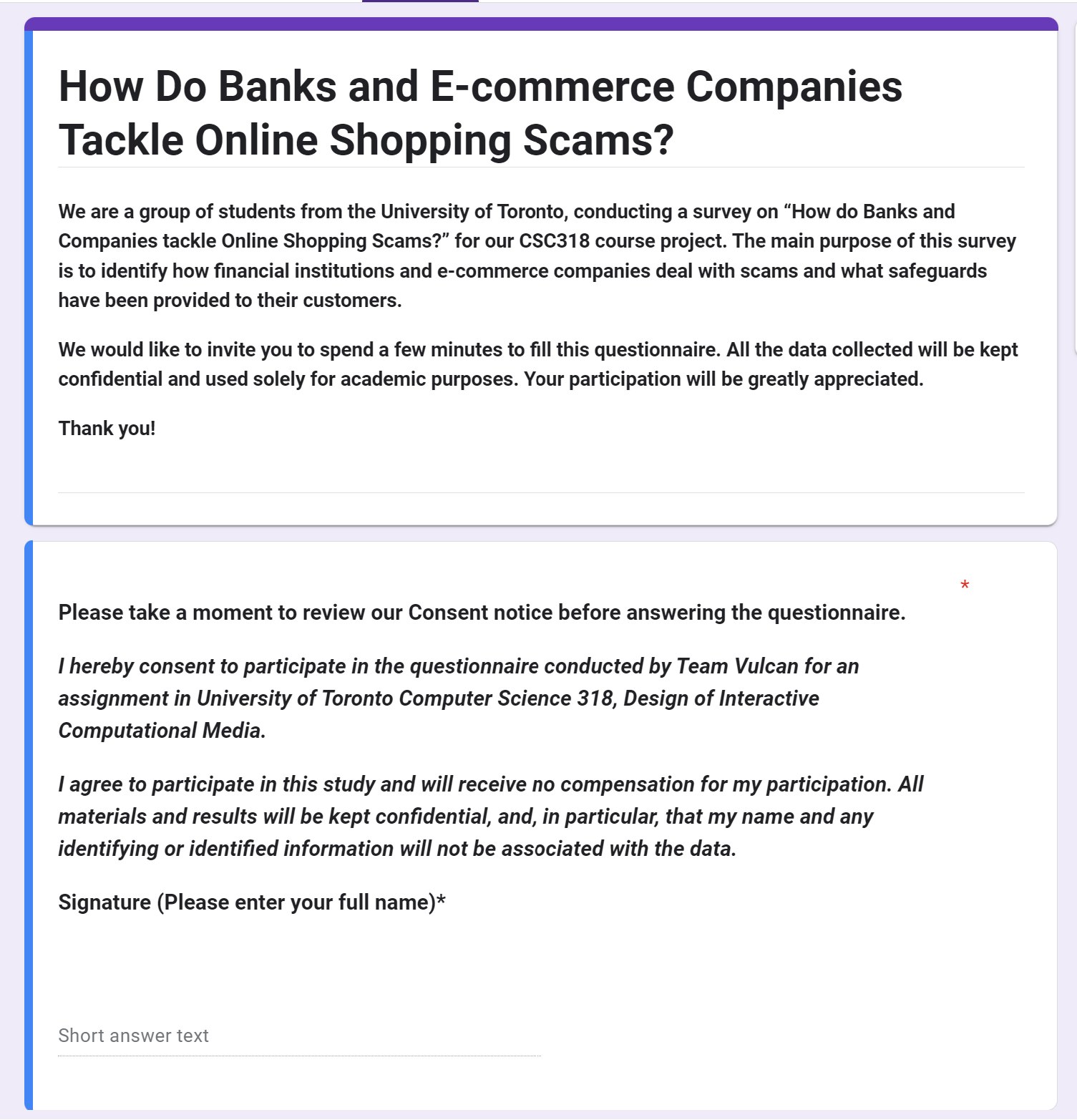


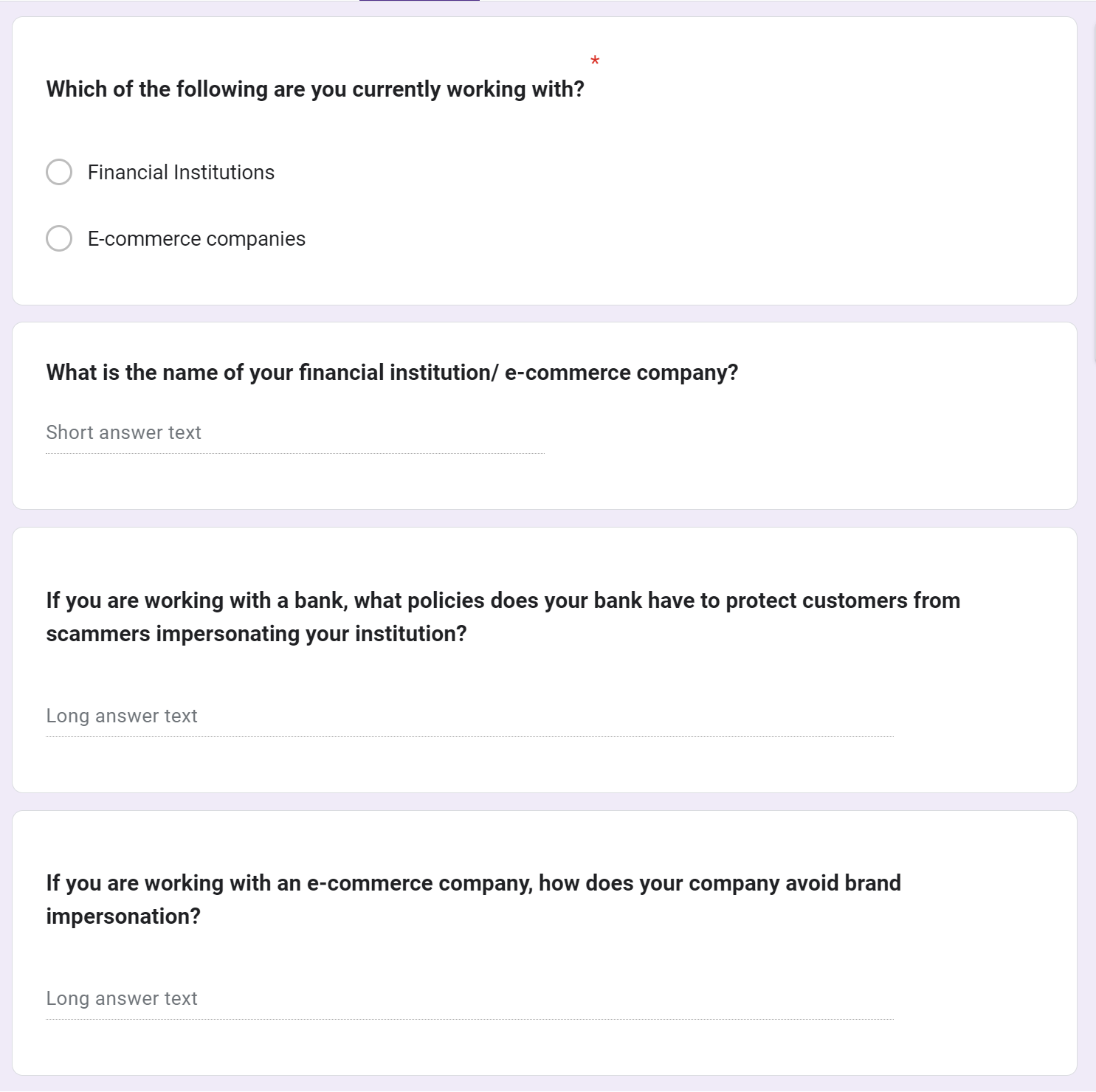


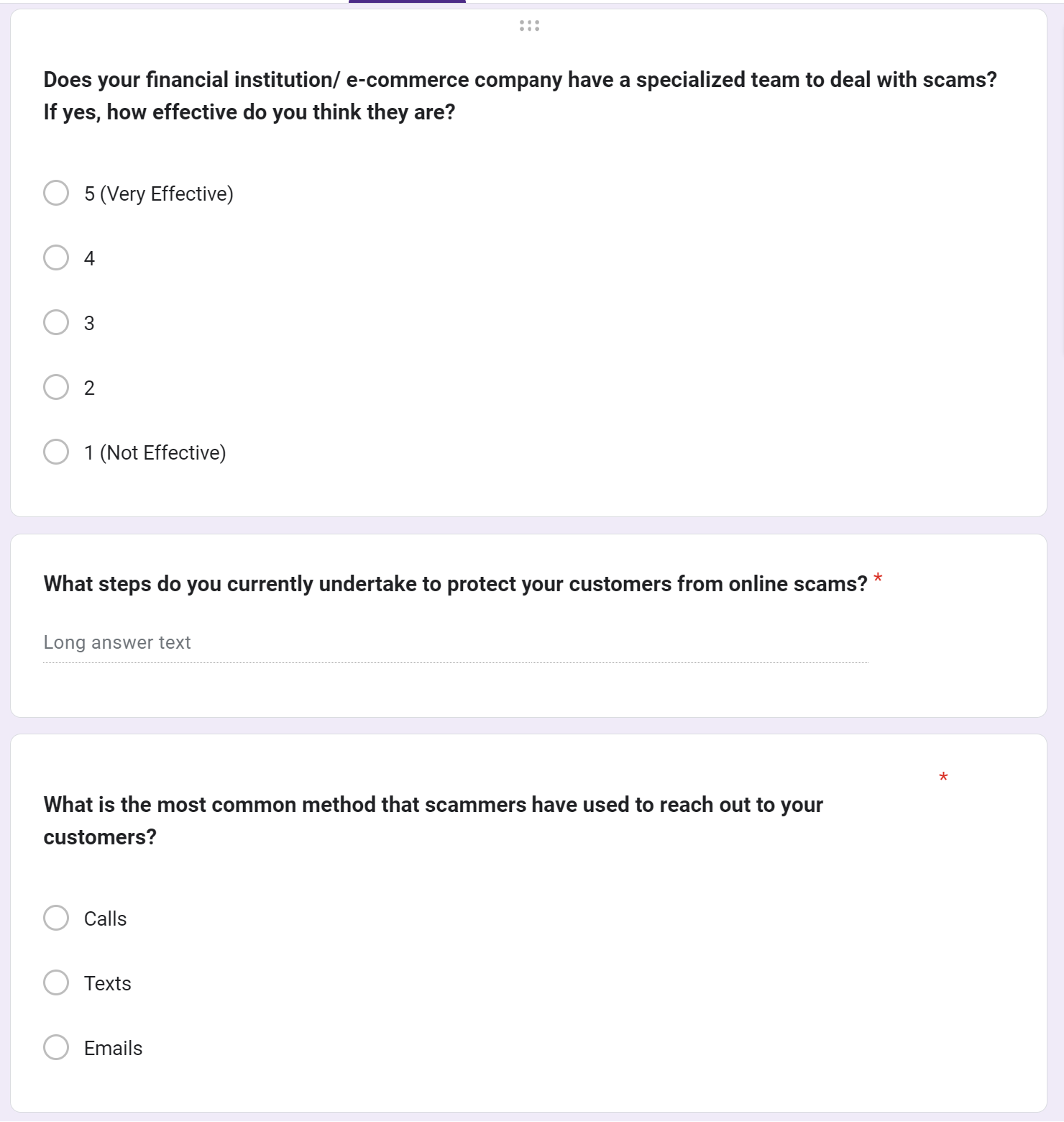
**Figure 4.2. Table of Questions and Reasons for the Primary Stakeholder Questionnaire**

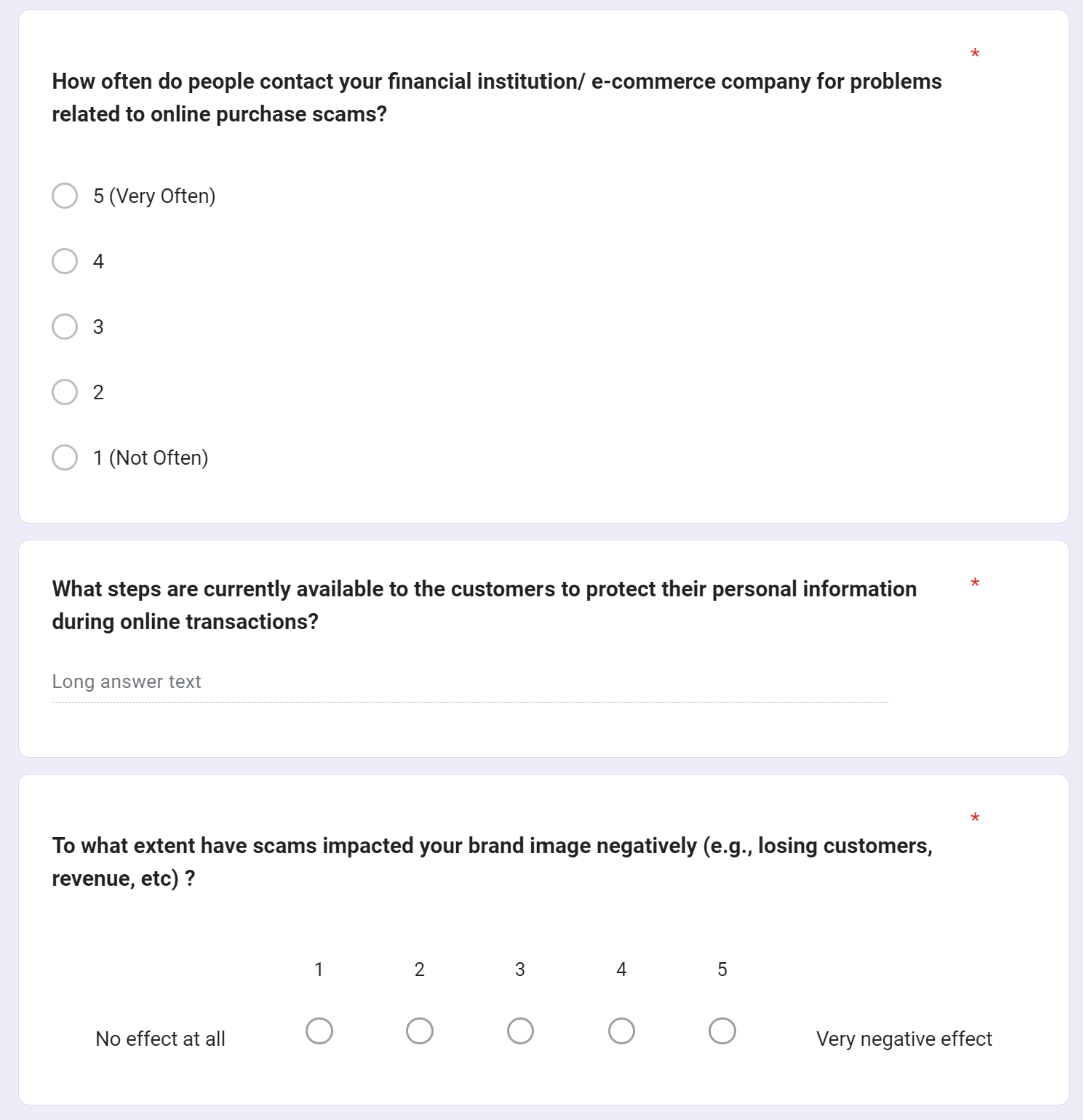
| QUESTIONS | REASONS |
| --- | --- |
| 1. What is your age? | Respondent's age is used to divide them into age groups. Different age groups may experience different types of online scams and develop new ways to avoid the scams. |
| 1. What is your total annual income? | We asked for the income range to know if someone in a lower range income might be targeted more often by the online scammers. |
| 1. How often do you order online in a month? | We want to test out our theory if people who shop more often would be more exposed to these online scams due to their frequency in using the online shopping platforms. |
| 1. How much do you spend online on your purchases in a month? | We would like to see if there is any correlation between spendings and vulnerability to scams. What this means is people who usually have lower spendings may be trying to save money, hence they might visit online shopping platforms that are more vulnerable to scams. |
| 1. Have you or any of your family members and friends ever received a scam call/ text/ email or received fakes from a seller? If yes, which of the following have you/ they experienced? | We try to classify the respondents based on their type of online scam experience and the frequency of them experiencing the scam. |
| 1. If you answer yes to the previous question, how often have you/they experienced these types of scams? | Knowing and understanding the frequency of the scams is crucial to determining which online scams we must prioritize to resolve first. |
| 1. What is your initial reaction after receiving a scam call/text/email? | We need to know how people initially react when experiencing a scam. Knowing this can help determine our method of tackling online shopping scam problems. |
| 1. How often do you reply to calls/ texts/ emails from unknown individuals? | We would like to know if there is any correlation between the frequency of picking up calls with the frequency of being scam-called. We have a theory that people who usually pick up scam calls, even without responding to them, will get scam calls more often. |
| 1. What steps do you currently undertake to protect your information on when to make purchases online? | By knowing the precautionary steps people take in handling online scams, we can decide whether we want to develop existing solutions or create new ones. |
| 1. Which bank(s) do you use? Are you aware of any form of support that your bank would provide in the event of an online scam? If yes, please elaborate. | Different banks have different steps to handle online scams. Usually, after experiencing a scam, people tend to contact their banks to ask for support/advice. By knowing what kind of support banks generally do, we can use the information to focus on methods for preventing the scam from ever happening. |
| 1. Have you ever experienced a situation where you came across an advertisement on a trusted site that is offering a great deal on an item you are very interested in purchasing? You are skeptical about the advertisement but the deal being offered is too good to ignore.   If yes, what did you do in this situation? | We wanted to know how people fall for online shopping platform scams by providing a scenario where the scammers make the platform very similar to the original one. By knowing this, we can try to come up with a solution to counter the problem. |
| 1. Have you ever received a call from an unknown number claiming to be from your bank and asking for your details in order to verify a transaction?   If yes, what did you do in such a situation? | We wanted to know how people fall to scam calls by providing a scenario where the scammers pretend to be working for a bank. By knowing this, we can try to come up with a solution to counter the problem. |
| 1. If you have not been scammed, how do you differentiate between scam calls/texts/emails and authentic calls/texts/emails (e.g. Email address and domain name do not match, urgent texts, etc.) | There are definitely people who haven't been scammed before and we are very interested in what they have been doing to avoid these types of scams. Maybe we can find a more efficient solution by implementing one of their methods. |
| 1. What do you think people can do to avoid getting tricked by online purchase scams? | We are trying to learn more about what people would generally do to avoid the scams and develop our solutions based on their weaknesses. |

Figure 4.3. Secondary Stakeholders Questionnaire









**Reasonings for the Questions**

| QUESTIONS | REASONS |
| --- | --- |
| 1. Which of the following are you currently working with? | We try to classify the respondents based on their jobs, either financial institutions or e-commerce platforms. |
| 1. What is the name of your financial institution/ e-commerce company? | Although not required, if we were to have the respondent’s company name, we may be able to find specific information if needed. |
| 1. If you are working with a bank, what policies does your bank have to protect customers from scammers impersonating your institution? | Since impersonation is a big part of online scams, we are trying to learn as much as we can from banks by studying their methods and precautions for handling online scams. |
| 1. If you are working with an e-commerce company, how does your company avoid brand impersonation? | Since impersonation is a big part of online scams, we are trying to learn as much as we can from e-commerce companies by studying their methods and precautions for handling online scams. |
| 1. Does your financial institution/ e-commerce company have a specialized team to deal with scams? If yes, how effective do you think they are? | We would like to test our theory on whether financial or e-commerce companies are effective in preventing external scams. It is better to prevent rather than handle scams after it happened. |
| 1. What steps do you currently undertake to protect your customers from online scams? | We are trying to learn more on what financial institutions or e-commerce companies would generally do to avoid the scams and develop our solutions based on their weaknesses. |
| 1. What is the most common method that scammers have used to reach out to your customers? | Knowing and understanding the frequency of the scams is crucial to determine which online scams we must prioritize to resolve first. |
| 1. How often do people contact your financial institution/ e-commerce company for problems related to online purchase scams? | By understanding the frequency of scam complaints, we can identify if the companies’ policies/ methods are working effectively. If it is, we can further develop the method and apply it to our solution. If it isn’t, we can focus on their weakness and create a new method. |
| 1. What steps are currently available to the customers to protect their personal information during online transactions? | As scams keep evolving, we wanted to know if companies keep updating their precautionary steps for their customers as well as increasing our knowledge towards dealing with scams. |
| 1. To what extent have scams impacted your brand image negatively (e.g., losing customers, revenue, etc) ? | We want to know if the steps implemented by the company are actually working or if it needs more improvement. We can use this information to further develop our solution later on. |

**V. RAW DATA FROM USER STUDIES**

**Interviews**

1. Interview with a banker (jot notes)
   1. The interviewee’s voice was stern, indicating how concerned they are with the overall problem
   2. The banker asked about our project, indicating that they ensured that the problem statement was relevant
   3. Mentioned a specific scenario regarding an instance of an online scam, indicating that the banker had a lot of experience to be able to recall
   4. The banker believed that our idea was very relevant and that coming up with a solution will be industry-changing
   5. The banker cautioned about the overall scope of the project, we need to look at many different lenses
   6. Gained insights and found 2 major key details referenced in this report
2. Transcript of interview with a fintech software engineer:
3. **Through your work, what goes into ensuring a transaction is safe and credible?**

Basically, you have to check certain different things, one of them is to verify if the actual person is making a transaction themselves. Secondly, you also check for thresholds of like for example: someone wants to send like $20, $15 it’s just usually accepted and goes through but if it’s like over a certain percent for example $10,000 $20,000 anything in the higher amounts $100,000. Depending on the usual transactions that someone makes if they’re just randomly sending a huge transaction when they don’t really do that, then they kind off get flagged down so it gets checked again or it’s just denied so like some people have limits for like their transactions and then if they want to allow their account to make more higher transactions then they can like call in and request a higher percentage allotted to their account. There’s like daily, weekly limits, stuff like that.

1. **What is the fintech company you work at doing to tackle scammers who are increasing by the day?**

So before like people didn’t really use two-factor authentication as commonly as it’s done now and I think a lot of fintech companies are trying to make sure people have two-factor for example getting a phone to verify when you login through a new device, sending you emails when there is a “suspicious” login into your account, or getting a text message with a code to verify that you’re the one making the transaction. I know for when we login into our online portal for work if it’s from a new device, or if you haven’t logged in in like seven days they also check your identity. Even if you know the password it doesn’t mean you can get the app to verify the second thing which is usually a text or a phone call with a code. That’s usually done now. Companies are using a lot of AI in the sense of like analyzing a user’s transaction to like see if they’re in line with what they usually do and then if they make something that’s suspicious or out of the ordinary then they get tracked down and blocked from making a transaction.

1. **What advice do you have for people that receive fraudulent links and text messages?**

If it’s a text message, usually you can report them to your provider. If it’s emails, if it doesn’t get caught by your email provider, you can manually report it as spam but sometimes you just need to verify yourself if it’s actually fraudulent. Check for the spelling, the links that are in the text message. Usually text messages have links which mimic the look of a bank link but don’t ever click them even if your bank sends you some sort of link, go to the website itself and don’t go to whatever links you get from text to better protect yourself from fraudulent online transactions and usually people will try to send you links or text messages that are like rushing you to make a decision like “Complete your online purchase this now”, “Your amazon delivery is waiting for pick up”. Usually a shopping platform will remind of something you left in your cart but will not coerce you into making a decision with a “rushed” tone. **So if there’s an urgency to any sort of any text or email, then you kind of know right away that it’s fraudulent.**

1. **How are you ensuring that people’s personal information is protected?**

Nowadays there’s a lot more security that could go with two things that weren’t there before. As an industry, people are moving a lot into encrypting data which usually happens by default on cloud-providers and cloud-services take Amazon for example. Usually, they have encryption enabled by default but before companies weren’t really into doing that as much because it would cost more money. But a lot of solutions nowadays for cloud computing or programming frameworks and stuff like that have this enabled by default and they kind of force shopping platforms to do these best security practices. But a lot of older companies still use older software, they kind of don’t really maintain it and I think there should be a push for a lot of older software and systems to update their systems into supporting higher encryption and verifying people’s identities and making sure people have stronger passwords as well. Educating people is something a lot of fintech platforms should be doing now.

1. **Why is hard to tackle scammers despite all the security measures set up by the industry?**

Because the problem is not really only on fintech companies itself, there’s a lot of users too that when they work with a shopping platform say here in Canada. English may not be their first language or they could be a newcomer a lot of scams can target them because they might not be as familiar with how things work in Canada as opposed to their home countries. It’s hard because while you can educate a lot of people not everyone can see what’s fraudulent and what’s not. You will always have people that are gullible and can fall into traps or like don’t know English that well so they can’t really understand what people are saying.

1. **Please walk me through what it takes for someone to regain their money after a scam.**

Usually because fintech companies act like a moderator between you and your bank when you make an online purchase, they usually ask you to contact your bank directly as they don’t really have any power to return your money. Banks will then work with you to return your money through CDIC which is money that is insured by the federal government (I believe it is up to $100,000). If it’s a credit card issue you would just call your bank and they will block your account from making more transactions and they will look at the charges but it really depends on what kind of transactions are made.

1. **What type of information is most prone to theft and how can one protect themselves from it?**

Personal information like your name, your address, your phone number, your birthdate, your mother’s maiden name. What scammers typically do is get “innocent” information about you that you wouldn’t really think twice if someone asked for your address, full name, or your phone number. What scammers do is take this information and then call your cell phone provider and they’ll get a new sim card on a new phone and take your two-factor authentication. They take over your cell phone number, therefore if you get a phone call or sms from your online tech platforms or bank it will go to them instead. A lot of things that happen nowadays is people get socially engineered and manipulated to get information and then scammers will use this information to contact other companies and pretend to be you even though it’s not you but they have all your information so the other end usually cannot prevent or identify that. It is easier to do that than just hack into your various accounts.

1. **Elderly people happen to be the most prone to scams and fraud, how can they protect themselves?**

Never trust unknown numbers texting or emailing you, and never click on any links you receive via email. If you have an elderly person in your family, teach them to not accept these scams or if people call them pretending to be a certain company (such as Amazon), don’t just give them information. What you should do is call the number that you know is verified and real, usually, you can find these on the platform’s official website. Then you know that you’re actually reaching that company and not some scammer in an unknown country.

1. **Are there any regulations that make it hard to tackle this issue?**

I don’t think there are any regulations that make it difficult. But I think what is an issue now is people can spoof phone numbers as well as calls from other countries such as India or Africa since a lot of scam calls come from there. I don’t think regulating bodies can just block the whole country from calling people here. It’s a hard issue to tackle because it also involves politics in a way. There’s not really anything that’s preventing you from being protected, it’s just more like an issue that’s hard to really contain because it can easily be done nowadays. You can buy a phone number online and start making phone calls with no traceability.

1. **How can regulating bodies help tackle this issue?**

I think what regulating bodies should do is make it a requirement for any financial corporation that handles customer’s money to have checks in place, for example, two-factor authentication for people’s purchases and transactions. As well as, protecting their own citizens, they should basically force cell-phone and email providers to start restricting calls and emails that come from unknown numbers/addresses and numbers/addresses that have repeatedly been reported to be scams. This should be done because a lot of people take advantage of people like that. I feel like we’re in a day and age where you can kind of detect scams easily. In other words, it’s not really difficult to see if someone is sending a spam link with keywords like bank names or companies. There should be more fraud protection on a massive scale like that. Fintech and shopping companies don’t really have an incentive to do that and usually dump that on organizations up in the hierarchy such as governments and banks because that’s just more work for them. But if it’s starting to be regulated then it would force them to take such responsibility.

1. **As someone who works in the industry, what measures are you taking to protect yourself?**

Honestly, a lot of it starts off as like never telling people your personal information like your cellphone, your birthdate, or your address. Make sure you are only handing that information if needed to people you trust and know because this information can usually be used against you and be at risk of people taking your identity. Second, all your online shopping accounts (ex. Amazon), should have two-factor identification for logging in. Even if it’s a harmless thing like Instagram, the most important thing is making sure the email you use for online purchases has to have two-factor verification enabled on that. Never log into your personal email on public computers because they don’t usually have strong security measures. Never click on any links you don’t know, always try to go to the official website yourself rather than clicking on the link in an email.

1. **Anything else you want to share that you think is important for us to know?**

No matter how much you educate people and create PSAs, there will always be vulnerable people who are easily manipulated such as the elderly and new-comers. Scammers could literally put fear into them to make them act NOW such as “If you don’t click on this link and finish this transaction you are risking jail time!”. Banks should constantly monitor fraudulent activity and transactions that seem suspicious, they should always verify all transactions that occur before money is deposited. Another thing too is when doing an online transaction, a lot of people don’t know how to check if a platform they are using is legit or not and that is also an important issue that should be tackled both by internet providers and personal awareness. Consumers should also never put their credit card information on websites that they are not familiar with. Always go to retailers that you know and make sure you are on their official website instead of clicking on ads that look similar to the official website. There are some providers that would give you a virtual credit card number and what you can do is use sites like that but make sure you verify they are legit. This is a good way to protect yourself against fraudulent online transactions because if scammers use that virtual number, you can easily just cancel that versus if it is your physical credit card number then you will need to cancel that and wait for it in the mail which can be a hassle. Also, never use your debit when online shopping.

**Primary Stakeholder Questionnaire**

<https://docs.google.com/spreadsheets/d/15Yz-eBU60O7oChE9b0DBuEMr0u1Sx7NzV1AXWKPIH90/edit?usp=sharing>

**Secondary Stakeholder Questionnaire**

<https://docs.google.com/spreadsheets/d/1y6OOljn3AoX-dGeqQvNh9BeJsTjTvdlTVsrmrRhmpqY/edit?usp=sharing>

**VI. GROUP MEETING NOTES**

MEETING NOTES

11 October 2023

1. Identify a particular type of scan to focus on:

Options:

1. Online Purchase Scams (will be focusing on this)
2. Job Scams
3. Imposter Scams?

2. How are these scams carried out?

Calls, texts, emails

3. Stakeholders?

People who order a lot online (P) - *what age groups? 16 yrs+*

Banks (S)

E-commerce companies (S)

4. Data gathering methods:

Interviews - Sahil (already interviewed one person), Asma, Madhav and Aayush

Madhav has found a person who has fallen victim to a lot of scams. Will be interviewing him today.

Questionnaire - Mugdha and Stephen

*Remember to use CONSENT forms*

5. Find some more secondary stakeholders for interviews, if possible.

6. Next meeting - Friday 11:00 am

MEETING NOTES

13 October 2023

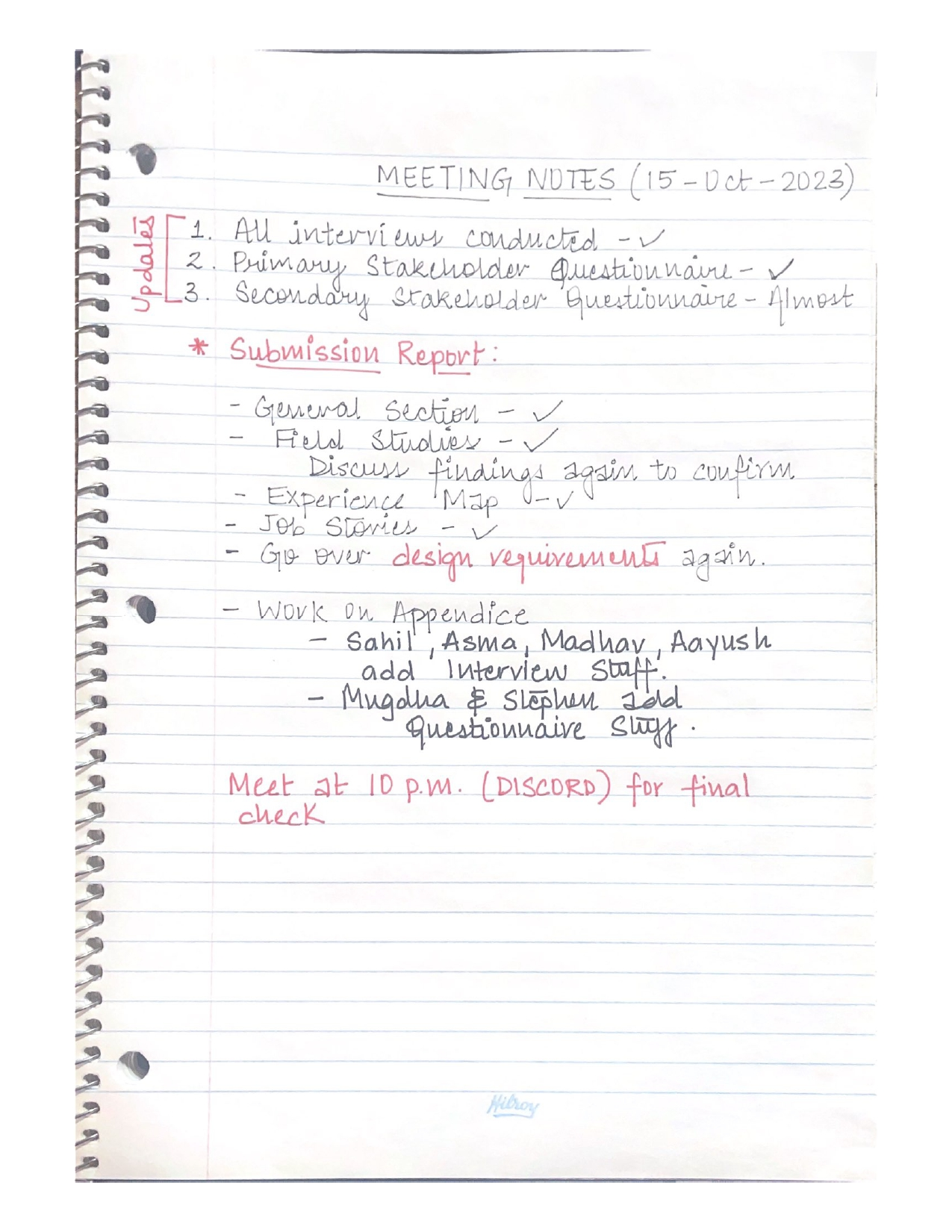
Updates:

* Questionnaire for primary stakeholders released and got 50+ responses
* Sahil has added findings of his interview in the report doc.

To Do:

* General problem section of the report - Aayush
* Create secondary stakeholders questionnaire and report findings from the data of primary questionnaire - Mugdha and Stephen
* Madhav and Asma will be adding his findings today

Next Meeting: Sunday 5 pm

****

***EXTRA STATEMENT***

*"The team is comfortable with Alfonsus Stephen Lim receiving the same grade as everyone else, as we believe he has contributed equally."*

1. Chen, Hongliang, Christopher E. Beaudoin, and Traci Hong. 2017. “Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviors.” Computers in Human Behavior 70: 291–302. <https://doi.org/10.1016/j.chb.2017.01.003.> [↑](#footnote-ref-0)
2. https://abcnews.go.com/Business/americans-lost-103-billion-internet-scams-2022-fbi/story?id=97832789 [↑](#footnote-ref-1)