"I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach

Yixin Zou, Abraham H. Mhaidli, Austin McCall, and Florian Schaub,
School of Information, University of Michigan

https://www.usenix.org/conference/soups2018/presentation/zou

This paper is included in the Proceedings of the Fourteenth Symposium on Usable Privacy and Security.

August 12–14, 2018 • Baltimore, MD, USA

ISBN 978-1-931971-45-4

Open access to the Proceedings of the Fourteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

"I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach

Yixin Zou, Abraham H. Mhaidli, Austin McCall, Florian Schaub
School of Information
University of Michigan
{yixinz, mhaidli, mccallau, fschaub}@umich.edu

ABSTRACT

Equifax, one of the three major U.S. credit bureaus, experienced a large-scale data breach in 2017. We investigated consumers' mental models of credit bureaus, how they perceive risks from this data breach, whether they took protective measures, and their reasons for inaction through 24 semi-structured interviews. We find that participants' mental models of credit bureaus are incomplete and partially inaccurate. Although many participants were aware of and concerned about the Equifax breach, few knew whether they were affected, and even fewer took protective measures after the breach. We find that this behavior is not primarily influenced by accuracy of mental models or risk awareness, but rather by costs associated with protective measures, optimism bias in estimating one's likelihood of victimization, sources of advice, and a general tendency towards delaying action until harm has occurred. We discuss legal, technical and educational implications and directions towards better protecting consumers in the credit reporting system.

1. INTRODUCTION

In the United States, credit bureaus (also called credit reporting agencies) are private, for-profit organizations that create aggregated reports of individual consumers' credit information. They offer this information as a service to businesses that need to assess their customers' creditworthiness. For instance, lenders use credit reports and credit scores to determine whether they approve a loan and at what interest rate; landlords may check credit scores before offering a lease for an apartment; employers may consider credit reports in hiring decisions [27]. As such, credit bureaus play a significant role in the lives of U.S. residents by impacting their access to many necessities. In the United States, there are hundreds of credit bureaus serving specialized credit reporting needs. The biggest among them are the three National Consumer Reporting Agencies (NCRAs) [15]: Equifax, Experian and TransUnion.

In 2017, Equifax suffered a large-scale data breach that resulted in hackers stealing sensitive data of over 146.6 million consumers [45]. The data stolen included names, social security numbers, birth dates, addresses, and driver's license numbers, along with credit card numbers for about 209,000 consumers and dispute documents for another 182,000 consumers [38].

The size, scale and potential consequences of this data breach are unprecedented: the 2017 Equifax breach put almost half of the U.S. population at risk of identity theft. Defined as "the unlawful use of another's identifying information for gain" [89], identity theft often manifests itself through fraudulent use of existing accounts (e.g., credit card, telephone, online and insurance) [40], opening of new accounts or credit lines in the victim's name, as well as non-financial crimes [62]. In 2014, about two-thirds of identity theft victims experienced an average financial loss of $1,343, and about 40% of identity theft victims reported emotional distress resulting from the incident [40].

Despite the identity theft risks posed by the Equifax breach, evidence suggests that consumers took little to no protective action after it became public. Surveys following the breach conducted by Credit Sesame, a credit monitoring site aggregating consumer data from TransUnion, showed that 10 days after the breach was announced in September 2017, only 0.44% of credit reports at TransUnion had a credit freeze on file — a slight 0.8% increase from June 2017 [18]. The percentage of consumers who placed effective credit freezes, i.e., freezing their credit reports at all three major bureaus, would only be smaller. While a credit freeze restricts access to one's credit report and is associated with fees in many states, fraud alerts, which are free, had not been used by most consumers either. The Credit Sesame report found that only 7% of its members had a fraud alert on their credit report at TransUnion as of September 2017 [18].

To investigate the seeming contradiction between the severity of the Equifax data breach and the apparent lack of action by consumers, we conducted semi-structured interviews with 24 participants to gain insights on people's mental models of credit bureaus (how credit bureaus work, how credit bureaus collect/use data, etc.), risk perceptions of identity theft, the protective actions they took in response to the Equifax data breach, and reasons for inaction.

Our key findings show that (1) participants' mental models of credit bureaus varied regarding perceived purpose and information flows. (2) The majority of participants were generally aware of the Equifax data breach and the resulting risks, but most did not take protective action after the

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018.
August 12–14, 2018, Baltimore, MD, USA.

breach. (3) We find that this inaction was not primarily influenced by accuracy of mental models or risk awareness, but rather by costs associated with protective measures, optimism bias in estimating one's likelihood of victimization, and a general tendency towards delaying action until harm has occurred. (4) Sources of advice appeared to be an influential factor in initiating actions; many participants who took action acted on advice from people they trust. Yet, taken actions also created a false sense of security for some, leading them to overlook other measures.

Based on our findings, we conclude that current protective measures offered by credit bureaus are insufficient to protect consumers. We discuss our findings in the context of prior research on privacy and security behavior, and suggest technical, legal and educational approaches to better protect consumer credit data and empower consumers with usable protection measures.

2. BACKGROUND

As context for our study, we first give an overview of how the U.S. credit reporting system operates; relevant regulation, protective measures; and the current state of data breaches and identity theft in the United States.

2.1 The U.S. Credit Reporting System

The U.S. credit reporting system relies on complex information flows between National Credit Reporting Agencies (NCRAs), smaller credit bureaus, data furnishers, public record repositories, users of credit reports, and consumers [15]. As the core entity of this ecosystem (see Figure 1), credit bureaus gather information about consumers' credit-related activity (referred to as trade lines) from data furnishers, including banks, credit unions, credit card issuers, auto and mortgage lenders, and many other entities who can provide information related to their transactions or experiences with consumers. NCRAs also purchase public record data on individuals' bankruptcy filings, tax liens, and court judgments. Some NCRAs also keep track of debts collected by third parties on behalf of the original creditors [15]. When such data is reported to credit bureaus, it is associated with Personally Identifiable Information (PII) of consumers, such as name, current and former addresses, birth date, and social security number (SSN). Each NCRA has their own channels to collect data, which they typically do not share with other credit bureaus. The amount of data processed by credit bureaus is vast: each of the NCRAs receive information on over 1.3 billion trade lines from data furnishers and updates on over 200 million credit files on a monthly basis [47].

The key function of credit bureaus is to provide credit reports on individual consumers. These reports typically include the consumer's name, current and former addresses, SSN, birth date, phone numbers, trade lines, public record information, and inquiries for the credit report by other entities [15]. Credit bureaus also calculate a credit score for the consumers, which may differ across NCRAs. Credit bureaus then sell these reports and scores to businesses who use them to assess the creditworthiness of their customers; primarily creditors and lenders, but also landlords, insurance companies, employers, debt collectors, utility services, and government agencies [44].

In the United States, the Fair Credit Reporting Act (FCRA) regulates the activities of credit bureaus. It details obligations for NCRAs, data furnishers and credit report users, and grants consumers the right to obtain a free copy from each NCRA annually and dispute errors on their credit files. In practice, however, errors on credit files are common [30], credit bureaus and data furnishers do not conduct thorough investigations into consumers' dispute requests [55], and the way NCRAs use consumer information and advertise their services has raised controversy [17]. Further legislation aims at combating identity theft. For instance, the Fair and Accurate Credit Transactions Act (FACTA) requires debit/credit card issuers to validate customer's address changes [8] and enables consumers to place fraud alerts at NCRAs [29].

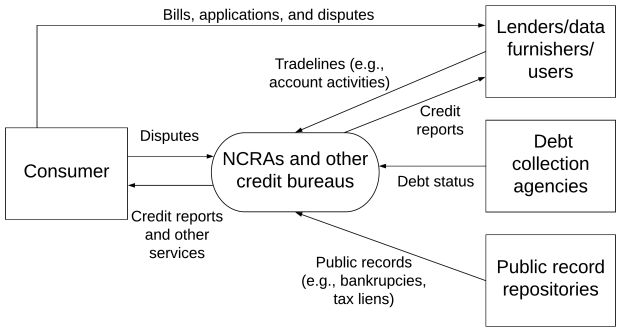

Figure 1: A simplified diagram of information flows around credit bureaus.

2.2 Available Protective Actions

Consumers have options for protecting and limiting access to their credit data, such as credit freezes, fraud alerts, checking credit reports, and using a credit monitoring service.

Credit freezes block inquiries for one's credit report, thus preventing new accounts or loans that require credit checks to be opened under the consumer's name. Unfreezing credit requires contacting the respective NCRA with a PIN to lift the freeze. However, a credit freeze is specific to a credit bureau [9], so effective protection requires placing credit freezes with each of the three NCRAs. Freezing or unfreezing one's credit typically costs $5-10 for each action with each NCRA, although some state laws prohibit those fees. A credit freeze only limits access to the credit report and thus does not protect against other types of identity theft that do not require credit checks (e.g., tax fraud).

Compared to credit freezes, fraud alerts are free but less effective. Creditors can still conduct credit checks on consumers' credit reports, but reports including fraud alerts signal that the consumer is at risk of credit fraud. Under this circumstance, creditors are expected to perform expanded identity verifications [26], but sometimes they may ignore such alerts and take no actions [61].

Consumers can further request their credit reports from the three NCRAs for inspection for free on a yearly basis, with additional costs for more frequent requests. Credit monitoring services and identity protection services are offered by NCRAs and other companies (e.g., LifeLock) as paid subscriptions. Credit monitoring alerts consumers about suspicious activity on credit reports only [82]. Identity protection services monitor more extensive information, but do

not capture tax or government benefits fraud [82]. Identity theft victims may consider identity recovery services and insurance to remediate or compensate harm, although the quality of these services seems to vary [11]. The the Federal Trade Commission (FTC) offers free online resources for victims of identity theft to help with recovery [84].

After the Equifax breach, in addition to the suggestions above, the FTC further recommended monitoring current accounts for fraudulent activity, using Equifax's dedicated website[1] to check whether one's information has been exposed, making use of a free year of credit monitoring offered by Equifax [83], as well as filing taxes early to prevent identity thieves from claiming a tax refund under one's name.

Given the range of protective measures and their respective caveats, it is not clear to what extent consumers are aware of these offerings, as well as their strengths and limitations. Furthermore, the complexity of these offerings is exacerbated by usability and reliability issues. For example, Equifax's official site for the data breach provided inconsistent results when consumers checked if they were affected [37]. Equifax even promoted the wrong web address in a tweet, sending consumers to a fake website instead [12]. In addition, Equifax tried to bundle the free credit monitoring they offered with a forced arbitration clause, so that consumers would have waived their right to sue Equifax in class-action lawsuits [57]. Other consumers were not able to place credit freezes at any of the three NCRAs, possibly due to a large volume of requests after the Equifax breach became public [22].

2.3 Data Breaches and Identity Theft

Data breaches have become increasingly prominent: 64% of the U.S. public having been affected by a major data breach [60]. Before Equifax, companies like Yahoo, Friend Finder, and eBay have suffered larger-scale data breaches [6]. Unlike these previous cases however, consumers have no choice to opt out of data collection by NCRAs.

Starting with California in 2003, most states in the U.S. have passed data breach notification laws, requiring companies to disclose data breaches immediately in a timely manner if the breach compromised consumer information. Romanosky et al. [71] found that the adoption of these laws reduced identity theft caused by data breaches about 6% on average. More recent amendments make further requirements about the compensation that affected companies should offer to consumers, such as providing free credit monitoring services if the breach involves SSN [77]. These compensations have shown to be effective in restoring customer sentiments [49].

However, there is a troubling gap between consumers' concerns and protective behaviors after data breaches. A report in 2014 [63] revealed that, following a data breach, consumers had a 21% increase of concern about being identity theft victims, but 32% of them reported that they ignored the notification and did nothing. This issue also surfaced after the Equifax data breach, when there was a less than 1% increase of newly initiated credit freezes at TransUnion [18]. These statistics imply the possibility of a pattern similar to the "privacy paradox" [48]: people claim they are concerned about their exposed data, but may not take protective actions. In our study, we investigate underlying reasons for this paradoxical behavior in the context of the Equifax data breach.

[1] `equifaxsecurity2017.com`

3. RELATED WORK

We discuss related work on security and privacy mental models, prior literature on risk perception, and user behaviors in reaction to security advice.

3.1 Security and Privacy Mental Models

Mental models are the representations of how objects or systems function in people's minds [19]. They have been studied to understand human cognition [85], reasoning [46], and decision-making [52]. Because mental models can be incomplete, imprecisely stated, with obscure or impugnable facts [35], sometimes they are also referred to as "folk models" [23, 91, 88]. In the context of human-computer interaction, studying mental models can provide insights on people's knowledge and understanding of a specific domain [41, 36], as well as help explain and predict people's interactions with complex interfaces or systems [59].

Mental models have been studied in usable privacy and security research to provide insights into users' understanding and behaviors [88, 10, 42, 65, 51, 10, 92, 91, 43, 14]. For example, Wash [88] investigated folk models of security threats and found that gaps in these models prevented users from taking actions against botnets. Bravo-Lillo et al. [10] examined mental models of security warnings and suggested that different interpretations of cues led users to diagnose underlying risks and respond differently. Zeng et al. [92] studied mental models of smart homes, revealing that end users had very limited technical understanding and concerns of potential security issues, which helped explain a lack of sophisticated mitigation strategies. Yao et al. [91] found that users had incomplete or inaccurate mental models of how online behavioral advertising (OBA) works, highlighting the importance of user education. Among these mental models studied, there are substantial discrepancies between experts and non-experts [43]. Understanding mental models of end-users hence can provide rich insights for effective communication regarding privacy and security risks [14].

Yet, little is known about consumers' mental models of credit bureaus. Studying and understanding mental models in this context can provide insights on consumers' reasoning, decision-making and behavior related to the Equifax data breach in particular, and credit bureaus and data breaches in general.

3.2 Risk Perception

Mental models have been used to study risk perception, i.e., the perceived chance that an individual will experience the effect of danger [76]. Contrary to technical or objective risk, risk perception is a person's subjective assessment of the probability that a specific event happens and how concerned they feel about its consequences [67]. Early paradigms like the psychometric model [32] interpret risk perception as a process of calculating risks versus benefits. Later theories (e.g., Cultural Theory [24, 21]) place greater emphasis on contextual factors, such as attitudes to the perceived risk and the sensitivity to general risks.

Risk perception can greatly impact individual privacy and security decisions and trigger protective actions [42]. Fagan and Khan [25], using a rational decision model, re-

vealed large differences of risk perception between users who followed common security practices (e.g., update software, use password manager) and those who did not. Altering risk perception was found to be effective in motivating end-users to make better decisions, as demonstrated by Harbach et al.'s study in which end-users behaved more privacy-consciously during the installation of Android applications after seeing personalized examples of personal information use [39].

3.3 Factors in Security and Privacy Behaviors

Risk perception is not the sole determinant of the complexity of privacy and security behaviors. Understanding risks does not automatically make users aware of appropriate countermeasures. Shay et al. [75] find that although users were aware of different account hijacking threats (e.g., malware, phishing, data breaches), most of their countermeasures focused on password management only. Differences in mental models and awareness between security experts and non-experts, are echoed in behavior: experts were found to use two-factor authentication and password managers more frequently, whereas non-experts prefer actions that demand less technical knowledge, such as using anti-virus software, changing passwords frequently, and only visiting known websites [43].

A variety of factors have been identified that prevent people from translating risk perception into protective behavior. Forget et al. [34] note the importance of awareness of technical expertise, as misalignment between estimated and actual expertise can result in insufficient security measures. Acquisti et al. [1] identified main categories that affect privacy and security choices as incomplete or asymmetric information flows; bounded rationality (the general tendency to simplify the decision-making process); and different kinds of cognitive and behavioral biases (e.g., framing effects, optimism bias, loss aversion, and status quo bias). Privacy preferences and behavior are further affected by uncertainty, context, and framing [2]. These factors have been validated in empirical studies [43, 72, 13, 3, 4, 2, 1, 90]. For instance, the belief that information is only secure within the person's own memory (e.g., "no one can hack my mind") explains why non-experts preferred memorizing the passwords themselves, and were skeptical about using expert-advocated password managers [43]. Sawaya et al. [72] showed a similar situation where self-confidence in computer security knowledge had a much greater impact on user behaviors than actual knowledge. Camp [13] pointed out that people tend to underestimate security risks when they have not experienced negative consequences from past risky behaviors.

In addition to individual factors, the source of security advice influences privacy and security behaviors [68, 69, 64, 81]. A representative survey conducted by Redmiles et al. [68] reported that users with lower Internet skill levels and socioeconomic status were less likely to get security advice from readily available sources, hence making themselves more vulnerable to security risks. Another study on security source selection [69] showed that advice from sources with a higher level of perceived trustworthiness was more likely to be taken, whereas sources that included too much marketing content or showed threats to privacy were less favored. Furthermore, Rader and Wash [64], by examining computer security advice from three different sources, discovered that each source uniquely focused on a single aspect of computer security, and it was unlikely that users could get a comprehensive picture of computer security from a single source.

We expand on prior work, by studying the underlying reasons for the suggested gap between consumers' concerns and behaviors following the Equifax data breach.

4. STUDY DESIGN

In our study, we investigated (1) consumers' mental models of how credit bureaus operate, (2) what consumers perceive as risks of the Equifax data breach, and (3) what protective actions consumers took or did not take in reaction to the perceived risks, and the reasons behind their decisions. To understand these questions, we conducted semi-structured interviews with 24 participants in January and February 2018. All interviews were audio-recorded and lasted 40 minutes on average, ranging from 20 minutes to 61 minutes. Each participant was compensated with $10. The study was determined to be exempt by our institution's IRB.

4.1 Interview Procedure

We developed and refined our script for the semi-structured interviews through multiple pilot interviews. The final interview script is included in Appendix A.

In the interviews, we started by asking participants how they manage their personal finances, leading into a discussion about their experiences with and understandings of credit bureaus. Next, we asked about their awareness of Equifax and the 2017 data breach, before providing a basic description for those who had not heard of it. We probed participants' risk perception by asking what they saw as consequences of the breach, reactions when hearing about the breach, and feelings about their data at Equifax. Then we asked whether participants have taken protective actions, and asked about their experiences and interpretations of an action's outcomes. Finally, we asked participants to recall previous experiences with data security issues (e.g., being affected by data breaches) and identity theft (e.g., someone applying for loans under their names). We wrapped up the interview by debriefing participants about the real purpose of the study (we used mild deception in recruitment to mitigate self-selection bias, see Sec. 4.2), and gave them time to ask clarification questions.

At the end of the session, participants were asked to complete two questionnaires that measured their financial decision-making ability [58] and self-determined financial well-being [16]. We collected such financial-related information after the interview to minimize potential priming. For instance, participants might otherwise think the study is about one's financial management and overstate how often they check credit reports. Conversely, the interview questions should have little impact on participants' responses to the exit survey, as they did not touch specifically on the same topics.

4.2 Recruitment

We recruited participants via online platforms (e.g., Reddit, Craigslist, and Facebook) and emails to a university research pool and campus mailing lists. We recruited for a "study on personal finance and credit bureaus" purposefully not mentioning Equifax or identity theft to avoid priming participants and limit self-selection bias. Prospective partic-

ID	Gender	Age	Education	Income	NFEC (0-8)	CFPB (0-100)
P1	F	60-69	Bachelor's	$125-150k	8	88
P2	M	30-39	Master's	$25-50k	6	61
P3	M	60-69	Bachelor's	<$25k	5	35
P4	M	18-29	Some college	$125-150k	7	73
P5	F	50-59	Master's	<$25k	3	41
P6	M	50-59	Bachelor's	$50-75k	6	45
P7	F	18-29	Bachelor's	$25-50k	4	50
P8	F	50-59	Some college	<$25k	6	47
P9	M	60-69	Bachelor's	<$25k	8	48
P10	F	18-29	Some college	$150k+	7	81
P11	F	18-29	Bachelor's	N.A	8	54
P12	M	40-49	Master's	$50-75k	7	65
P13	F	30-39	Professional degree	$50-75k	5	58
P14	F	18-29	Some college	<25k	5	56
P15	M	40-49	Bachelor's	<25k	8	49
P16	M	50-59	Master's	$75-100k	7	57
P17	F	30-39	Master's	$150k+	6	75
P18	M	30-39	Bachelor's	$25-50k	6	57
P19	F	50-59	Master's	$100-125k	7	56
P20	F	18-29	Master's	$50-75k	7	64
P21	M	50-59	Some college	$125-150k	8	82
P22	M	18-29	Bachelor's	$25-50k	6	52
P23	F	40-49	Master's	$75-100k	8	60
P24	F	40-49	Associate's	$50-75k	7	56

Table 1: Demographics of participants, and scores of NFEC financial decision [58] and CFPB financial well-being scales [16].

ipants provided basic demographic information in an online screening survey (see Appendix B). We only recruited U.S. citizens and permanent residents who had lived in the U.S. for more than five years, as recent immigrants might not be familiar with the U.S. credit reporting system or may not be included in credit bureaus' databases, yet. We deliberately selected a diverse sample of 24 participants in terms of age, gender, education, occupation, and income, as prior literature suggests demographic factors can influence people's financial experiences and responsibilities [54, 20].

4.3 Qualitative Data Analysis

With permission of the participants, we audio recorded and then transcribed all interviews. We then conducted thematic analysis [7], a common approach used for qualitative studies in human-computer interaction [50] and usable privacy and security [34, 80, 91]. The initial version of the codebook was developed by two of the authors, who coded a subset of interviews independently and grouped them into initial themes. Through multiple rounds of collaborative refinement, we achieved good inter-coder reliability (Cohen's κ=.79) [33]. The final version of the codebook included 14 overarching themes (e.g., "understanding of credit bureaus," "attitudes toward the breach," and "actions suggested by participants") and a total of 53 unique codes (see Appendix C). One researcher then coded the remaining interviews and recoded previous ones using the final version.

5. RESULTS

We first describe our sample population and then present our results focusing on three areas: mental models of credit bureaus, risk perceptions of the Equifax breach, and protective actions.

5.1 Sample Population

Table 1 summarizes the demographics of our interview participants. Our sample was diverse in terms of age, gender, education, occupation and income. We interviewed 11 male and 13 female participants. Their ages ranged from 21 to 68, with a median age of 44 years. Five (5) participants had no college experience, 10 had a Bachelor's or Associate's degree, and 9 had a graduate degree (e.g., Master's or Professional degree). Eight (8) participants worked in a university setting as students or staff, and the rest had various occupations (e.g., engineering or IT professionals, medical, business, social work, and retired). P16 was the only participant with a cybersecurity background. Our participants' annual household income ranged from less than $25,000 to more than $150,000, with the median income in the range of $50,000 to $74,999. The NFEC financial decision test [58] score ranged from 3 to 8 with a median score of 7 (out of 8); 19 of our 24 participants got a score of 6 or higher, indicating they are financially literate enough to "make entry level financial decisions" [58]. The CFPB financial well-being score [16] ranged from 35 to 88 with median score of 56.5 (out of 100), which suggests average financial well-being in our sample [16].

5.2 Mental Models of Credit Bureaus

Among the 24 participants, 19 of them were aware of the big three credit bureaus, 17 of them correctly interpreted their function as assigning credit scores to individual consumers, yet none of them could fully describe the types of information collected by credit bureaus and corresponding information exchange entities, leading their mental models to be either incomplete or inaccurate.

5.2.1 General awareness of the big three bureaus

While most participants (19) knew that there are three big credit bureaus in the United States, only 7 participants could list the specific names of all three. Four (4) participants mentioned that other smaller-scale credit bureaus also exist, e.g., *"I wouldn't be surprised if there are other smaller companies that track and monitor credit scores and stuff." (P11)*, but none of our participants were able to give specific names. A few (5) participants had difficulty mapping the names they've heard of with the concept of credit bureaus. P15 said: *"I don't know if the credit bureau is separate, or if Equifax, Experian, et al., are considered credit bureaus."* P3 considered Credit Karma, a company that offers free credit monitoring, as a credit bureau, citing his experience of checking credit scores using Credit Karma: *"It is on the same level as those three major ones [...] With Credit Karma, since they're trying to get into the market, I think, you can go to them any day and night, and they're not charging. But they have that same information."*

5.2.2 Purpose of credit bureaus

Seventeen (17) participants described credit bureaus as companies that assign credit scores to individual consumers. Most of them (14) went on to say these scores represent one's creditworthiness and hence help lenders, insurance companies and others make decisions. In contrast, a third of participants gave inaccurate descriptions of credit bureaus. P11 viewed credit bureaus as government-related: *"I think that is basically government agency that tracks and monitors each person's history, financial history."* Some confused credit bureaus with other organizations such as credit unions, debt collectors, and loan companies. P23, for instance, confused credit bureaus with credit rating agencies, who rate creditworthiness of companies and governments rather than individual consumers: *"I guess they need to support the rating [...] and maybe the credibility of that organization. Maybe*

any complaint from the customer. How they use their funding and if it's a bank, how they use the customer's money." P4 referred to credit bureaus as loan companies: *"They loan out money to their credit card that they expect you to pay back. Then if you don't pay back, then they just charge you more interest."*

5.2.3 Incomplete understanding of collected data

Regarding the types of information collected by credit bureaus, PII (e.g., names, addresses, SSN) and financial-related information (e.g., number of credit cards and loans, credit limits, late payments) were noted most frequently, even for participants who did not conceptualize the purpose of credit bureaus correctly. Half of the participants mentioned the collection of employment history, public records (e.g., tax lien and bankruptcy), and inquiries made by creditors in recent years. About one fourth of participants (7) stated that the information collected by credit bureaus is "a lot," "a variety of different things," or "almost everything," yet no participant covered all types of data collected by NCRAs. Participants' knowledge was closely tied with their personal experience with credit bureaus. Those who checked their credit reports recently and more frequently were able to recall more details, but still showed uncertainty sometimes: *"Well I think they use past accounts and maybe employment history. I know they use length of credit. But like I said, I don't know, random guessing."* (P24).

Some participants thought credit bureaus collected certain data, which credit bureaus do not actually collect. For instance, P9 thought credit bureaus checked in with a consumer's relatives and kept tabs on social media profiles such as Facebook: *"Facebook I think would just show things like their hobbies and [...] travel, like to go to Europe or Las Vegas [...] it would give you an idea of their lifestyle, and if they're throwing money around."*

5.2.4 Information providers and customers

Many (19) participants noted that financial institutions are the primary information providers for credit bureaus. *"I guess people who provide information are like banks, loan companies, loan providers, debt collectors and just people who you've rented with before and haven't paid back or stores or credit card companies"* (P13). Some participants mentioned auto dealers, governments, and utility companies as information providers, but these were brought up much less frequently. As for customers of credit bureaus, more participants (19) mentioned creditors and lenders than other businesses (e.g., car dealerships and landlords). Some participants noted that information providers of credit bureaus are simultaneously their customers, and there exists collaboration between these institutions. According to P16: *"What I also imagine is that they also send some of that information back to banks and lenders, it's a two-way street I assume, and there's probably data sharing agreements between the two of them."*

5.2.5 Offerings of credit bureaus

Many (14) participants were aware of their right to obtain a free credit report annually. Only a few (4) mentioned other products and services offered by credit bureaus that are associated with a fee, such as a credit monitoring service. A substantial portion of participants (15) noted that although they knew they could check credit scores directly at credit bureaus, they preferred to check their scores through other means (such as banks or third-party financial management tools like Credit Karma) due to low cost, convenience and frequency of updates. A prominent issue is that participants rarely knew the difference between FICO score and the scores provided by NCRAs, which are calculated using different models. P22 asked: *"As far as I know, I'm not sure how, I guess, the credit bureau interacts with the FICO credit scores, or if they create them?"*

Notably, low income participants generally knew these services were offered, but chose not to take advantage of them, in some cases refusing to interact with credit bureaus altogether. P5 and P15 both said they had no interest in checking their credit reports. According to P15: *"I can find out my credit score [...] there's a website where you can, but of course I have been reluctant to do that because, (a) I know my credit's terrible, (b) I don't want to give them any information."* Participants with higher income who did not use these offerings cited how they did not see the need to apply for credit cards, borrow money, or make big purchases.

5.2.6 Negative perceptions of credit bureaus

Almost half of our participants (10) expressed a moderately or strongly negative sentiment towards credit bureaus and/or the whole credit reporting system. In some instances, negative perceptions stemmed from doubts on whether the credit reporting system was fair to consumers. P19 said: *"I don't like the idea that things like auto insurance and getting an apartment [...] people come up with cash upfront and they still get denied because of a credit report [...] it does make sense that there is something like this, but not the way it's running right now."* P14 described how credit bureaus increased inequality by worsening the financial well-being of people who were less affluent: *"It's really like a bad cycle. If you don't have enough money and then you need a loan, and then you can't get a loan or your interest rate is really high and you can't afford to pay it."* Some (5) participants explicitly stated that credit bureaus and related institutions such as banks took advantage of individual consumers. P24 said that credit bureaus work to serve the interest of lenders, with little concerns about individual consumers: *"For the interest of who? Those in power to make these laws ... I'm assuming they probably all have lobbyists and things that could potentially benefit collaborators of credit bureaus, like lenders, businesses and car companies."*

Other negative perceptions originated from personal experiences with credit bureaus. P1 said that her husband was once denied a credit card, because credit bureaus provided the credit file of another person with the same name to the credit card company. P5 went through a long process of disputing erroneous credit card charges, during which credit bureaus offered little support, leading her to lose faith in the system: *"[The dispute process] It's probably all automated and they only take what people give them. I've been on there for things that I should not have been, but I feel powerless to try to get that stuff off. I just give up. I don't care. That's why I say I don't want to look [up my credit report]. Because how much stress and time that would take?"*

Moreover, some (5) participants expressed confusion and concern over the data collection and aggregation process between credit bureaus and their information providers and

customers. For instance, P3 expressed his frustration when he found out information about transactions between him and other businesses will inevitably fall into the hands of credit bureaus, a process he defined as "breach of confidentiality": *"When it comes to credit bureaus, I don't think there is any such thing as confidentiality [...] Whatever I'm talking to these people [banks], whatever they do, that should be strictly between them and I. Okay? But somehow, in my mind, the credit bureau ends up with this information."*

5.3 Perceived High Risk of the Equifax Breach

More than half of our participants had heard of the Equifax data breach before the interview. They conceptualized identity theft as the primary risk of the breach and described different ways that it could happen. Several (3) participants also noted privacy invasion as a secondary risk. Nevertheless, participants seldom associated these risks with themselves, implying the existence of optimism bias.

5.3.1 Aware but vague memory of the event

Participants showed a high awareness of the occurrence of the 2017 Equifax breach. A majority of participants (20) knew a data breach happened to one of the big three bureaus. 14 of them knew the breach was at Equifax, and the rest either did not remember the name, or attributed the breach to Experian.

Similar to our findings on the perceived types of data collected by credit bureaus, participants generally had a vague idea that the company was hacked, leading to the disclosure of "a lot of" information, but many participants stated that they could not remember a lot of details. P2 said: *"I don't know the specifics, if it was a hacker attack or something like that, but I know that a lot of information got out and millions of people were affected."* As for types of information that were exposed, PII including name, address, date of birth, and SSN, was mentioned most frequently, followed by bank account numbers and credit card numbers. 6 participants, who all included credit card transactions and loan history in their mental models of credit bureaus' data collection, also erroneously assumed these types of information were exposed in the breach whereas in reality they were not.

5.3.2 Identity theft as the primary risk

Most participants (19) mentioned risk of identity theft as a direct consequence of the data breach. Some (10) participants followed up with examples of how identity theft could happen. *"The consequences? Probably a lot of identity theft. It could make it very easy if somebody wants to steal somebody's identity. They could get hold of those big three or four, the name, SSN, and birth date and could just open up a bunch of accounts under their name, and they'd be none the wiser"* (P2). However, most of these examples focused on the opening of new accounts and fraudulent charges on existing accounts; only 2 participants brought up misuses of stolen personal information that did not require credit checks, such as tax fraud. P12 further mentioned that this breach prompted him to consider filing his tax return earlier this year: *"It could lead to some fraud around tax time. I heard the other day where people are... or criminals take other people's tax returns. I'm going to file my tax returns as soon as I can."*

Participants' knowledge of what data was exposed influenced their perception of the risk posed by identity theft. The loss of SSN triggered more identity theft concerns compared to other types of PII (e.g., names, addresses and dates of birth) and financial information (e.g., credit history and credit card numbers). P13 differentiated the sensitivity of exposed information based on how publicly accessible it was: *"You can find someone's date of birth and name online, but the social security number should be harder to find."* P19 was concerned due to how SSN's are hard to replace: *"You can't get a new Social Security Number, the government is not very accommodating about that and all these other things. I would prefer not to think about it because you'll just be screwed."* Both P13 and P19 mentioned that it is the combination of different kinds of data that scared them the most. As P19 said, *"If someone were to steal your identity [...] you would just be helpless. It's not like sometimes someone will take a credit card out in your name or somehow try and use your bank, and you have some recourse, but if they've got everything I have no idea what you would do."*

5.3.3 Privacy invasion as the secondary risk

In addition to identity theft, 3 participants stated that the exposure of such sensitive data is an invasion of privacy. Although P5 did not use the word 'privacy' explicitly, she described her panic when she thought about how much the hackers could know about her: *"The hackers, they would find out my personal information, which really scares me. I don't want people to know where I live. I don't want people to know whatever information they have."* P16, who did not explicitly state his own privacy concern, noted the possibility of knowing one's personal life in detail based on the exposed data: *"As they aggregate that data they can get more and more information about you. For example if there's detailed credit card information, which God I hope not, they would know your shopping habits, they might know where you live, what kinds of cars you drive."* P22 said he would value his financial information as privacy, but did not value it as highly as the loss of his SSN, due to the latter's repercussions for identity theft: *"I guess I would value my Social Security number, number one, because I don't want my identity stolen. I also value my privacy, but I feel like I haven't gotten to a point yet where I've made lots of these kinds of credit-based purchases, so not yet at a point where that's my number one."*

5.3.4 Change of trust

Based on the perceived risks, 9 participants noted that this breach eroded their trust in Equifax's ability to ensure the security of consumers' data. P14 said that consumers had no choice but to trust Equifax because: *"They're gonna get your information whether you wanted them to or not."* P12 claimed his trust in Equifax decreased to the point that he did not accept the free credit monitoring service offered by Equifax: *"Well, you didn't handle the other information, why should I trust you to monitor anymore information?"* Interestingly, a counterexample is provided by P24, who said she would trust Equifax more because Equifax would now have better security practices: *"I'd probably go back to them just because they're probably going to be a little bit more cautious than the one that didn't get hit."*

5.3.5 *Underestimated likelihood of being affected*

While almost all participants demonstrated an understanding of the risks of the breach, the majority (17) did not assume they would be personally affected, exhibiting optimism bias [1]. We identified multiple reasons for the underestimation of personal risk. Four (4) participants mentioned how they checked the Equifax website to see if they were affected and received the message "your personal information was not impacted by this incident." Another reason is the notion of 'I have nothing to lose,' especially for low income participants. P5 said: *"I don't have any credit. I have a bad record so I wouldn't do that [check if were affected]. Nobody can hurt me, it's already at the lowest place."* The third reason is the absence of signals indicating negative repercussions, such as a lack of notifications to individual consumers from Equifax and lack of suspicious account activities since the breach occurred. P7 said: *"They [Equifax] were like there was a breach and if you were directly affected we will let you know. [But then you never received?] No, so I was fine."* The fourth reason is the presumption of not being included in Equifax's database, or having limited information in the database. For instance, P6 asserted he could not be affected because he had never held any credit cards so was not included in credit bureaus' databases. P8, who held a credit card but never checked her credit reports, believed her information shared with credit bureaus was not as extensive as someone who checks their credit reports or interacts with credit bureaus in other direct ways.

Even though some participants thought they might be affected by the breach, none claimed it in an assertive way. Among the 5 participants who received the "Your personal information might have been impacted by this incident" statement from Equifax's site, most were doubtful about the meaning of "might." P13 interpreted it as a public relation strategy which did not necessarily reflect the truth, causing little concern to her: *"If they say no and then you get affected, you might be like: you said I wasn't gonna be affected so I didn't worry and I wasn't monitoring, you know? But if they say yes, then of course you're gonna freak out and start calling them, asking them for advice or services, whatever. But if they say maybe, that's like a safe, middle ground for a company to say."* Other participants who did not check the website but felt they might be affected developed this notion based on the sense that *"[if] these many people were affected, it's likely that I was affected"* (P2).

5.4 Negligence of Protective Actions

Figure 2 lists the frequency of protective actions taken, based on the FTC's suggestions for the Equifax data breach and identity theft in general [83]. More than half of our participants (14) did not actively take any protective measures after the Equifax breach, despite the perceived high risk. Participants were either unaware of available tools, or intentionally avoided using them for various reasons.

5.4.1 *Insufficient knowledge*

The high portion of participants who were unaware of available protective measures suggests insufficient knowledge as a primary reason for inaction. Only 3 participants correctly described fraud alerts, and all of them learned it from being affected by previous data breaches and being offered the service as compensation. The remaining participants either said they did not know what fraud alerts were, or associated

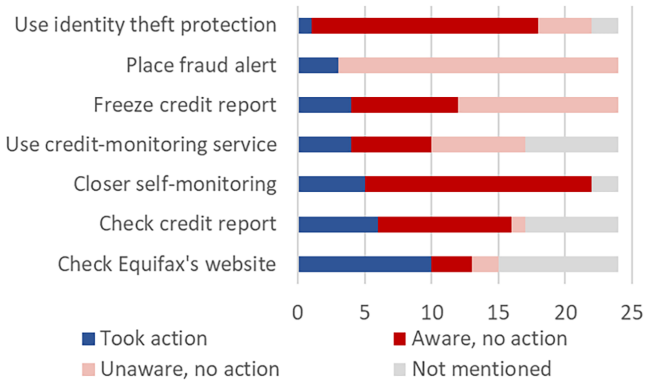

Figure 2: Status of suggested actions taken or not taken by participants.

fraud alerts with alerts sent from banks and credit card companies when fraudulent activities occur. Similarly, credit freezes were incorrectly interpreted as freezing credit cards by half of our participants. Participants generally considered the measures offered by banks and credit card companies as effective and useful in preventing identity theft. However, their unawareness of the nature of fraud alert and credit freeze measures provided by credit bureaus hampers them in utilizing these actions to protect their credit information.

5.4.2 *Costs inhibit action taking*

Cost appears to be a significant issue in determining the likelihood of whether an action was adopted. Actions with no cost were more favored: checking Equifax's website was the one taken by most participants (10), followed by checking credit reports either through the annual credit report site or third-party services for free (6), and a closer self-monitoring of existing accounts (5). For the remaining four options in Figure 2, most actions were initiated prior to the Equifax breach when participants had been affected by previous, separate data breaches and received free services as compensation. In particular, 7 participants expressed their doubts about the effectiveness of identity theft protection in relation to the associated cost. P22 said: *"It feels like you're giving them money for nothing. Also I don't know if I believe them because they can't own all of my data, so how are they actually protecting me?"*

For the 4 participants who had initiated a credit freeze, only P19 paid to have her report frozen at all three NCRAs after the breach. P16 froze his credit at all three NCRAs for free since he had been a documented victim of a previous data breach. P12 placed a credit freeze only at Equifax, which was offered for free. P20 placed only a free credit freeze at ChexSystems, a smaller-scale credit bureau. Almost one third of participants (7) expressed that freezing and unfreezing credit reports should be free, not only for Equifax but also for other credit bureaus.

Some (5) participants viewed identity theft protection services as a waste of money. P3 said: *"I'm poor. I'm having a hard time keeping my head above water or staying. I'm not giving them [credit bureaus] money for their profits."* P8 considered these services as an unwise investment: *"It wouldn't*

be worth paying for something like that, but if I had a lot of assets then I would pay for something like that, because I'd be more likely to lose money."

5.4.3 Optimism bias

A few (5) participants attributed their reason for inaction to the perceived low likelihood of being affected by the breach, making the assumption that whoever had access to the stolen data would target people who were more affluent and had a better credit history. P9 described himself as "a small fish in the pond": *"Why would they come after me? If they're going to go to all the bother of stealing my identity, why don't they go after somebody with some real wealth?"* It is worth noting that this stance was not limited to those with lower income. P1, who claimed to have an affluent income and high credit scores, did not consider herself a target either: *"These days people can be so tricky about applying for things in your name [...] and especially people who had good credit. I would think they would definitely target them. Someone like my son who has a high FICO score they might make that a priority."*

5.4.4 Tendency to delay actions

A fourth reason for inaction is a general retroactive way of dealing with risks. Six (6) participants stated that they have not noticed anything bad happen to them since the breach occurred, and saw this as reassurance that no protective actions were needed. When asked about why she did not do anything in response to the breach, P10 said: *"I haven't had any problems with my credit since that happened, that I heard about, so I'm not too concerned."* Three (3) participants noted that this might not be the most effective approach, but such awareness was not enough to trigger action. For instance, P9 shared his general attitudes towards risks in life: *"Right now, I don't have any problems, so I'm not really going to worry about it, and that's probably a very bad attitude, but I have enough problems in life without looking for trouble."* Similarly, P23 reflected that she might not have a very proactive approach: *"I wait until something bad happens and then I will react to it, so maybe it's not as good as a proactive approach. So far I think I'm okay with all the finance and nobody's stole my identity yet."*

5.4.5 Sources of advice for initiated actions

For participants who did initiate actions, 10 said they were motivated or reminded to take actions after receiving advice from a variety of sources. News media were brought up most often, primarily informing participants about the breach and available options rather than prompting actions. For instance, P9 reflected he heard of the breach from NBC Nightly News but did not follow their recommendations: *"I'm not sure which company it was, Equifax or which one, but I remember, it's been a while [...] consumers were supposed to take action and do something, but I didn't pay much attention to it because I didn't feel threatened."* Four (4) participants mentioned TV advertisements of LifeLock as the information source of identity theft protection, but none of them had signed up for the service.

In contrast, 4 participants who learned about available actions from sources they trusted (e.g., family members, colleagues, and experts) followed the given advice. P19 talked about how she decided to initiate credit freezes after hearing recommendations from a colleague: *"He's our tech guy, he put together an e-mail from various things that he'd seen about how to find out and what to do, and so I finally did something."* P16 followed a security expert's advice to place credit freezes at all three big NCRAs after he was involved in a previous data breach: *"There's a gentleman named Brian Krebs, who is active in the security community, and he gave a very informative article about what's involved with credit freezes, and why he chose to take that path to protect his credit. Given the way I use credit and given the way I have a very good credit rating, and given the data breaches it made a lot of sense for me to do that."* P16 also mentioned that he shared Krebs' article to his family members after knowing his son was affected by the Equifax breach.

5.4.6 False sense of security

Three (3) participants mentioned that taking actions created a *"false sense of security"* (P16) that led to them not taking other actions. P19, for example, after freezing her credit report at all three bureaus, did not continue to monitor her credit reports or accounts: *"I downloaded the reports so I had a copy of it then, but I haven't done anything since then with regards to looking at it, since I assumed that the freeze is working. I guess I am trusting the freeze, and also I just don't want the hassle of having to worry about it all the time."* P16 said how, after he was involved in a prior data breach and froze his report, he checked his reports once a year instead of increasing the frequency at which he checked his reports, which he thought he should do. He was also aware that a credit freeze cannot fully eliminate the risk of identity theft: *"I think the credit freeze can help with some of it, but again it depends on the institution that they're using... let's say for example it was a car loan. If somebody was able to misrepresent themselves as me they might be able to get the loan, and because the person didn't find out that there was a credit freeze, maybe there's an agency or maybe someone else besides the big three that is used to verify someone's credit information. That would be a concern to me."*

5.4.7 Usability issues

Usability issues did not necessarily deter participants from taking actions but still affected their experience. Two (2) participants mentioned the need to use a PIN to lift the freeze was inconvenient. P8 described how a credit freeze created a lot of hassles for her elderly parents: *"I know my father one time I was with him and he wanted to buy something, and he had to call the company, TransUnion, but then he couldn't remember his account, his numbers and it just seemed like it was a lot of trouble, and nowadays since you always have to know so many different passwords it makes it difficult to remember."* Another instance is P20, who initially tried to place credit freeze at NCRAs, but found it "costs money and delays things," so she eventually placed a credit freeze at a smaller bureau ChexSystems.

Participants also offered suggestions on making the information flows around credit bureaus more transparent. For instance, P5 was not satisfied that consumers could only partially check what data credit bureaus collect about them, with limited resources for intervention: *"I think that I can learn what they know about me, but I don't have the power and the access to find out ... well, I guess it should be equal, those reporting should be the same as those who have their name reported, but I'm skeptical."* P23 expressed confusion about different credit scores provided by different bureaus,

and argued that they should all be the same. Some participants stated that Equifax should communicate more openly about its mistake, instead of publishing a website and assigning the responsibility of checking and taking actions to consumers. P21 said: *"They should have reached out to their companies or their customers. Be very open about what exactly happened to the extent possible on a personal basis and communicate that to me personally."* P16 offered a general suggestion to the credit reporting system: *"I think the best way to regulate them is to define the boundaries around privacy and data, and then to come up with means and standards to protect that information. Then on top of that there should be means for consumers to work with those companies to have them respond to errors and misinformation, and to meet consumer needs."*

6. DISCUSSION

Our findings provide insights on the reasons why consumers' concerns and risk awareness did not translate into protective behaviors after the Equifax data breach. Next, we first discuss potential limitations of our study, before summarizing our key insights and discussing the implications of our findings for public policy, technical solutions, and educational efforts.

6.1 Limitations

Our study has certain limitations. First, as is common for qualitative research [50], our sample size cannot support quantitative conclusions about the general U.S. population. We also acknowledge that our sample exhibits a higher level of education on average. However, we believe our study provides rich qualitative insights on people's mental models of credit bureaus and hurdles in taking protective actions after data breaches. Findings like optimism bias and a reactive approach to dealing with risk are unlikely to be specific to more educated people. We recruited a demographically diverse sample to gather a wide range of issues, perceptions and perspectives. Furthermore, while we studied credit bureaus and protective behavior in the context of the 2017 Equifax breach, our findings provide insights beyond this particular data breach.

Second, we conducted our study four months after the 2017 Equifax breach was made public. This may have resulted in a dilution effect — a decrease in awareness of the breach during the time between the breach and our interviews. We chose the timing deliberately to ensure participants had sufficient time to take any protective actions they might want to take. Although most participants had vague memory of the details of the breach, they still remembered clearly that it occurred as well as what actions they did and did not take, and were able to articulate the reasons why.

Third, our study is limited by the self-reported nature of interviews. Participants may overclaim their security and privacy concerns due to social desirability bias. To mitigate this issue, we designed our interview script to avoid biasing participants about security and privacy risks, giving them opportunities to bring up details of their own attitudes and actions before prompting them about protective measures.

6.2 Key Insights

Our findings reveal that protective actions were less influenced by mental models and risk perception, but more influenced by costs, sources of advice, an optimism bias of "the rich will be targeted" and "I've got nothing to lose."

6.2.1 Awareness does not lead to action

Our participants' mental models of credit bureaus and their risk awareness were not the primary factors affecting their protective behaviors. In line with previous work [88, 10, 92, 91], we found connections between certain components of participants' mental models and their identity theft risk perception: for instance, the only 2 participants who mentioned the potential of tax fraud also specified government agencies as information providers of credit bureaus. A majority of participants showed detailed awareness of identity theft risks (regardless of the sophistication of their mental models), and yet most did not translate this awareness into action. For participants who had articulated mental models of credit bureaus but chose not to take action, their decisions seemed to be influenced by the misinterpretation of the outcome of existing tools and their own biases, rather than a lack of knowledge on how credit bureaus operate.

6.2.2 Costs as a barrier for protective action

A striking theme among our findings is how credit reports not only disadvantage people with low income, but on top of that, the fees associated with protective actions (such as freezing or unfreezing one's credit report) further enhance the barriers to take protective actions for people with low income. Identity theft protection, for instance, was perceived as an untrustworthy and unwise investment by about one fourth of the participants. For participants who had initiated a credit freeze, half of them did not place it at all NCRAs due to the costs at the other credit bureaus: hence, their credit freezes were not fully effective. Most participants who took actions in response to the breach chose economical options, such as checking the free annual credit report and keeping a close monitoring on existing accounts themselves.

6.2.3 Security advice as a trigger for action

Our findings confirm the significance of the source as an important factor in security advice adherence, similar to previous studies [69, 68], and provide additional insights about potential effects of different types of sources. Quite a few participants gained the awareness of the breach and certain protective actions from news media, but the awareness was not enough to trigger taking protective actions. Among those who took actions, many of them actually followed recommendations from sources with high perceived expertise and trustworthiness, rather than seeking information themselves. A possible explanation is that participants generally received high-level information of the incident from news media, but were more likely to resonate with the detailed, personal experiences provided by people they trusted. Our finding implies the importance for future research to examine how different characteristics of sources (e.g., social closeness, accessibility, quality, credibility, up-to-dateness) may affect the selection of sources and effectiveness of security advice.

6.2.4 Underestimating risk of being affected

The reasons for inaction are related to factors previously identified as preventing users from using security and privacy measures. For example, optimism bias — the general tendency of underestimating the possibility of being affected by negative events [74] — is a significant factor in affecting

privacy and security decisions [1]. Our study confirms this by showing that, regardless of participants' own income levels, they tended to think the 'rich' were more likely to become the target of identity theft. Our results exhibit similar patterns to Camp's findings [13], in that people tend to underestimate security risks when the negative consequences of previous risky behaviors are unnoticed, which reinforces the notion that protective action is not needed.

6.2.5 The "I've got nothing to lose" fallacy

Among participants with low income, the lack of motivation to take actions is similar to the well-known 'I've got nothing to hide' fallacy in privacy research [78] — some people believe they do not need to be concerned about privacy, as long as they have no secrets to hide. Similarly, several participants in our study did not exhibit strong motivations to take actions because they thought they had nothing to lose, given their limited income or assets. Nevertheless, this notion runs counter to a population survey conducted in 2013 [66]: people in low income households were highly likely to have negative online experiences, such as having email and social media accounts compromised. In addition, this survey pointed out that median households were most likely to be victims of identity theft rather than high income households [66], potentially due to the latter group being more capable of affording identity theft protection services.

6.3 Implications and Recommendations

Our findings have implications for public policy, as well as for technical and educational approaches for improving consumers' reaction to data breaches.

6.3.1 Public policy recommendations

Our findings demonstrate the need to revise or amend the Fair Credit Reporting Act to better protect consumers' sensitive information held by credit bureaus as well as lower the barriers for consumers to take sufficient protective actions.

Free and frequent access to credit reports. We argue that consumers should be able to obtain their detailed credit reports from the NCRAs for free at anytime. Under the FCRA, consumers are entitled to check their credit reports for free once a year at each NCRA. We found that participants preferred to check their credit status through banks and third-party financial management services, due to lower costs, greater convenience and usability, and the ability to more frequently check their credit scores. Nevertheless, many of these third-party offerings only show a credit score and a simplified version of the report, which may lead consumers to overlook important details in a full version report. In some cases, these services aggregate credit scores from different credit bureaus but do not explain it explicitly to participants, leading to confusion. Given these issues, and the impacts of identity theft and erroneous credit reports on someone's life, a free and frequent access to credit reports is needed to lower the barriers for consumers to monitor their credit reports for irregular activities.

Free credit freezes. Similarly, credit freezes — which are currently the most effective way of limiting undesired access to one's credit data — should be free under any circumstance in all states (some U.S. states already have state legislation mandating credit freezes to be free), as also suggested by Bruce Schneier in his congress testimony on the Equifax breach [73]. Currently, a freeze or unfreeze operation can cost up to $10 per NCRA depending on the state of residence, and this credit freeze has to be performed at each NRCA separately.

Stringent and preemptive oversight. The magnitude of the 2017 Equifax breach indicates a need for more stringent oversight of credit bureaus and better auditing credit bureaus' operation and data security. In the past, the FTC has charged both credit bureaus [28] and data furnishers [31] for violating rules of the FCRA. While such measures might be appropriate reactions after a breach occurred, our findings showed that participants in general held a negative sentiment towards credit bureaus on many aspects, such as inaccurate credit files, opaque data aggregation practices, and inappropriate handling of data breaches. In addition to remedial enforcement, more emphasis should be placed on preemptive oversight measures (such as detecting and preventing misconduct through audits), in order to ensure the security and accuracy of consumer credit data.

6.3.2 Technical recommendations

Accompanying public policy reform, better technical solutions should be implemented to ensure that regulatory efforts result in improved protective measures for consumers.

Enhancing usability of protection mechanisms. Our findings revealed the tools consumers use to manage their credit data have severe usability issues: participants experienced hassles when using some of the tools (e.g., forgetting whether a credit freeze had been placed), or avoided using them due to low perceived trustworthiness. Educating consumers about protective actions would not make sense unless these usability issues are addressed. We argue that credit freezes, for instance, should be offered as an integrated, user-friendly system. Similar to fraud alerts, credit freeze requests should be automatically communicated between all three NCRAs, rather than requiring consumers to work through (and pay for) the steps of freezing or unfreezing their credit with each bureau.

Enhancing transparency of information flows. Further research should focus on making credit-related information flows more transparent and on re-thinking how consumers can be integrated into these information flows. Our study shows that the opaque data collection and aggregation process of credit bureaus leads to misconception: some participants believed they were not included in credit bureaus' databases since they had no credit card, whereas in reality credit bureaus can still collect data about them from other information providers such as car dealerships and utility companies. Compounding this is how consumers cannot opt out of Equifax's services. Even though they can avoid using certain paid services, such as credit monitoring, consumers have no control over the information exchange between NCRAs or other credit bureaus and their data providers.

Nevertheless, efforts can be made to make the information flows more transparent with higher engagement from consumers. One possibility is to develop just-in-time notifications informing consumers whenever companies request access to their credit data, new data is added to their credit file, or any credit bureau creates a credit file about them.

Such a notification system could be a centralized offering, similar to the FTC's annual credit report website, or (less ideally) offered by individual credit bureaus. Once a consumer signed up for this service and their identity has been verified, these notifications could be delivered in various formats (e.g., mobile app, text message, email). These notifications should also be quick to read and easy to understand.

Such notifications could even be combined with an approval process between credit bureaus and consumers when a credit request is made by a third party, so that consumers have the agency to allow or deny those requests [73] — similar to permission requests on smartphones. Moreover, given how for some participants the current dispute process is problematic and can erode trust, dispute options could be integrated directly into this notification system. For instance, consumers could immediately raise a red flag when they notice wrong data being added to their files, thus making the dispute process function more timely and efficient. This might lead to higher quality of credit data overall, thus benefiting not only consumers, but credit bureaus and lenders as well.

6.3.3 Educational efforts

Furthermore, the implementation of regulatory and technical measures should be accompanied by the development and assessment of effective consumer education. Similar to previous findings [18], participants in our study showed a limited understanding of existing tools such as credit freeze and fraud alert, and frequently misinterpreted their outcomes.

Aiming educational resources at influencers. Efforts to educate consumers about financial literacy and identity theft protection should aim to enhance not only the understanding of key financial concepts, but also the aptitude in managing personal finances and making reasonable financial decisions [70]. While making resources more widely accessible online is important, our findings suggest that provisioning resources alone is not sufficient to reach the majority of consumers. Our participants tended to act primarily upon advice from people they trusted rather than news and online resources, and the fact that no participant mentioned the abundant free resources on identity theft protection, such as the FTC's identity theft website, illuminates the significant gap between consumers' awareness and available public resources. However, it also suggests an interesting opportunity: enlisting financially-literate or tech-savvy consumers as 'influencers' to educate their community. Rather than creating 'one-size-fits-all' educational materials and resources, help people who are already motivated and well versed in these matters better communicate ideas and recomendations to others.

7. CONCLUSION

We examined consumers' mental models of credit bureaus, risk perceptions, and reasons for taking or not taking protective action in the context of the 2017 Equifax data breach. We found that mental models varied, especially with regards to information flows and information providers of credit bureaus. We also found that identity theft and privacy invasion were perceived as the primary and secondary risks of this breach, with most participants demonstrating a good understanding of how these risks may manifest. But more importantly, we found that, overall, the accuracy or completeness of consumers' mental model, and awareness of the data breach and its risks, did little to explain consumers' inaction; instead, factors such as insufficient knowledge regarding protective actions, optimism bias, a belief that only 'rich' people would be targets, a tendency to delay actions, a false sense of security, usability issues, and associated fees played a much more prominent role.

In line with our findings, we propose directions for future research. One is to confirm and quantify our results through larger-scale surveys, examining the prevalence of our identified reasons for taking or not taking protective measures, and also formalizing the aspects of mental models we identified through structural equation modeling. Another direction is to conduct longitudinal studies to investigate whether there is any significant shift of consumers' attitudes and behaviors in reaction to a data breach over time. Furthermore, future research should analyze other types of non-self-reported data that may better represent consumers' actual behaviors, such as comments regarding the breach on social media, and numbers of credit freezes placed at each NCRA.

We outline implications and recommendations for public policy, technical and educational efforts aimed at enhancing consumer protections and empowering consumers to more effectively protect themselves after data breaches. Efforts in these areas should be pursued simultaneously in order to increase chances of success. Consumer protection regulation needs to be augmented with usable protection mechanisms and systems that make the credit system's information flows more transparent. At the same time, new systems are needed to better integrate consumers into these information flows through just-in-time notifications and integrated approval and dispute capabilities. However, on their own new usability and technology solutions are unlikely to be adopted by NCRAs due to little incentive to provide usable or free measures to consumers, unless mandated through regulatory oversight. Educational efforts, furthermore, are needed to make consumers aware of their rights and available choices and guide them to take actions.

So far, the 2017 Equifax data breach has not resulted in regulatory changes, despite efforts by consumers and policy makers. A class action lawsuit against Equifax by consumers is on-going [5]. The Consumer Financial Protection Bureau (CFPB) has received more than 20,000 complaints regarding the Equifax data breach, but the CFPB has not yet responded [79]. Recently, bills have been introduced in Congress aiming to impose stricter penalties for data breaches [87] and to make fraud alerts and credit freezes more accessible for consumers [86]. Nevertheless, Congress has not been able to translate these proposals into legislation due to conflicting interests, particularly from industry [56], resulting in counter proposals that instead would make it easier for financial institutions to evade responsibilities when a data breach occurs [53].

While we conducted our study in the context of credit bureaus and the 2017 Equifax data breach, we believe that our findings also provide indications as to why people might not act after data breaches in general. The combination of optimism bias, usability issues, and financial hurdles seems to be a powerful deterrent to protective actions, which requires further investigations in other contexts and the development of holistic approaches to address these issues together rather than focusing only on one or a subset of them.

8. REFERENCES

[1] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, et al. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50(3):44, 2017.

[2] A. Acquisti, L. Brandimarte, and G. Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015.

[3] A. Acquisti, L. K. John, and G. Loewenstein. The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*, 49(2):160–174, 2012.

[4] I. Adjerid, A. Acquisti, L. Brandimarte, and G. Loewenstein. Sleights of privacy: Framing, disclosures, and the limits of transparency. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, page 9. ACM, 2013.

[5] E. Ambrose. How to get in on a class-action lawsuit against equifax. `https://finance.yahoo.com/news/class-action-lawsuit-against-equifax-174234204.html`, 2018. last accessed on: 05.22.2018.

[6] T. Armerding. The 17 biggest data breaches of the 21st century. `https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html`, 2017. last accessed on: 02.12.2018.

[7] J. Aronson. A pragmatic view of thematic analysis. *The qualitative report*, 2(1):1–3, 1995.

[8] Association of Corporate Counsel. The fair and accurate credit transactions act (FACTA). `http://www.acc.com/legalresources/quickcounsel/tfaacta.cfm`, 2011. last accessed on: 01.22.2018.

[9] A. Bahney. Credit freeze: What is it and should you do it? `http://money.cnn.com/2017/09/12/pf/what-is-a-credit-freeze/index.html`, 2017. last accessed on: 02.12.2018.

[10] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2011.

[11] J. Bromberg, T. Alexander, S. Kerney, and V. Tarpinian. Identity theft services: Services offer some benefits but are limited in preventing fraud. Technical report, Government Accountability Office, Washington D.C., United States, 2017.

[12] D. Cameron. Equifax has been sending consumers to a fake phishing site for almost two weeks. `https://gizmodo.com/equifax-has-been-sending-consumers-to-a-fake-phishing-s-1818588764`, 2017. last accessed on: 01.22.2018.

[13] L. J. Camp. Mental models of privacy and security. *IEEE Technology and society magazine*, 28(3), 2009.

[14] L. J. Camp, F. Asgharpour, D. Liu, and I. Bloomington. Experimental evaluations of expert and non-expert computer users' mental models of security risks. *Proceedings of WEIS 2007*, 2007.

[15] Consumer Financial Protection Bureau. Key dimensions and processes in the US credit reporting system: A review of how the nation's largest credit bureaus manage consumer data. Technical report, Washington, DC: US Government Printing Office, 2012.

[16] Consumer Financial Protection Bureau. Measuring financial well-being: A guide to using the CFPB Financial Well-Being Scale. `https://www.consumerfinance.gov/data-research/research-reports/financial-well-being-scale/`, 2015. last accessed on: 02.16.2018.

[17] Consumer Financial Protection Bureau. CFPB orders TransUnion and Equifax to pay for deceiving consumers in marketing credit scores and credit products. `https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-transunion-and-equifax-pay-deceiving-consumers-marketing-credit-scores-and-credit-products/`, 2017. last accessed on: 01.22.2018.

[18] L. K. Cox. Your credit cards keep getting hacked: Only 1% use credit freezes. `https://www.creditsesame.com/blog/credit/credit-cards-hacked-only-one-percent-fight-back-with-credit-freezes/`, 2017. last accessed on: 02.12.2018.

[19] K. Craik. The nature of explanation. *Cambridge University, Cambridge UK*, 1967.

[20] B. Cude, F. Lawrence, A. Lyons, K. Metzger, E. LeJeune, L. Marks, and K. Machtmes. College students and financial literacy: What they know and what we need to learn. *Proceedings of the Eastern Family Economics and Resource Management Association*, 102(9):106–109, 2006.

[21] K. Dake. Orienting dispositions in the perception of risk: An analysis of contemporary worldviews and cultural biases. *Journal of cross-cultural psychology*, 22(1):61–82, 1991.

[22] A. E. Dastagir. Equifax data breach: I tried to freeze my credit. there were problems. `https://www.usatoday.com/story/money/2017/09/13/equifax-data-breach-tried-freeze-my-credit-there-were-problems/663014001/`, 2017. last accessed on: 01.22.2018.

[23] S. Dekker and E. Hollnagel. Human factors and folk models. *Cognition, Technology & Work*, 6(2):79–86, 2004.

[24] M. Douglas and A. Wildavsky. *Risk and culture: An essay on the selection of technological and environmental dangers*. Univ of California Press, 1983.

[25] M. Fagan and M. M. H. Khan. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 59–75, 2016.

[26] L. Fair. Fraud alerts vs. credit freezes: FTC FAQs. `https://www.ftc.gov/news-events/blogs/business-blog/2017/09/fraud-alerts-vs-credit-freezes-ftc-faqs`, 2017. last accessed on: 01.22.2018.

[27] Federal Reserve System. Credit reports and credit scores. `https://www.federalreserve.gov/creditreports/pdf/credit_reports_scores_2.pdf`, 2017. last accessed on: 01.22.2018.

[28] Federal Trade Commission. Nation's big three consumer reporting agencies agree to pay $2.5 million to settle ftc charges of violating fair credit reporting act. https://www.ftc.gov/news-events/press-releases/2000/01/nations-big-three-consumer-reporting-agencies-agree-pay-25, 2000. last accessed on: 01.22.2018.

[29] Federal Trade Commission. Fair and accurate credit transactions act of 2003. https://www.ftc.gov/enforcement/statutes/fair-accurate-credit-transactions-act-2003, 2003. last accessed on: 01.22.2018.

[30] Federal Trade Commission. Report to congress under section 319 of the fair and accurate credit transactions act of 2003. Technical report, Washington DC: US Government Printing Office, 2012.

[31] Federal Trade Commission. Debt collector settles ftc charges it violated fair credit reporting act. https://www.ftc.gov/news-events/press-releases/2016/05/debt-collector-settles-ftc-charges-it-violated-fair-credit, 2016. last accessed on: 01.22.2018.

[32] B. Fischhoff, P. Slovic, S. Lichtenstein, S. Read, and B. Combs. How safe is safe enough? a psychometric study of attitudes towards technological risks and benefits. *Policy sciences*, 9(2):127–152, 1978.

[33] J. L. Fleiss, B. Levin, and M. C. Paik. *Statistical methods for rates and proportions*. John Wiley & Sons, 2013.

[34] A. Forget, S. Pearman, J. Thomas, A. Acquisti, N. Christin, L. F. Cranor, S. Egelman, M. Harbach, and R. Telang. Do or do not, there is no try: user engagement may not improve security outcomes. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 97–111, 2016.

[35] J. W. Forrester. Counterintuitive behavior of social systems. *Technological Forecasting and Social Change*, 3:1–22, 1971.

[36] D. Gentner and A. L. Stevens. *Mental models*. Psychology Press, 2014.

[37] K. B. Grant. How to protect yourself after the Equifax breach: Assume you're affected. https://www.cnbc.com/2017/09/08/how-to-protect-yourself-after-the-equifax-data-breach.html, 2017. last accessed on: 01.22.2018.

[38] M. Hadi and B. Logan. Equifax: Hackers may have the personal details of 143 million US customers. http://www.businessinsider.com/equifax-hackers-may-have-accessed-personal-details-143-million-us-customers-2017-9, 2017. last accessed on: 01.22.2018.

[39] M. Harbach, M. Hettig, S. Weber, and M. Smith. Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 2647–2656. ACM, 2014.

[40] E. Harrell and L. Langton. *Victims of identity theft, 2014*. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, 2015.

[41] M. Helander, T. Landauer, and P. Prabhu. Mental models and user models. In *Handbook of human-computer interaction*, pages 49–63. Elsevier, 1997.

[42] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne. The psychology of security for the home computer user. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 209–223. IEEE, 2012.

[43] I. Ion, R. Reeder, and S. Consolvo. "... no one can hack my mind": Comparing expert and non-expert security practices. In *SOUPS*, volume 15, pages 1–20, 2015.

[44] L. Irby. 8 people who check your credit report. https://www.thebalance.com/people-who-check-credit-report-960517, 2017. last accessed on: 02.12.2018.

[45] A. Johnson. Equifax breaks down just how bad last year's data breach was. https://www.nbcnews.com/news/us-news/equifax-breaks-down-just-how-bad-last-year-s-data-n872496, 2018. last accessed on: 05.22.2018.

[46] P. N. Johnson-Laird. Mental models and reasoning. *The nature of reasoning*, pages 169–204, 2004.

[47] A. Klein. The real problem with credit reports is the astounding number of errors. https://www.brookings.edu/research/the-real-problem-with-credit-reports-is-the-astounding-number-of-errors/, 2017. last accessed on: 01.22.2018.

[48] S. Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64:122–134, 2017.

[49] T. Kude, H. Hoehle, and T. A. Sykes. Big data breaches and customer compensation strategies: Personality traits and social influence as antecedents of perceived compensation. *International Journal of Operations & Production Management*, 37(1):56–74, 2017.

[50] J. Lazar, J. H. Feng, and H. Hochheiser. *Research methods in human-computer interaction*. Morgan Kaufmann, 2017.

[51] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, pages 501–510. ACM, 2012.

[52] R. Lipshitz and O. Ben Shaul. Schemata and mental models in recognition-primed decision making. *Naturalistic decision making*, pages 293–303, 1997.

[53] M. Litt. Three bills in congress this week would let equifax off the hook. https://uspirg.org/news/usp/three-bills-congress-week-would-let-equifax-hook, 2018. last accessed on: 05.22.2018.

[54] A. Lusardi and O. S. Mitchell. How ordinary consumers make complex economic decisions: Financial literacy and retirement readiness. *Quarterly Journal of Finance*, 7(03):1750008, 2017.

[55] M. Mahoney. Errors and gotchas: How credit report errors and unreliable credit scores hurt consumers. Technical report, Washington, DC: Consumers Union, 2014.

[56] M. Matishak. After equifax breach, anger but no action in congress.

https://www.politico.com/story/2018/01/01/equifax-data-breach-congress-action-319631, 2018. last accessed on: 05.22.2018.

[57] A. Naini. Equifax and wells fargo reveal what's offensively wrong with forced arbitration. http://www.nydailynews.com/opinion/equifax-wells-fargo-reveal-wrong-forced-arbitration-article-1.3520644, 2017. last accessed on: 02.15.2018.

[58] National Financial Educators Council. Test your knowledge with the nfec financial foundation test. https://www.financialeducatorscouncil.org/financial-foundation-test/, 2017. last accessed on 01.22.2018.

[59] D. A. Norman. Some observations on mental models. *Mental models*, 7(112):7–14, 1983.

[60] K. Olmstead and A. Smith. Americans and cybersecurity. Technical report, The Pew Research Center, 2017.

[61] M. Osakwe. What's the difference between fraud alerts and credit freezes? https://www.huffingtonpost.com/entry/whats-the-difference-between-fraud-alerts-and-credit_us_596e4acde4b07f87578e6c7b, 2017. last accessed on: 01.22.2018.

[62] M. W. Perl. It's not always about the money: Why the state identity theft laws fail to adequately address criminal record identity theft. *J. Crim. L. & Criminology*, 94:169, 2003.

[63] Ponemon Institute. The aftermath of a data breach: Consumer sentiment. Technical report, Ponemon Institute LLC, 2014.

[64] E. Rader and R. Wash. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, 1(1):121–144, 2015.

[65] E. Rader, R. Wash, and B. Brooks. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, page 6. ACM, 2012.

[66] L. Rainie, S. Kiesler, R. Kang, and M. Madden. Online identity theft, security issues, and reputational damage. Technical report, 2013.

[67] S. Rayner and R. Cantor. How fair is safe enough? the cultural approach to societal technology choice. *Risk analysis*, 7(1):3–9, 1987.

[68] E. M. Redmiles, S. Kross, and M. L. Mazurek. How i learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 666–677. ACM, 2016.

[69] E. M. Redmiles, A. R. Malone, and M. L. Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *Security and Privacy (SP), 2016 IEEE Symposium on*, pages 272–288. IEEE, 2016.

[70] D. L. Remund. Financial literacy explicated: The case for a clearer definition in an increasingly complex economy. *Journal of Consumer Affairs*, 44(2):276–295, 2010.

[71] S. Romanosky, R. Telang, and A. Acquisti. Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, 30(2):256–286, 2011.

[72] Y. Sawaya, M. Sharif, N. Christin, A. Kubota, A. Nakarai, and A. Yamada. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 2202–2214. ACM, 2017.

[73] B. Schneier. Me on the equifax breach. https://www.schneier.com/blog/archives/2017/11/me_on_the_equif.html, Nov 2017. last accessed on: 02.12.2018.

[74] T. Sharot. The optimism bias. *Current biology*, 21(23):R941–R945, 2011.

[75] R. Shay, I. Ion, R. W. Reeder, and S. Consolvo. My religious aunt asked why i was trying to sell her viagra: experiences with account hijacking. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, pages 2657–2666. ACM, 2014.

[76] J. F. Short. The social fabric at risk: toward the social transformation of risk analysis. *American sociological review*, 49(6):711–725, 1984.

[77] C. Skeath. Delaware amends data breach notification law to require credit monitoring, attorney general notification. https://www.insideprivacy.com/data-security/data-breaches/delaware-amends-data-breach-notification-law-to-require-credit-monitoring-attorney-general-notification/, 2017. last accessed on: 01.22.2018.

[78] D. J. Solove. I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.*, 44:745, 2007.

[79] E. Stewart. Consumers have filed thousands of complaints about the equifax data breach. the government still hasn't acted. https://www.vox.com/policy-and-politics/2018/4/30/17277172/equifax-data-breach-cfpb-elizabeth-warren-mick-mulvaney, 2018. last accessed on: 05.22.2018.

[80] E. Stobert and R. Biddle. The password life cycle: user behaviour in managing passwords. In *Proc. SOUPS*, 2014.

[81] P. Szewczyk and S. Furnell. Assessing the online security awareness of australian internet users. 2009.

[82] The Federal Trade Commission. Consumer reports: What information furnishers need to know. https://www.ftc.gov/system/files/documents/plain-language/bus33-consumer-reports-what-information-furnishers-need-know_0_0.pdf, 2016. last accessed on 01.22.2018.

[83] The Federal Trade Commission. The equifax data breach: What to do. https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do, 2017. last accessed on 02.12.2018.

[84] The Federal Trade Commission. Identity theft recovery steps. https://www.identitytheft.gov/, 2018. last accessed on: 02.15.2018.

[85] S. Vosniadou and W. F. Brewer. Mental models of the earth: A study of conceptual change in childhood. *Cognitive psychology*, 24(4):535–585, 1992.

[86] Warren, Elizabeth. S.1816 - freedom from equifax exploitation act. Technical report, United States Congress, 2018.

[87] Warren, Elizabeth. S.2289 - data breach prevention and compensation act of 2018. Technical report, United States Congress, 2018.

[88] R. Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, page 11. ACM, 2010.

[89] M. D. White and C. Fisher. Assessing our knowledge of identity theft: The challenges to effective prevention and control efforts. *Criminal Justice Policy Review*, 19(1):3–24, 2008.

[90] H. Xia and J. C. Brustoloni. Hardening web browsers against man-in-the-middle and eavesdropping attacks. In *Proceedings of the 14th international conference on World Wide Web*, pages 489–498. ACM, 2005.

[91] Y. Yao, D. L. Re, and Y. Wang. Folk models of online behavioral advertising. In *CSCW*, pages 1957–1969, 2017.

[92] E. Zeng, S. Mare, and F. Roesner. End user security & privacy concerns with smart homes. In *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

APPENDIX

A. INTERVIEW GUIDE

1. Could you tell me how you manage your personal finance, such as income and credit cards? Has it changed over time?
   (a) If yes, could you tell me any particular points that the change occurred?
   (b) If no, could you explain why?
2. What's the first thing that comes into your mind when you hear the term "credit bureau"?
   (a) From your point of view, what do credit bureaus do?
   (b) You just said credit bureaus do... How do they do this? Could you draw or sketch on the paper to make it clear? (A few prompts listed as below if necessary)
      i. What information do they collect?
      ii. What parties do they share information with?
      iii. What do they know about you?
      iv. What information you can get from them?
      v. What is their purpose?
   (c) Could you name some credit bureaus?
3. Could you tell me your personal experience with credit bureaus?
   (a) Have you ever interacted with credit bureaus directly?
      i. If yes, when was the last time, and how was the experience?
      ii. If no, could you explain why?
   (b) What do you know about your credit history and credit scores?
   (c) Have you ever checked your credit report?
      i. If yes, when was the last time? What prompted you to check it? How did you do it? With which credit bureau? Only one or multiple?
      ii. If no, why not?
   (d) Have you ever checked your credit score? (if they have checked report, ask if credit report included credit score)
      i. If yes, when was the last time? What prompted you to check it? How did you do it? With which credit bureau? Only one or multiple?
      ii. If no, why not?
   (e) Do you feel that credit bureaus have an impact on your life?
      i. If yes, what is the impact?
      ii. If no, could you explain why not?
4. Have you ever heard of Equifax?
   (a) If yes, what do you know about it?
   (b) If no, "Equifax is one of the big three consumer-focused credit bureaus in the United States".
5. Equifax experienced a data breach in 2017. How much do you know about the data breach of Equifax?
   (a) Have you ever heard of this Equifax data breach before this interview?
      i. If yes, could you describe what happened based on your understanding?
      ii. If no, "It happened between May and July in 2017 and compromised the personal information (i.e. names, addresses, birth dates and Social Security Numbers) of over 145 million Americans".
   (b) In your view, what are the potential consequences of this breach?
   (c) What was your reaction when you heard about the Equifax data breach?
   (d) How do you feel about your data at Equifax now? Did it change after the breach?
   (e) Do you know if you were personally affected by this breach?
      i. Do you know if data about you was exposed in the data breach?
         A. If yes, how do you know?
      ii. Did you check if you were affected?
         A. If yes, how did you do it?
      iii. Did you check your credit reports at any point since you learned about the breach?
         A. When did you do it? How often?
         B. How did you do it?
         C. Only at Equifax or also at other credit bureaus?
   (f) Do you know what you could do to protect your credit data in general?
   (g) Did you do anything to protect yourself in response to the breach?
      i. Have you heard of fraud alerts?
         A. Can you describe what it is?
         B. Have you placed a fraud alert before or after the Equifax data breach?
         C. Can you describe how?
         D. With Equifax? With other credit bureaus? Which ones?
         E. Did you pay money for it?
         F. How long has the fraud alert been active for?

ii. Have you heard of a credit freeze?
   A. Can you describe what it is?
   B. Have you placed a credit freeze before or after the Equifax data breach?
   C. Can you describe how?
   D. With Equifax? With other credit bureaus? Which ones?
   E. Did you pay money for it?
   F. How would you unfreeze your credit?
iii. Did you start monitoring your credit and bank accounts more often since then?
   A. Can you describe how?
   B. With Equifax? With other credit bureaus? Which ones?
   C. Do you pay money for it?
iv. Have you heard of identity theft protection?
   A. Can you describe what it is?
   B. Have you signed up for any identity theft protection services?
   C. Can you describe how?
   D. With what company/entity?
   E. Do you pay money for it?
v. Did you do any other things not mentioned previously?

6. Before this breach occurred...
   (a) Have you ever experienced any data security problem, such as someone secretly changed your password?
   (b) Have you ever experienced identity theft, such as someone applying for credit cards under your name? (For each question, if yes, follow up with "Could you tell me more about the experience? Do you feel it has any impact on you?")

B. SCREENING SURVEY

Thank you for your interest in our study! Please answer a few questions about your demographics and availability for the interview.

1. In which year were you born?
2. What is your current gender identity?
   (a) Male
   (b) Female
   (c) Non-binary/third-gender
   (d) Not listed (please specify)
   (e) Prefer not to answer
3. What is the highest level of education you have completed?
   (a) Less than high school
   (b) High schhol degree or equivalent
   (c) Some college but no degree
   (d) Trade, technical, or vocational degree
   (e) Associate's degree
   (f) Bachelor's degree
   (g) Master's degree
   (h) Doctoral degree
   (i) Professional degree (JD, MD, etc.)
   (j) Other (please specify)
   (k) Prefer not to answer
4. Which of the following categories best describes your occupation?
   (a) Administrative support (e.g., secretary, assistant)
   (b) Art, Writing, or Journalism (e.g., author, reporter, sculptor)
   (c) Business, Management, or Financial (e.g., manager, accountant, banker)
   (d) Education or Science (e.g., teacher, professor, scientist)
   (e) Homemaker
   (f) Legal (e.g., lawyer, law consultant, or law professor)
   (g) Medical (e.g., doctor, nurse, dentist)
   (h) Engineering or IT Professional (e.g., programmer, IT consultant)
   (i) Service (e.g., retail clerk, server)
   (j) Skilled Labor (e.g., electrician, plumber, carpenter)
   (k) Unemployed
   (l) Retired
   (m) College student
   (n) Graduate student
   (o) Not listed (please specify)
   (p) Prefer not to answer
5. What was your total household income before taxes during the past 12 months?
   (a) Less than $25,000
   (b) $25,000 to $49,999
   (c) $50,000 to $74,999
   (d) $75,000 to $99,999
   (e) $100,000 to $124,999
   (f) $125,000 to $149,999
   (g) $150,000 or more
   (h) Prefer not to answer
6. What is your citizen status?
   (a) I am a citizen of the United States.
   (b) I am a permanent resident of the United States.
   (c) I am neither a citizen nor a permanent resident of te United States.
   (d) Other (please specify)
   (e) Prefer not to answer

   (If answer to above question was "citizen of the United States" or "permanent resident"
7. How many years have you been living in the United States?
   (a) $<$ 1 year
   (b) 1-2 years
   (c) 2-3 years
   (d) 3-4 years
   (e) 4-5 years
   (f) $>$ 5 years
   (g) Prefer not to say

C. CODEBOOK

Below is the codebook used for interview transcript analysis, grouped into four big categories.

C.1 Category: Financial Management

Financial status: Description of general financial situation, e.g., income, number of checking/saving accounts, number of credit cards currently held, late payment, as well as the mentioning of occupation, big purchases (e.g., cars and mortgages).

Financial tracking: The way to keep track of earnings and spendings, manage different credit cards, use checks or do everything online, the way of paying bills (e.g., set up automatic withdrawals or pay bills whenever it comes).

Financial behavior change: Any particular change in the ways of managing one's finance, how and why it occurred, may also include behavioral change resulting from attitudinal change (e.g., I tried to spend less because I wanted to save money).

C.2 Credit Bureau Related

Understanding of credit status: (1) The knowledge of the meaning and components of credit scores in general, how credit score is generated, whether it costs money to check credit scores, the mentioning that different bureaus may have different scores etc. (2) The impression of whether the participant's own credit score is good or bad, the description of when's the last time checking it and how to check it, where does the credit score come from (e.g., one of the three big bureaus or banks) (3) The impression of one's credit history, things included in the credit report, whether or not they have things like late payments and debts.

Awareness of credit bureaus: The number of credit bureaus, specific names of credit bureaus, also use this when they say they can't remember it or can't give the full name, also include the participant's knowledge or guess about whether there are bureaus other than the big three.

Impact of credit bureaus: "What impacts do credit bureaus have on you": how credit bureaus may impact consumer lives by giving credit ratings/scores or in other ways. Also include cases where participants say credit bureaus have little or no impact on them personally because of various reasons.

Check credit status at credit bureaus: Directly contact credit bureaus to access credit reports or sign up for other credit-related products and services, description of the process (e.g., schedule times to make use of the free opportunity to check credit reports annually).

Check credit status at other places: Usually through banks and third-party financial aggregation app (such as NerdWallet, Credit Karma, and Mint) to check credit history, credit score, or credit status in general, and the reason for doing it (e.g., it's free and more convenient), the frequency of the received updates, whether or not it might be helpful.

Reasons for no interactions: Description of having little or no interactions with credit bureaus, didn't check credit status through either credit bureaus or other places, and the reasons for doing it, e.g., I don't need to make big purchases or I don't want to know my credit status because it's poor.

Dispute process: Anything related to the dispute system within the credit reporting system, can be (1) the general telling that consumers have the right to dispute incorrect information; or (2) the complaint that the current dispute system doesn't work to solve consumers' problems (e.g., they have to spend a lot of time filing the dispute and it's hard to get the error eventually corrected).

Information providers of credit bureaus: Companies and organizations that provide information to credit bureaus, e.g., government, IRS, lending companies.

Customers of credit bureaus: Entities to which credit bureaus share or sell individual consumer's information, who may have the access to consumer credit files at credit bureaus. Also include cases where participants may not explicitly mention it but rather say it's an information exchange process, e.g., "I think that banks quarry them but they would also ask banks about".

Types of information collected: The types of information credit bureaus collect from their providers (e.g., checking accounts, savings, credit history, loans) about individual consumers, usually the answer following "what types of information do credit bureaus collect?" and "what do credit bureaus know about you?"

Offerings of credit bureaus: What information consumers can receive from credit bureaus, such as the annual free credit reports, credit reports that cost money to see credit scores, credit monitoring services.

Purpose of credit bureaus: This will refer to how credit bureaus use the collected information for, what their purposes are, e.g., assessing one's creditworthiness, generating credit scores. Answers following the question "what's the first word that you associate with credit bureaus" and "what are their purpose" might fall under this category.

Errors in mental models: This code encompass any obvious errors that we capture in participants' describing of credit bureaus.

Inaccurate credit files: Specific instance of negative perception - the experience that credit bureaus get errors on consumer credit files or retrieve the file of the wrong person, and hence leading to bad or unpleasant experience for consumers.

Opaque data aggregation process: Specific instance of negative perception - mentioning of the process how credit bureaus collect and aggregate all different types of information as opaque, unclear, not idea about what's going on behind the curtain.

Abusive use of power: Specific instance of negative perception - the mentioning that credit bureaus (and other related institutions such as governments and banks) are in the position of holding great power/have little interest in protecting consumer rights; consumers are in a relatively weak position.

Insidious data collection: Specific instance of negative perception - describing the data sharing between credit bureaus and data furnishers as passive, creepy or scary, without obtaining consent from consumers. As for consumers,

they have limited control and choice over this kind of data collection.

Positive perception of credit bureaus: Positive description of credit bureaus in general, the statement that credit bureaus have a positive image in the participant's mind.

Negative perception of credit bureaus: Negative description of credit bureaus, the statement that credit bureaus have a negative image in the participant's mind, note that if they just say "credit bureaus steal money from people" it doesn't count, there should be specific negative adjectives to describe it being bad or their negative feelings about it.

C.3 Risk Perception

Emotional feelings of the breach: The emotional feelings that participants experienced after heard of the breach (e.g., angry, disgusting, indifferent, not surprised), the emotional/attitude change towards Equifax (or other bureaus) after the breach compared to the time before.

Change of trust: Mentioning that after this breach, Equifax (or other credit bureaus) will have a less reputable image in the mind of consumers, or the participant personally will have less trust in the company.

Expectation of credit bureaus: Expectations towards Equifax, or other companies that have experienced data breaches about what they should do as the countermeasure of the breach, whether they have meet or failed the expectations in the past, as well as their expectations to these companies' future actions.

The class action lawsuit: The specific mentioning of the class action lawsuit against Equifax following the breach, whether participants might have heard of it or joined it, how they feel about it.

Prevalence of data breaches: The mentioning that there are too many previous data breaches in recent years that the occurrence of the Equifax breach doesn't make the participant too surprised, and that there is too much data available online.

Mentioning identity theft: Direct mentioning of identity theft or indirect conceptualization through examples as a consequence of the Equifax breach, or just identity theft in general.

Victims of the breach: Talking of targets that are more likely to be affected by the breach, e.g., people who have good credit.

Likelihood of being personally affected: The knowledge, assumption or assessment of whether participants themselves are personally affected, and if yes, to what extent, can be either an assured response or a guess.

Negative consequences of the breach: Mentioning consequences that's not about identity theft but can still happen after the Equifax data breach, such as invasion of personal privacy when so much personal and financial information was exposed.

Knowledge of Equifax: Impression of Equifax as a company, e.g., it's one of the big three credit bureaus, it's the one that got hacked, also include cases where participants say they've never heard of it.

Cause of the breach: The description that this breach was conducted by people other than hackers, such as governments, and/or it was profit-driven, e.g., some participants assumed that hackers will sell the stolen data to someone else, others believed that it's an internal breach and someone's disclosing the information intentionally.

Types of exposed data: Description of the general impression of some data being exposed in the Equifax data breach (e.g., a lot of personal information released) or specific types of data (e.g., SSN, credit card numbers). Also include cases where participants say they don't know.

Awareness of the breach: Memory of whether or not this participant has heard of the breach, what happened in general in the breach.

Previous data security experience: Previous experience of data security problem, such as being involved in a data breach and having password compromised somewhere.

Previous identity theft experience: Previous experience of being an identity theft victim, such as someone else applying for credit-related products under the participant's name, the effort in solving the related problems, or the reason for not conducting any kind of follow-up investigations.

C.4 Protective Actions

Check Equifax's website: The mentioning of someone (either the participant or other related people) check the Equifax website for his or her own breaching status. Also include this code when participants say they didn't check it.

Credit freeze: The action of placing a credit freeze, the interpretation of what credit freeze means/what's the expected outcome, the cost of credit freeze, why someone may want to initiate a credit freeze, their assumptions of what a credit freeze may do.

Check credit report after the breach: The mentioning of checking credit report following the data breach as a safeguard measure.

Fraud alert: The mentioning of placing a fraud alert on file, either for this breach or previous ones, their assumptions of what a fraud alert might do, the process of how to place a fraud alert.

Credit monitoring service: Enroll in credit monitoring services provided by credit bureaus, governments, or other entities.

Self-monitoring: The action of checking accounts more frequently, keeping an closer eye on them, and the related outcomes.

Identity theft protection: Conceptualization of what this type of service does, why someone may want it.

General security practices: Strategies to protect one's credit data/online privacy in general, e.g., don't disclose personal information such as SSN and passwords to others, avoiding suspicious emails, not using PayPal.

Self-initiated actions after the breach: Things that the participant has done in reaction to the breach or knows that they could have done, also include cases where they say they don't know.

Reasons for taking actions: Any reasons why the participant chose to take any one of the suggested actions above.

Reasons for not taking actions: Any reasons why the participant chose to not taking any one of the suggested actions above.

Triggering new actions: Any places where participants say they will or might consider doing some actions after the interview, the conversation inspires them to do something, and the reasons behind.

Suggestion from participants: The suggestion or proposal made by participants throughout the interview, e.g., credit bureaus shouldn't charge money for their certain offerings such as credit freeze, and there should be a consistent way to calculate credit scores.

Sources of recommendation: Protective actions recommended by anyone who's considered as reputable, trustworthy or expert by the participant, e.g., family member, financial advisor. Also include cases where participants said they provided recommendations for other people and hence became the source of knowledge.

Usability issues: Reporting about problems and hurdles participants encountered (or other people they know) when trying to initiate any one of the suggested actions.

Compensations after data breaches: Description of products and services offered by companies following previous data breaches that the participant or someone he/she knows was involved in (e.g., some companies may offer free or paid credit monitoring services and fraud alerts for victims).