Developing Questionnaire Items to Measure Identity Theft

Theresa DeMaio, Jennifer Beck[1]
U.S. Census Bureau, 4600 Silver Hill Rd, Washington, DC 20233

Abstract

Identity theft, defined as the misuse of someone's personal information for fraudulent purposes, is becoming a growing concern among policy makers. In an effort to collect detailed information on the scope and nature of identity theft, the U.S. Department of Justice asked the U.S. Census Bureau to collect these data through a supplement on the National Crime Victimization Survey (NCVS). The complex nature of this crime presented some key challenges to questionnaire development. First, because victims were eager to share all of their identity theft experiences, they tended not to differentiate between successful misuses of personal information and attempted misuses of personal information. Second, it was difficult for victims to isolate the individual misuses that made up their identity theft experience. Victims tended to think of their identity theft experiences as a single unit, rather than as an amalgamation of individual misuses. Finally, identity theft is often a "faceless crime," because identity theft involves personal information that someone can easily access without interacting with the victim. In this paper we discuss in some detail each of these challenges in collecting information about identity theft and present solutions.

Key Words: Identity theft, questionnaire development, cognitive interviews

1. Developing an Identity Theft Questionnaire

Identity theft, which involves the misuse of personal information (PI) for fraudulent purposes, is becoming a growing concern. In recent years the media increasingly has publicized consumers' stories of identity theft that range from credit card fraud to the purchase of new homes. Advertisements for products and services that monitor credit and protect against identity theft also have become more visible.

In 2005 the Federal Trade Commission (FTC), the agency responsible for protecting consumers from fraud and identity theft, reported that approximately 8.3 million Americans were victims of some form of identity theft totaling more than 15 billion dollars in consumer losses (Synovate, 2007). The prevalence and costliness of identity theft prompted the U. S. Department of Justice to begin collecting official statistics on the crime through its NCVS. The 2004 NCVS attempted to gain a surface understanding of identity theft, by including ten questions into the core crime questionnaire. The data from these questions were fairly consistent with earlier findings, revealing that approximately 3.6 million American households had at least one member who had been the victim of identity theft during the previous 6 months (U.S. Department of Justice, 2006). However, a desire for more detailed information about identity theft led the Department of Justice, the Federal Trade Commission, and several other federal agencies to develop a more extensive questionnaire, an Identity Theft Supplement to the NCVS. This supplement, administered from January to June, 2008, collects detailed information about a wide range of aspects of the identity theft experience.

This paper discusses the process of developing and pretesting the Identity Theft Supplement questionnaire. In the following sections we discuss the complicated and emotionally salient nature of identity theft that posed significant challenges to the questionnaire development process. We also discuss our methodology for pretesting the questionnaire and four significant problems that we encountered while testing it: a) getting respondents to report actual and attempted misuses of their PI correctly; b) getting respondents to categorize the types of misuse correctly; c) collecting detailed information on individual misuses of PI, and d) getting respondents to report knowledge about the identity thieves. We conclude with a discussion of the challenges of questionnaire development in these types of complex experiences.

[1] This report is released to inform interested parties of ongoing research and to encourage discussion. Any views expressed on the methodological issues are those of the authors and not necessarily those of the U.S. Census Bureau.

1.1 The Nature of Identity Theft

Identity theft is a complex experience. There are multiple ways in which the thief can access and misuse his or her victim's PI. A thief can steal the victim's wallet containing his or her driver's license and social security card, steal PIN numbers from an ATM, or steal Social Security Numbers after a security breach. Most importantly, the identity thief can easily obtain this PI without ever having to interact with the victim. Many victims have limited or no information on how the thief got a hold of his or her PI, leaving victims with limited knowledge about the source of the misuses.

Also, the ways in which identity thieves can misuse their victims' PI and the severity of the misuse are as diverse as the ways in which they can obtain it. The misuse can be as "minor" as using the victim's credit card without his or her permission or as "serious" as using the victim's credit history to buy a house. It even can involve criminal acts, such as using the victim's identity after being picked up by the police or getting health insurance and medical treatment.

This diversity of misuse makes the scope of identity theft quite broad. The misuse can be a one-time event, such as using the victim's credit card to make a single purchase. It also can involve a complex series of misuses over a long period of time. The more complicated the identity theft experience, the longer it may take victims to uncover the scope of the misuses.

Finally, because identity theft involves the misuse of PI that often is linked with the victim permanently, such as a Social Security Number, victims often describe their identity theft experience as "never ending." They express uncertainty about whether they have been able to curtail all future misuses. Also, while victims can be fairly successful at monitoring existing accounts they routinely use, they are less successful at monitoring for newly-created accounts and predicting future victimizations. Victims often do not discover these misuses for a long period of time, making it impossible to fully report all of their identity theft experiences.

Ultimately, the number of incidents, the length of time it takes for victims to discover the misuse, and uncertainty about unknown misuses complicate the process of eliciting information about the identity theft(s). The complexity of the phenomenon made it very difficult to create a set of questions that can apply to every victim's experience. The complexity also made it difficult to elicit meaningful and consistent reports about the crime. In the next sections, we highlight our pretesting methods and findings that illuminated the complex nature of identity theft.

2. Methodology

To pretest the questionnaire, we used the traditional cognitive interview method. We instructed respondents to think aloud as they answered the survey questions and followed up their responses with structured probes. The structured probes were meant to find out details about respondents' answers and their definitions for certain key terms in the questions. We used unstructured probes when the respondents' answers suggested some uncertainty in their interpretation of the question or appeared inconsistent with their answers to earlier questions. We also used unstructured probes when respondents' answers revealed a complicated situation about which the interviewer needed more information to determine the source of the problem with the question.

We conducted a total of 24 interviews between May and August, 2007. Twenty respondents were actual identity theft victims, and four were victims of attempted identity theft. Victims of attempted identity theft were people who, although they had their PI stolen, were able to contact a credit card company, for example, and stop offenders from successfully misusing that information. We recruited both kinds of identity theft victims because we wanted to make sure that victims of attempted identity theft correctly would report these misuses as unsuccessful. We had no other selection criteria for our respondents. As a result, the demographic characteristics were skewed towards females and more highly educated individuals (having more than a college degree). Table 1 contains a breakdown of respondent demographic characteristics.

Table 1: Respondent Demographic Characteristics

Sex		*Race*		*Age*				*Education*			
Male	6	*White*	13	*20-29 yrs. old*	4	*50-59 yrs old*	1	*High school*	1	*Some Graduate school*	2
Female	18	*Black*	9	*30-39 yrs. old*	6	*60-69 yrs old*	5	*Some college*	6	*Advanced degree*	7
		Asian	2	*40-49yrs. old*	7	*70-79yrs. old*	1	*College degree*	7	*Unknown*	1

The 24 interviews took place during eight iterative rounds of cognitive testing. We did not have a predetermined number of respondents per round. Some rounds had as few as two interviews, while others had up to four interviews. Our main goals were to correct significant problems with the survey questions immediately, verify that the changes we made were improvements, and continue to test the questionnaire on a wide variety of experiences.

For the remainder of the paper we will discuss the specific challenges we faced while developing and testing the Identity Theft Supplement.

3. Questionnaire Development Issues

The most significant problems we encountered during questionnaire development revolved around respondents' inability to map their identity theft experiences onto the survey questions and correctly report them. Respondents had difficulty understanding what kinds of information they should report and were hesitant to provide speculative information. This was most apparent and problematic at the beginning of the survey. If respondents inaccurately reported their experiences in the initial questions, not only would we have an inaccurate account of the identity theft experience, we also would have an incomplete picture of the crime. Respondents' answers to the earlier questions in the survey determined which questions they would answer later on in the survey.

3.1 Correctly Reporting Actual and Attempted Misuse of Information

In the early rounds of pretesting, the questionnaire collected reports of actual and attempted identity theft in two separate questions. The sponsors were more interested in collecting detailed information on successful misuses of PI than collecting information on unsuccessful misuses of PI. They also sought to measure the prevalence of specific types of misuses, as well as obtain an overall estimate of the prevalence of attempted misuses.

As the supplement initially was structured, respondents first reported the successful misuses of their personal information using the following categories: a) misuses of existing bank accounts; b) misuses of existing credit cards; c) misuses of other types of existing accounts; d) the opening of any kind of new account; e) misuses of PI for any other purposes, such as medical care, and f) any other types of misuse (see Figure 1 for the exact question wording). Then, through a single "yes/no" format question, respondents indicated if someone had attempted to misuse his or her PI in any way. Respondents were not asked to report the specific ways in which an identity thief attempted to misuse their PI. Separating reports of attempted and actual instances of misuse proved to be problematic for respondents. They tended to misreport the scope of their identity theft experience. This inaccuracy was the result of two different factors: questionnaire design effects, and respondent knowledge.

1. Since _____, 20__, has someone, without your permission:
   a. Used your existing bank account, including debit or ATM cards?
   b. Used your existing credit card account?
   c. Used another type of existing account such as your telephone, utilities, online payment account like Paypal, insurance policies, or something else?
   d. Used your personal information to open any NEW accounts such as wireless telephone accounts, credit card accounts, loans, banking, online payment or something else?
   e. Used your personal information for some other fraudulent purpose such as getting medical care, a job, or government benefits; renting an apartment or house; giving your information to the police when they were charged with a crime or traffic violation; or something else?
   f. Used your personal information in some other way?

1a. Since _____, 20__, has someone, without your permission:
   a. Attempted, but failed, to use your information in any of the ways just mentioned?

Figure 1: Initial Version of Questions for Reporting Actual and Attempted Misuses

First, and most importantly, the design of the questionnaire led respondents to misreport successful and unsuccessful misuses of their PI. When reporting the successful misuses, respondents did not know they would later be asked about attempted misuses. As a result of this lack of context, respondents often misreported attempted misuses of PI as successful misuses. Respondents listened to the various categories of successful misuses, and when they heard one that was similar to the attempted misuse, gave a positive response. Responses to later questions frequently revealed that the misuse was not successful. This response error was particularly prevalent among respondents who had experienced both attempted and actual misuses of their PI. For example, one respondent indicated that someone had misused her online banking account successfully. However, her responses to later questions revealed that, although someone had tried to get into her online banking account, it had been closed so the identity thief was unable to access it. Another respondent reported that someone had opened a new account in her name, but later probing revealed that someone had attempted to open a new account, but was unsuccessful.

Because respondents were eager to report all their identity theft experiences, and were not anticipating a separate question about attempted misuses of PI, they over-reported successful misuses of PI. To address this misreporting issue, we combined

the questions about actual and attempted misuse into a single reworded question. We first asked respondents, "…has anyone used or attempted to use" their PI, using the categories in the original question (see Figure 2). Each positive response was followed up with a question asking if the misuse was successful or unsuccessful. Combining the report of actual and attempted misuses with the follow-up question was successful at getting respondents to accurately report attempted and successful misuses. While most of the respondents in the later rounds tended to report successful misuses, respondents who reported attempted misuses did so correctly. They indicated that someone was attempting to misuse their PI (answering "yes" to the first question), but that the attempt was not successful ("no" to the follow-up question). Later questions did not reveal any discrepancies in the respondents' answers. This revision proved to be effective at getting respondents to correctly identify unsuccessful misuses.

1. Since _____, 20__, has someone, without your permission:
a. Used or attempted to use your existing bank account, including debit or ATM cards?
a.1. Were they successful in getting anything from your account?
b. Used or attempted to use your existing credit card account?
b.1. Were they successful in charging anything to your account?
c. Used or attempted to use another type of existing account such as your telephone, utilities, online payment account like Paypal, insurance policies, or something else?
c.1. Were they successful in obtaining any goods or services from this account?
d. Used or attempted to use your personal information to open any NEW accounts such as wireless telephone accounts, credit card accounts, loans, banking, online payment, or something else?
d.1. Were they successful in actually opening any NEW accounts?
e. Used or attempted to use your personal information for some other fraudulent purpose such as getting medical care, a job, or government benefits; renting an apartment or house; giving your information to the police when they were charged with a crime or traffic violation; or something else?
e.1. Were they successful in using your identity for any of these purposes?
f. Used your personal information in some other way?

Figure 2: Revised Version of Questions for Reporting Actual and Attempted Misuses

The second factor contributing to the misreporting of successful and unsuccessful misuses was the respondents' own knowledge of the scope of the misuses. Respondents often did not have detailed or sufficient knowledge of each misuse. Respondents did not always know if a particular incident was a successful or unsuccessful misuse. This lack of detailed knowledge usually was associated with how the respondent discovered the misuse. In one case a cell phone provider notified the respondent that an account had been set up in his name, but that the Social Security Number the identity thief provided did not match with the respondent's date of birth. The respondent first answered "no" to the category for the successful opening of a new account, but then changed his answer to "yes" because his records indicated that "an account was sent up in [town name]."

The identity theft experience can be ambiguous, and most respondents will not have notes and documents readily available during the survey interview. Revisions to the question wording or structure will not prompt people to give more accurate reports of misuses if they do not have sufficient information. This is one source of inaccuracy experience that questionnaire revisions could not solve.

3.2 Categorizing Identity Theft Experiences

A second significant problem we encountered during questionnaire development was that respondents had difficulty thinking about their identity theft experience in a way that was consistent with how the sponsors wanted to categorize the data. As we described previously (and Figure 1 illustrates), the sponsors were interested in separating the identity theft experience into discrete categories of misuses. Unfortunately these predetermined categories were not "cut and dried" for our respondents. Respondents made several errors when attempting to map their identity theft experience onto the response categories specified by the sponsors.

First, some respondents tended to report the same misuse in multiple categories. For example, one respondent had someone misuse her debit card to make two separate purchases: magazine subscriptions and a new internet service provider account. She correctly reported these misuses in "the misuse of existing bank account" category. However, she also went on to report each of the two charges on the debit card in additional categories. She reported the internet provider service charges as "the opening of a new account" and reported the magazine subscription charges as a misuse of her PI in "some other way." "Double-reporting" the charge for the Internet Service Provider account most likely was not a response error. This particular misuse probably fell into both categories. Not only did the identity thief purchase the service, but they also presumably had to open a new account. However, "double-reporting" the magazine subscription purchases on the debit card was a response

error. This respondent seemed to adopt an interpretation of her identity theft experience that was inconsistent with the sponsors' intent. In effect this respondent, like others, tended to characterize individual purchases and misuses of a single account in multiple ways. This type of reporting may be fairly common among people who have experienced multiple misuses of PI.

A second type of error respondents made when mapping their experiences onto the questions was reporting in the wrong category. First, some respondents tended to confuse certain types of accounts. Respondents would often misclassify the misuse of debit cards and check cards as the misuse of credit cards. This error was particularly common when the thief used the debit card as a credit card. These respondents did not differentiate between credit cards and debit cards. To some extent, this type of misclassification is not a tractable problem. Thinking of a debit card as a credit card is inherent to some people's understanding of their banking account. In this case, it is not possible to structure the initial misuse question to elicit the correct classification. However, for respondents who did differentiate between debit and credit cards, we rearranged some of the response categories. As the question was originally structured, respondents first reported any bank account and debit card misuse and were unaware that we next would be asking about credit cards. They were uncertain if the bank account category best fit the misuse of the check card. We revised the question so that respondents would be asked credit card misuse first, changing how we referenced these types of accounts, and then about bank accounts and debit cards. Figure 3 shows the revised structure and wording of the question. We hypothesized that first hearing the specific reference to "credit card accounts" would prompt respondents not to misreport the debit card misuse. While this change did help some respondents to not misreport debit card misuse as credit card misuse, the problem still persisted for respondents who did not differentiate between the two types of cards.

First, I'd like to ask you some questions about the misuse of any of your EXISTING ACCOUNTS .

1. Since _____, 20__, has someone, without your permission, misused any of your EXISTING ACCOUNTS in any of the following ways? Has someone....

a. Used or attempted to use one or more of your existing accounts, such as a bank account, credit card account, telephone account, insurance policies, or something else?

b. Did someone use or attempt to use your credit card account?

c. Were they successful in charging anything to your account?

d. Did someone use or attempt to use your checking or savings account, including debit or ATM cards?

e. Were they successful in getting anything from your account?

f. Did someone use or attempt to use another type of existing account such as your telephone, utilities, online payment account like Paypal, insurance policies, or something else?

g. Were they successful in obtaining any goods or services from this account?

Next, I have some questions about any NEW ACCOUNTS someone might have opened.

Since _____, 20__, has someone, without your permission...

h. Used or attempted to use your personal information to open any NEW accounts such as wireless telephone accounts, credit card accounts, loans, banking, online payment, or something else?

i. Were they successful in actually opening any NEW accounts?

j. Used or attempted to use your personal information for some other fraudulent purpose such as getting medical care, a job, or government benefits; renting an apartment or house; giving your information to the police when they were charged with a crime or traffic violation; or something else?

k. Were they successful in using your identity for any of these purposes?

l. Used or attempted to use your personal information in some other way?

Figure 3: Revised Version of Misuse Questions Distinguishing between New and Existing Accounts

We also observed a second type of error of commission. Two respondents did not seem to understand the distinction between the opening of new accounts and the misuse of existing accounts. Both of these respondents seemed to be searching for key words that described their particular misuse, and were not remembering the supra-ordinate categories of "existing" and "new" accounts. This confusion was most likely because of the long descriptions of misuses in each response category of the question, some of which were the same for both new and existing accounts. Ordinarily, because only two respondents seemed to be confused about the difference between new and existing accounts, making changes to a questionnaire would not be prudent. However, because this error was quite problematic for accurately collecting information on identity theft, we wanted to minimize the possibility of other respondents having the same confusion. We made a simple change to the questionnaire to make the differences between new and existing accounts more explicit. As Figure 3 shows, we developed separate introductions, which made a distinction between existing and new accounts and served to divide these two types of misuses into two separate questions. We did not observe any problems after we made this revision. The question laid out the

framework for the information in which we were interested. Respondents understood the distinction between new and existing accounts and were able to report misuses of both types of accounts correctly.

3.3 Reporting on Individual Episodes of Identity Theft

Another significant challenge came from the sponsor's wish to collect and summarize detailed information about the nature and severity of the individual misuses of PI that make up an identity theft experience. Analytically, the data are easier to interpret if the actions and effects of each separate experience can be parceled out. The sponsors also assumed that some identity theft experiences would be more salient for the victim than others, and wanted to collect information about the "most serious" misuse in the event of multiple identity theft victimizations.

However, it became clear early on in the pretesting that people who had been victims of multiple incidents were unable to think of their identity theft experiences as a series of isolated misuses. Throughout the multiple rounds of testing, and despite revisions to the questions that reinforced this limited focus, respondents were unable to limit their reporting to what they selected as the single, "most serious" misuse of PI. Some respondents found it difficult even to choose the most serious misuse or felt that the most serious aspect was not a particular misuse. For example, one respondent felt that the most serious misuse of her PI was not a misuse at all, but instead was the fact that someone had her Social Security Number, which he or she had gotten from the respondent's stolen driver's license. She ultimately selected the misuse of her bank account as the most serious misuse, but continued to report actions she took towards resolving the misuse of her credit cards.

Also, despite explicit reference to the most serious misuse, overshadowing effects still occurred when respondents answered questions about the physical and psychological effects of identity theft. Respondents should have limited their reports of emotional and physical reactions only to the most serious misuse. However, probing revealed that respondents were thinking about all of their identity theft experiences and not partitioning out the emotional and physical effects of the most serious misuse.

To address the problem of respondents not limiting their focus to the most serious misuse, we tried two different changes to this question series. First, because many questions intervened between the respondents' selection of the most serious misuse and when they were asked specific questions about it, we attempted to "remind" respondents of the most serious misuse. In questions for which the respondents needed to report on only the most serious misuse, we inserted an "automatic fill" with the misuse the respondent named in the earlier question. For example, if the respondent said that the misuse of his "bank account" was the most serious misuse, we inserted "bank account" into the text of the question. However, this change continued to be ineffective at limiting respondents' focus to the most serious misuse. As a result, we decided that it was not possible to collect these data and recommended that the sponsors not ask respondents to focus on the most serious incident. The sponsors agreed to this change, but still wanted respondents to indicate what they felt was the most serious misuse. We moved the question to the end of the supplement and no longer used it as a filter for the earlier questions.

Ultimately, because the identity theft experiences were highly salient and emotional, respondents were eager to talk about and share all of their experiences, even if the questions directed them to focus their reporting on a subset. People tended not to think of each individual misuse as a separate "crime," but instead tended to think of all misuses as a whole. This holistic view made it difficult to satisfy the sponsors' goal of collecting detailed information on the effects of different misuses of PI.

3.4 Identifying the Offender

One final challenge to developing a questionnaire on identity theft was the sometimes anonymous nature of the crime. Identity thieves can access and misuse PI, often without meeting or interacting with their victim. This anonymity made it difficult to develop questions about the identity thief and how he or she was able to access the respondent's PI.

The sponsors wanted respondents to report any information they might have about the people who stole or misused the PI, even if the information was speculative. Figures 4 and 5 show the text of these questions, which asked how someone was able to get the PI and who the offender might have been. Respondents were reluctant to provide speculative information about possible sources of the breach. Throughout the interview, respondents indicated their speculations about how their PI was stolen, but were reluctant to report this information because they did not have proof. For example, one respondent believed that her bank accidentally released her Social Security Number in a well-publicized "security breach." Although she had never received confirmation that this was how someone was able to get a hold of her Social Security Number and subsequently misuse it, she "strongly suspected" that the breach was the source. Because she had not received confirmation of her suspicions, she answered that she knew nothing about how someone was able to get her PI.

Respondents also freely offered information throughout the interview about the identity thief, but would contradict this knowledge when answering the questions designed to capture that information. This was not only attributable to people's

reluctance to incriminate others, but also to respondents' doubts about the true identity of the offender. A frequent source of identity theft for our respondents, and presumably for people outside our interviews, was a stolen wallet, purse, or credit/debit card. Several of our respondents had their wallets stolen while dining in a public place. These respondents either realized the person who bumped into them had stolen their wallet, or they never noticed the theft in the first place. As a result of the uncertainty, respondents were unwilling to report "knowing anything" about the people who misused their PI.

Also, some respondents were unwilling to divulge information about the identity thieves because they only knew the names of the people who misused their PI. Finally, identity thieves sometimes use someone else's PI under assumed names and addresses. One respondent reported not knowing anything about the people who misused his PI because he did not believe that the names and addresses on the newly opened account were real. Because he had no way of confirming the veridicality of the names and addresses, they were reluctant to provide information about these people.

Question wording was a factor in respondents' reticence to report information of interest. To address this reticence, we added wording that would allow respondents to answer these questions, even in their uncertainty. For the questions about how someone got a hold of the respondents' PI, we added wording that would encourage respondents to report what they might know, even if it was speculation (see Figure 4 for a comparison of the two question versions). We made minor changes to the wording, including the additional phrase, "even if you are not completely certain." Adding this conditional phrasing seemed to encourage respondents to report their speculations about the source of their identity theft. This change was successful: in fact, one respondent reported that she "had a hunch" that someone got her PI when they copied her driver's license at a used car dealership. The dealership had to have a copy of this respondent's license in order for her to be able to test-drive a car.

Before Revision:
Do you know anything about HOW your personal information was obtained?

After Revision:
Do you have any idea of HOW your personal information was obtained, even if you are not completely certain?

Figure 4: Before and After Versions of Question about How Someone Obtained the Personal Information

The wording of the questions was most problematic for the questions about the identity of the thief. Respondents were first asked if they knew anything about the thief. If they answered yes to this initial question, they received a follow-up question asking if this person was a stranger or someone the respondent knew in some capacity. The ultimate goal of these questions was to ascertain if the identity thief was someone the respondent knew or if the thief was a complete stranger. However, this intended meaning was not clear to respondents with the first question. Respondents did not consider knowing the name of the identity thief as "knowing" anything about that person. However, these respondents did know that the identity thief was not someone they had previously known, such as a friend, a relative, or a spouse. Because respondents were blind to the follow-up question, they were missing the important contextual information for indicating what "knowing anything" about the thief meant. They interpreted this question to mean finding out concrete information about the thief, rather than just reporting if the person was a complete stranger or someone with whom they had some sort of relationship.

To address the problems with the question about the identity thief, we added wording that would encourage respondents to report even seemingly trivial information about the identity thief or potential aliases (see Figure 5 for a comparison of the two question versions). We asked respondents if they knew anything "at all" about the people who had misused the PI. However, despite these changes we were unable to structure these questions in a way that consistently elicited the respondent's knowledge about the offender. For example, one respondent saw the person who stole her wallet, but indicated that she knew nothing about the identity thieves (giving a "no" response to the first question in this series). However, she did know that this person was a stranger. Because she did not have the context of the follow-up question, she indicated that she knew nothing about this person.

Before Revision:
Do you know, or have you learned, anything about the person(s) who misused your personal information?
Was the person who misused your personal information someone you knew or had seen before, or a stranger?

After Revision:
Do you know, or have you learned, anything at all about the person(s) who misused your personal information?
Was the person who misused your personal information someone you knew or had seen before, or a stranger?

Figure 5: Before and After versions of Questions about the Identity of the Identity Thief

Respondents' unwillingness to report speculative or vague information about whom they suspect misused their PI will have consequences for the survey data. The sponsors will not be able to collect accurate information on the relationship between identity thieves and their victims. Because identity theft can be a faceless and impersonal crime, and respondents are unwilling to report speculations, collecting accurate information about the relationship between the offender and the victim may not be possible.

4. Discussion

Developing a questionnaire to collect information on the identity theft experience was far more challenging than we had initially anticipated. The challenges came from the fact that identity theft is a complex crime made up of multiple experiences. It was difficult to create and structure questions that would elicit accurate reports and correct classifications of respondents' experiences. Not only did respondents have difficulty reporting all of the ways in which someone misused their PI, they also had trouble reporting information about how someone was able to misuse that information, and who ultimately misused it.

Throughout questionnaire development, there seemed to be one key underlying issue, inherent to the nature of identity theft, which contributed to respondents' difficulty in answering these questions. Because identity theft can be anonymous, victims often remain unaware of the misuse for long periods of time. They also never fully know if they have been successful at stopping the misuse of their PI. Once an identity thief has the respondent's Social Security Number, there is no guarantee that they will not continue to misuse it in the future. Identity theft seems to involve ongoing victimization, and as a result, many respondents were reluctant to answer many of the questions with certainty. For example, when asking about the different types of misuses, respondents would often say, "Not that I know of," "I'm not sure," "They're not using any accounts that I have currently," and "No, not that I can prove." Victims of identity theft never can be certain that there are not additional misuses of which they are unaware.

Complicating this issue of future victimization is respondent's lack of knowledge about the entirety of the identity theft experience. Often, respondents would report knowledge of some type of new account, or some type of purchase about which they would not have any detailed information. Respondents were not always able to find out more information from credit card companies, banks, hospitals, or cell phone companies about new accounts or specific charges, despite the fact that it was their own PI. This uncertainty factored into their responses to the questions and led to some inaccurate reports of misuses of PI. Through the iterative process described in this paper, we were able to learn and appreciate how to collect information on a complex experience with many moving parts. While we were able to make some successful revisions to the questionnaire, we also had to accept some shortcomings. For some aspects of identity theft, finding the right structure and wording to elicit complete and accurate information remained elusive. Due to the diverse nature of identity theft, it may not be possible to gather an accurate picture from all respondents.

References

Synovate. "Federal Trade Commission – 2006 Identity Theft Survey Report," Unpublished report, November, 2007.
U. S. Department of Justice. Bureau of Justice Statistics Bulletin: Identity Theft, 2004. April, 2006.