Report of Cognitive Research to Develop the 2008 NCVS Identity Theft Supplement

Prepared by Theresa DeMaio, Jennifer Beck, and Dawn Norris
U.S. Census Bureau
November 5, 2007

In December, 2007, the Bureau of Justice Statistics (BJS) came to the U.S. Census Bureau with a request to launch a new Identity Theft Supplement, which was co-sponsored by the Federal Trade Commission (FTC), the Office of Victims of Crime, the Bureau of Justice Assistance, and Office of Justice Programs. A draft questionnaire existed, and in a series of lengthy twice-weekly-meetings over several months, staff from the Demographic Surveys Division and the Center for Survey Methods Research in the Statistical Research Division met with the sponsors to make major changes to the questionnaire and finalize it for pretesting.

Staff from the Center for Survey Methods Research in the Statistical Division conducted cognitive interviewing with the revised questionnaire. This report documents the results of the pretesting.

METHODS

Participants

People who had been victims of identity theft or attempted identity theft were targeted for participation in the pretesting. One source of subjects was a list of people who had contacted the FTC's www.consumer.gov identity theft website. FTC made initial contacts with people in their database, who were then called by the Census Bureau's recruiter. While a few respondents were recruited this way, it was not a total success. Considering the nature of identity theft, it is easy to see why people might not be receptive to calls from strangers and asked to provide details about their victimization. Respondents were also recruited through ads on Craigslist.com, broadcast messages at BJS, and personal networks.

We conducted a total of 24 cognitive interviews between May and August, 2007. Twenty were with identity theft victims; four were with victims of attempted identity theft. Almost all were conducted in the Washington DC metropolitan area--at the Census Bureau's cognitive laboratory, BJS offices, respondents' offices, and local coffee shops. One interview was conducted by telephone with a respondent in St. Louis, MO. Respondents who were not federal employees were paid $40 for their assistance with the project. Staff from BJS and FTC observed some of the interviews.

A breakdown of the respondent characteristics is as follows:

AGE					
20s	30s	40s	50s	60s	70+
4	6	7	1	5	1

RACE		
White	Black	Asian
13	9	2

SEX	
Male	Female
6	18

EDUCATION LEVEL					
High School	Some College	College Degree	Some Graduate School	Advanced Degree	Unknown
1	6	7	2	7	1

Due to the nature of the recruiting, we did not have complete demographic information on all respondents. Age in particular reflects the interviewer's perception of the person they interviewed. Education level also does not reflect every respondent's self-reported education, but rather also reflects information the interviewer gleaned from the respondent during the course of the interview.

The distribution of some of the respondent demographic characteristics is skewed, especially the distribution of education. This group of respondents was definitely more highly educated than average. However, our main goal was not to get a "representative" group but rather to get respondents who had experienced either actual or attempted identity theft and therefore could answer our questions.

Questionnaire

The Identity Theft Supplement will be administered on an automated instrument (CATI/CAPI). However, these interviews were conducted using a paper version of the questionnaire.

We conducted eight rounds of pretesting. Iterations were not based on number of interviews but rather on our identification of problems and the seriousness of the problems. In some cases only two or three interviews were conducted in a round. The number of interviews per round is as follows:

	ROUND							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Number of Interviews	3	4	2	4	4	2	3	2

We used concurrent think-aloud interviews with concurrent and retrospective probing to test the questionnaire. Respondents were asked to think out loud as they reacted to the questions,

formulated their responses, and answered the questions. The initial questionnaire is included as Attachment 1. We enumerate the revisions to each question are enumerated in the discussion of the question-by-question results in the following sections. Attachment 2 contains the final recommendations after all 8 rounds of cognitive interviewing.

RESULTS

In this section we provide question-by-question results of the cognitive interviews. For each question, we include the question wording and findings for each version of the question that we tested.

SECTION A: SCREEN QUESTIONS

INTRO: Now, I would like to ask you questions about identity theft. Identity theft means someone else using your personal information without your permission to buy something, get cash or services, pay bills, or avoid the law.

Question 1:

We began this research with two versions of Question 1. The only difference between these two questions was the introductory sentence. The first version (A below) contained no mention of identity theft; the second version (B below) contained an explicit reference to identity theft and the presupposition that the following sub-items were instances of identity theft.

In addition to these differences, we tested four different versions of the question throughout the course of testing.

Rounds 1 through 3

1. (A) Since _____, 20__, has someone, without your permission:

OR

(B) Since _____, 20__, have you personally experienced identity theft, where someone, without your permission:

a. Used your existing bank account, including debit or ATM cards?	**YES**	**NO**
b. Used your existing credit card account?	**YES**	**NO**
c. Used another type of existing account such as your telephone, utilities, online payment account, like Paypal, insurance policies, or something else?	**YES**	**NO**
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?	**YES**	**NO**
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?	**YES**	**NO**
f. Used your personal information in some other way?	**YES**	**NO**

1a. Since _____, 20__, has someone, without your permission:

a. Attempted, but failed, to use your information in any of the ways just mentioned?	**YES**	**NO**

Summary of Results:

In Rounds 1 through 3, Q1a, which asked about attempted identity theft, followed Q1 in both versions A and B. of Question 1.

We administered this question to eight respondents: four respondents received Version A, and four received Version B. Since we did not observe any respondent reactions to the introductory sentence, and neither version seemed to be a problem, we combined all the interviews to present the results.

Four of the eight respondents said “yes” to “used your information in some other way.” Some were legitimate and others were either irrelevant or should have been recorded in a different category. One, reported above, reported one of the charges on her debit card. Another respondent mentioned that someone had “purchased something.” This response sounds like it should have been reported in part a. or b., and she had previously mentioned in passing that “something was on my credit,” but she said ‘no’ to part b. Two additional respondents provided details of attempted rather than actual misuses. Another respondent said “don’t know” and went on to mention several thefts of personal information but no specific knowledge of other information misuse.

Respondents clearly were attentive to the two-year reference period. Although we tried to recruit participants whose identity theft experiences had occurred within the reference period, this was not always possible. In some cases, the respondent answered “no” to all the question parts but mentioned experiences that happened prior to the cutoff date. For all but one of those cases respondents we changed the reference date to enable us to test the questions with the identity theft victims. There were cases in which respondents had been a victim within the reference period as well as at some time in the past. For the most part they were able to report on the occurrence within the reference period. It is worth noting, however, a couple respondents’ answers were “all over the map,” containing relevant and irrelevant information that was both in-scope and out-of-scope. This inconsistency included both accurate and inaccurate responses.

The separation of the questions about actual and attempted identity theft was problematic. Respondents did not know that a separate question about attempted identity theft was coming. They tended to misreport attempted misuses as actual misuses when hearing the question that they felt described their situation. This error was especially prevalent among respondents who had experienced both attempted and actual misuses of their information.

In some cases, respondents were not sure if accounts had actually been opened or if the perpetrators were caught in the process. One respondent referred to his notes, which he had brought with him to the interview, to decide that someone opened a cell phone account. He said the telephone provider sent him a letter saying that because the SSN provided did not match his date of birth, he would not be held responsible for the charges. This event was recorded as an actual information misuse.

Respondents also misreported the same misuse in multiple categories. One respondent, who had someone misuse her debit card to purchase magazines and to open an Internet service provider account, reported that her existing bank account was misused (in part a), that new accounts were opened (in part d.), and that her information was misused in some other way to purchase magazines (in part f). Perhaps because she correctly reported the opening of a new account to reflect one of these charges, she felt she should also find a category to report the second charge on her debit card. Another respondent reported that someone misused her existing bank account (in part a) at a mobile phone company. She didn’t know whether the charge reflected payment for a new mobile phone account, payment of bill, or the purchase of a new phone, but she nonetheless reported that someone opened a new account. It is not clear whether this is an error or not, since we do not know the details of what happened.

Respondents also had problems classifying their identity theft experiences. One respondent reported misuse of an existing account as the opening of a new account (although the larger issue was that her misuse was attempted rather than actual). Someone had tried to get into her online banking account but she had closed it so the bank sent her a notice. This respondent said “yes” to part d.

In terms of content, at least one respondent said “yes” to each subpart of the question. (This includes respondents whose events were attempts as well as actual thefts.) The most commonly reported misuse was opening new accounts and the least frequently reported misuse was misuses for other fraudulent purposes.

Because of the nature of identity theft, respondents were somewhat uncertain about their “no” responses. They often said things like, “no, not that I can prove,” “no, not that I know of,” or “I don’t know, they’re not using any of the accounts that I have currently.” Interviewers should be encouraged to probe “don’t know” answers to determine if a “don’t know” response is really “no.”

To deal with the main problem--respondents reporting attempted misuses in Q1.--we reorganized the question to allow reports of attempted misuses and reports of actual misuses. The question was revised to elicit both types of misuses at the same time (“used or attempted to use…”), and then ”yes” answers received a follow-up question to determine whether someone was successful at obtaining anything.

Round 4

1. (A) Since _____, 20__, has someone, without your permission:

OR

(B) Since _____, 20__, have you personally experienced identity theft, where someone, without your permission:

a. Used or attempted to use your existing bank account, including debit or ATM cards?	**YES**	**NO**
a.1. Were they successful in getting anything from your account?	**YES**	**NO**
b. Used or attempted to use your existing credit card account?	**YES**	**NO**
b.1. Were they successful in charging anything to your account?	**YES**	**NO**
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?	**YES**	**NO**
c.1. Were they successful in obtaining any goods or services from this account?	**YES**	**NO**
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?	**YES**	**NO**
d.1. Were they successful in actually opening any NEW accounts?	**YES**	**NO**
e. Used or attempted to use your personal information for some other fraudulent purposes 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?	**YES**	**NO**
e.1. Were they successful in using your identity for any of these purposes?	**YES**	**NO**
f. Used your personal information in some other way?	**YES**	**NO**

Summary of Results:

Four respondents were administered this version of the question. One respondent was administered Version A, and three respondents were administered Version B. Again, there were no problems or respondent reactions to the introductory sentence, and therefore, we present the results of all four interviews together.

The revised structure of the question performed well at addressing the attempted vs. actual misuse problem. The follow-up question was successful in distinguishing attempted from actual misuses. Only one respondent reported an unsuccessful attempt.

Respondents most frequently reported the misuse of "existing bank accounts." No one reported the misuse of "other existing accounts" or misuses for "other fraudulent purposes."

One respondent correctly understood that the term "bank accounts" included checking accounts (part a.), and answered "yes" because someone had misused her checking account. However, she expressed a preference to see the term "checking accounts" in the question, rather than just the term "debit." This explicit mention made sense, since many respondents had reported thefts of checkbooks or boxes of checks.

Several respondents reported that someone had misused their debit card as a credit card. The dual functions of these types of cards could lead respondents to misclassify this type of misuse. However, this dual function was generally not problematic. Respondents tended to report the situation as the misuse of debit cards. Only one respondent reported this type of misuse in both places.

One respondent answered "yes" to part f. Someone had created a new drivers license with her Social Security Number and used it to get access to her checking account.

We needed to make a choice (between Version A and Version B) as to which version to include in the final questionnaire. As noted, we did not notice great differences among respondents' reactions to the question while they were answering it. We probed them at the end of the interview for their definitions of identity theft. Some respondents gave generic definitions ("when someone steals your information and uses it illegally," "when somebody claims to be you to gain some type of advantage, to acquire something without the burden of having some liability to it," "someone takes your information for their benefit to pose as you.") Other respondents gave boundaries, and these boundaries were not always the same ("when somebody steals information and assumes an identity that is not theirs, even if it's for one minor transaction;" "someone able to, in any situation, just to walk in and be me (impersonating her with at photo ID and Social Security number); "when somebody actually uses your identity to buy a house or take out a loan." One respondent thought there were two types of identity theft: "Identity theft is when someone fraudulently uses your information like your name, it could be your name, Social Security number, medical card, or anything. That's one aspect of it. Another one is assuming your identity, just taking all that information and using it as if they are you…Like buy a car, buy a house, or get a job." Another respondent came to hold this same view by virtue of her experience. Before her victimization, her definition identity theft was "not when a credit card is stolen. It's when someone presents themselves as you to get a job, in front of law enforcement, etc. Now it includes "when someone represents themselves as you to make a purchase." These different interpretations of the concept

suggested that respondents were concentrating on the specific aspects of the questions rather than the overarching topic of identity theft.

Although this version worked well, the number of interviews was small and we thought we could improve reporting, especially of people misreporting existing and new accounts. We revised the question wording to emphasize them and to distinguish between them. We created two questions, as follows:

> *Since _____, 20__, has someone, without your permission, misused any of your EXISTING ACCOUNTS in any of the following ways?*
>
> *Next, I have some questions about any NEW ACCOUNTS someone might have opened. Since _____, 20__, has someone, without your permission...*

We also created a new question that served as a screener for the three types of existing accounts that are of interest to the sponsor (bank accounts, credit card accounts, or other accounts:

> *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?*

Within the existing accounts section, the questions about bank accounts and credit card accounts were reversed. This change was made to prevent further confusion and misclassifications of credit cards and debit cards. We wanted to give respondents a chance to report credit cards first, so that they would not report the use of debit cards in the wrong place. In addition, the term "existing savings or checking account" replaced the term "existing bank account."

Since respondents did not seem to prefer the Version B over Versions A, we decided to use Version A version for the rest of the testing. This change made it easier to implement the above revision of Q1.

Round 5

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? **YES NO**

b. Did someone use or attempt to use your credit card account? **YES NO**

c. Were they successful in charging anything to your account? **YES NO**

d. Did someone use or attempt to use your checking or savings account, including debit or ATM cards? **YES NO**

e. Were they successful in getting anything from your account? **YES NO**

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? **YES NO**

g. Were they successful in obtaining any goods or services from this account? **YES NO**

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? **YES NO**

i. Were they successful in actually opening any NEW accounts? **YES NO**

j. Used or attempted to use your personal information for some other fraudulent purposes 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? **YES NO**

k. Were they successful in using your identity for any of these purposes? **YES NO**

l. Used or attempted to use your personal information in some other way? **YES NO**

Summary of Results:

Four respondents were administered this version of the question. Respondents reported successful attempts to use credit cards, checking and savings accounts, new accounts and other fraudulent purposes. One respondent reported an unsuccessful attempt to open new accounts.

We observed no problems. Respondents reported that they understood the distinction between new and existing accounts.

One respondent reported that someone had misused her personal information "in some other way" (part l). She had previously reported that someone had used her existing credit card to buy gift cards from a department store. In part l. she said that these people continued to use the gift cards after she cancelled the credit card. This response seems to be a duplicate report. Although purchasing gift card extended the amount of time someone was able to capitalize on the identity theft, no additional monies were involved.

While we did not observe any respondent problems, we felt that the wording of parts b., d., and h. was awkward. The repetition of "did someone use or attempt to use" wording in each question sounded redundant--and very wordy. To make this series of questions sound more natural, we revised the wording of these questions as follows:

b. Was it a credit card account?

d. Was it your checking or savings account, including debit or ATM cards?

h. Was it another type of existing account such as your telephone, utilities, online payment account like Paypal, insurance policies or something else?

Rounds 6 through 8

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? YES NO

b. Was it a credit card account? YES NO

c. Were they successful in charging anything to your account? YES NO

d. Was it your checking or savings account, including debit or ATM cards? YES NO

e. Were they successful in getting anything from your account? YES NO

f. Was it another type of existing account, such as your telephone, utilities, online payment account like Paypal, insurance policies, or something else? YES NO

g. Were they successful in obtaining any goods or services from this account? YES NO

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? YES NO

i. Were they successful in actually opening any NEW accounts? YES NO

j. Used or attempted to use your personal information for some other fraudulent purposes 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? YES NO

k. Were they successful in using your identity for any of these purposes? YES NO

l. Used or attempted to use your personal information in some other way? YES NO

Summary of Results:

Seven respondents were administered this question version.

The question worked well, capturing a variety of incidents. Respondents reported actual and attempted misuses of credit cards, bank accounts, and the opening of new accounts. Two respondents reported that someone had used or attempted to use their information in some other way.

Respondents also were attentive to the reference period. One respondent correctly recognized that her experiences were outside the scope of the survey. She said someone used her name on a blogging website. She also reported that someone posted pictures of her on an adult website and abused her library privileges.

Another respondent said someone opened a new business credit card. This report may have been an error. Perhaps this should have been reported under "new accounts," but the respondent didn't know whether it was a business loan or a business spending account (a new credit card). If this type of experience should be classified as a new credit card account, perhaps some terminology should be added to the Interviewers Aid used to determine the appropriate place for reporting this type of misuse

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's Feedback:

Recommendation accepted.

Question 2:

We tested two different versions of this question.

Rounds 1 through 3

2. You said that one or more of your existing accounts, other than credit card or banking accounts, had been misused. Which of the following types of EXISTING accounts did the person run up charges, take money from, or otherwise misuse? Did they misuse your.....

(READ ANSWER CATEGORIES)

a. Medical insurance accounts?	**YES**	**NO**
b. Telephone accounts?	**YES**	**NO**
c. Utilities accounts?	**YES**	**NO**
d. Online payment account such as Paypal?	**YES**	**NO**
e. Investment accounts?	**YES**	**NO**
f. Some other type of existing account?	**YES**	**NO**

Summary of Results:

Two respondents were administered this version of the question. Both respondents reported the misuse of telephone accounts. In one case the respondent reported the wrong incident. She should have reported the misuse of a medical account. However, she had misreported it in Q1 as an existing account when it actually was an attempt to open a new account.

One change was made in the question so that the wording would be grammatically correct. The phrase "run up charges" was changed to "run up charges on."

Rounds 4 through 8

2. You said that one or more of your existing accounts, other than credit card or banking accounts, had been misused. Which of the following types of EXISTING accounts did the person run up charges <u>on</u>, take money from, or otherwise misuse? Did they misuse your.....

(READ ANSWER CATEGORIES)

a. Medical insurance accounts?	**YES**	**NO**
b. Telephone accounts?	**YES**	**NO**
c. Utilities accounts?	**YES**	**NO**
d. Online payment account such as Paypal?	**YES**	**NO**
e. Investment accounts?	**YES**	**NO**
f. Some other type of existing account?	**YES**	**NO**

Summary of Results:

No one was asked this question in Rounds 6-8 so it did not receive any further testing.

Final recommendations:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 3:

We tested one version of this question.

3. You said that someone used your personal information to open one or more NEW accounts. Which of the following types of NEW accounts did someone open? Did someone open...

(READ ANSWER CATEGORIES)

a. New telephone accounts?	**YES**	**NO**
b. New credit card accounts?	**YES**	**NO**
c. New checking or savings accounts?	**YES**	**NO**
d. New loans or mortgages?	**YES**	**NO**
e. New medical insurance policies?	**YES**	**NO**
f. New automobile insurance policies?	**YES**	**NO**
g. New online payment accounts, such as Paypal?	**YES**	**NO**
h. Some other type of new accounts?	**YES**	**NO**

Summary of Results:

Ten respondents were administered this question.

The only problem we observed with the question was that one respondent incorrectly answered "yes" to option g. She thought she heard the question as asking about "online service accounts" instead of "online payment accounts." This error may have been because someone set up an online service account in the respondent's name, and she this misuse was on her mind during the interview.

Other reporting errors reflected the problems that originated in early versions of Q1. Three people misreported attempted misuses, and one person incorrectly reported a credit card purchase as "some other type of new account." This respondent correctly reported one of the purchases on her credit card as a new account and incorrectly reported the other purchase as in the "other new account"

category. Perhaps she thought that both misuses of her credit card should be accounted for in this question.

One respondent answered "don't know" for "new checking or savings accounts" and "new online payment accounts." This respondent had a complicated identity theft experience. Several banking institutions contacted him about the opening of new accounts, but would not provide him any detailed information about the type of accounts or the dollar amounts involved.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 4:

We tested one version of this question.

4. How many new accounts were opened through the misuse of your information?

_____ *Number of new accounts opened*

Summary of Results:

Ten respondents were administered this question.

The responses ranged from 0 (by a respondent in the early rounds who reported an attempt in Q1.) to 12. This respondent said he had been contacted by 8 banks and he didn't know how many accounts were actually opened. When pressed to give an answer, his best guess was '8-12.' This uncertainty was the only problem we observed with this question.

Final recommendation:

No changes.

Question 5a:

We tested one version of this question. After Round 1, we added the bracketed text to reorient the respondent if he or she reported both existing account misuse and the opening of any new accounts.

5a. [You said that someone misused one or more of your existing accounts.] <Was the existing account/Were the existing accounts> that someone misused part of a joint account with your spouse or another individual?

1. Yes - ASK Q5b
2. No – GO TO probe before Check Item F

Summary of Results:

Fifteen respondents were administered this question. Only two of them reported that the misused accounts were joint accounts.

We observed no problems with this question.

Final recommendation:

No changes.

Question 5b:

We tested one version of this question.

5b. Including yourself, how many people are joint owners on this/these account(s)?

_____ *Total number of joint account holders (including the current respondent)*

Summary of Results:

Two respondents were administered this question. One account had 3 joint owners; the other had 2.

We observed no problems with this question.

Final recommendation:

No changes.

Question 5c:

We tested one version of this question.

5c. Are ALL the account holders of <this/these> joint account(s) currently members of your household?

1. Yes - ASK Q5d
2. No - ASK Q5d

Summary of Results:

Two respondents were administered this question. In both cases, all the account members were currently household members.

We observed no problems with this question.

Final recommendation:

No changes.

Question 5d:

We tested one version of this question.

5d. What are the names of the other members of this household who are joint owners of this account?

_____ *Name of first joint account holder*
_____ *Name of second joint account holder*
_____ *Name of third joint account holder*

Summary of Results:

Two respondents were administered this question.

One respondent, who had a joint account with her parents, regarded this as a sensitive question and asked "Do I have to give these?" She did not want to provide actual names, but was comfortable with using the titles 'Mom' and 'Dad.' The other respondent did not view the question as sensitive, but he provided the relationship ('wife') instead of his wife's name.

This question will not appear as worded in the Identity Theft Supplement. For pretesting purposes we asked for the names of the household members. But in the actual field administration, this supplement will be preceded by the NCVS questionnaire, which will collect a household roster, so the question will collect the line number or relationship of the household member to the respondent.

Final recommendation:

No changes.

Question 5e:

We tested one version of this question.

5e. Who was the primary person in your household who addressed the misuse of this account?

(DO NOT READ ANSWER CATEGORIES)

(SELECT A SINGLE RESPONSE)
- ___ *1. Respondent*
- ___ *2. Spouse*
- ___ *3. Parent*
- ___ *4. Son/Daughter (step-son, step-daughter, son-in-law, daughter-in-law)*
- ___ *5. Someone else (specify) _____*
- ___ *6. No household member (specify) _____*

Summary of Results:

Two respondents were administered this question. One respondent said the primary person in charge was a "parent;" the other said the primary person was himself ('respondent').

We observed no problems with this question.

Final recommendation:

No changes.

Question 6:

We tested one version of this question.

6. You said that someone used your personal information for some fraudulent purpose. As far as you know, did the person use your information in any of the following ways? Did they use your information ...

(READ ANSWER CATEGORIES)

a. To file a fraudulent tax return?	**YES NO**
b. To get medical treatment?	**YES NO**
c. To apply for a job?	**YES NO**
d. To provide false information to law enforcement when being charged with a crime or traffic violation?	**YES NO**
e. To rent an apartment or house?	**YES NO**
f. To apply for government benefits, such as social security, Medicare, disaster relief, food stamps, etc.?	**YES NO**
g. In some other way?	**YES NO** (specify) _____

Summary of Results:

One respondent was administered this question. She said that someone in California had gotten a medical card in her name, so they probably received medical treatment.

We observed no problems with this question.

Final recommendation:

No changes.

SECTION B: How/When identity theft discovered

INTRO: The next couple of questions I have are about how and when you discovered the misuse of your personal information.

Question 7a:

We tested two different versions of this question.

Rounds 1 & 2

7a. How did you FIRST find out someone had misused your personal information? When answering this question, please think only about when you found out about the actual misuse, not when you think your personal information was stolen.

(DO NOT READ CATEGORIES)

DISCOVERED BY RESPONDENT
___ *a. I noticed money missing from my account.*
___ *b. I noticed fraudulent charges on my account.*
___ *c. I received merchandise or a card that I did not order.*
___ *d. I had problems using my card or account because it was declined, closed, or had insufficient funds (bounced check)*
___ *e. I applied for credit, a bank account or loan, telephone service, employment, or government benefits, etc. and had problems.*
___ *f. I checked my credit report*
___ *g. I received a bill that I did not owe.*

NOTIFIED BY FINANCIAL INSTITUTION
___ *h. Credit card company or bank contacted me about suspicious activity on my account.*
___ *i. A credit monitoring service contacted me.*
___ *j. A collection agency, credit card company, or other company contacted me about late or unpaid bills*

NOTIFIED BY OTHER PARTY
___ *k. A law enforcement agency notified me.*
___ *l. A company/agency that had my personal information notified me.*

OTHER
___ *m. Discovered in another way - (specify)* _____

Summary of Results:

Seven respondents were administered the question. Responses fell into four different response categories. Respondents did not have any problems understanding the question.

Respondents most frequently reported, "had something else happen," suggesting that the response categories were inadequate. Two respondents had a company notify them and let them know about fraudulent charges. One respondent, a resident of the District of Columbia, received two letters from a California medical program provider about her enrollment in their medical program. Another local resident received a call from a telephone company telling him that an account had been set up in Ohio, and the SSN and the birthdates provided did not match, which raised suspicions. This response did not exactly fit with response category k. "A company/agency that had my personal information notified me." These companies did not necessarily have the respondents' personal information *before* someone set up the fraudulent accounts. Based on this evidence, response category k. was revised for the next round of testing. It was changed to read "*A company or agency notified me*."

The third case was one in which the respondent called the cell phone company to discontinue service after her son's death and learned about fraudulent charges. This situation did not fit into any of the 'Discovered by respondent' categories but is likely to be a fairly infrequent occurrence.

Rounds 3 through 8

7a. How did you FIRST find out someone had misused your personal information? When answering this question, please think only about when you found out about the actual misuse.

(DO NOT READ CATEGORIES)

DISCOVERED BY RESPONDENT
___ *a. I noticed money missing from my account.*
___ *b. I noticed fraudulent charges on my account.*
___ *c. I received merchandise or a card that I did not order.*
___ *d. I had problems using my card or account because it was declined, closed, or had insufficient funds (bounced check)*
___ *e. I applied for credit, a bank account or loan, telephone service, employment, or government benefits, etc. and had problems.*
___ *f. I checked my credit report*
___ *g. I received a bill that I did not owe.*

NOTIFIED BY FINANCIAL INSTITUTION
___ *h. Credit card company or bank contacted me about suspicious activity on my account.*
___ *i. My credit monitoring service contacted me.*
___ *j. A collection agency, credit card company, or other company contacted me about late or unpaid bills*

NOTIFIED BY OTHER PARTY
___ *k. A law enforcement agency notified me.*
___ *l. A company/agency notified me.*

OTHER
___ *m. Discovered in another way - (specify)*_____

Summary of Results:

In Rounds 3 through 8, this question was administered to 12 respondents. Again, respondents did not have any difficulty in understanding the question's intent. Although if they had been victimized more than once, they sometimes mentioned how they discovered each instance of victimization. Thus, respondents were not interpreting the word "FIRST" in the absolute chronological sense, but rather in terms of each incident. It is not surprising that respondents would do this, since these incidents are very salient. However, respondents often provided the correct information in their comments, and the interviewer was able probe the respondent and elicit the correct answer.

The responses ranged from "I noticed money missing from my account" to "credit card company or bank contacted me about suspicious activity on my account." No one gave a response that fit into the revised response category. (But note that in Q43 it had the desired effect of capturing the

response of a respondent in the "attempted" section who had received a rejection letter from one of the credit bureaus for a fashion retail store credit card.) However, there were still three responses that fell into the "other" category. Two responses were cases in which the respondent made the initial call to notify a credit card company that a card had been stolen, and someone had already used the card by the time the respondent made the call. Although this type of "notification" might fit into the "a bank or company notified me" category, that category is under the "notified by other party" subheading, while these respondents were notified by a financial institution. This seems like it could be a fairly common occurrence, and if the sponsor wants to differentiate between whether respondents are notified by financial institutions or other some other party, it should be included in the pre-coded categories.

In the third case, the respondent's bank sent him an email, indicating that his online banking password had been changed. Since he had not changed the password, he contacted the bank and learned that he had been a victim of identity theft.

Final recommendations:

We recommend that a new response category be added under the 'Notified by Financial Institution' heading. It would say "*I contacted credit card company or bank to report a theft and was told that fraudulent charges had already been made*."

We also recommend that interviewer training include instructions about probing to determine which incident of discovered misuse occurred first if respondents provide answers about each incident.

Sponsor's feedback:

Recommendation accepted.

Question 7b:

We tested two different versions of this question.

Rounds 1 through 6

7b. How long ago did you make this first discovery that someone had misused your personal information?

Enter specific date:
_____*Month (01-12)*
_____*Day (01-31)*
_____*Year (2006-2008)*

OR
_____*Number of months ago*

Summary of Results:

Sixteen respondents were administered this question in Rounds 1 through 6.

The majority of respondents reported in terms of dates (e.g., October 2006) while others reported in terms of elapsed time (e.g., 1 ½ years ago). Responses ranged from Summer 2003 to February 2007, with the majority of responses in 2005 or 2006.

The extent to which respondents were able to recall the information requested in this question varied. Some respondents remembered the exact date because the incident was such a salient event, while others used seasons or things they were doing at the time to reconstruct when they discovered this misuse. For some respondents, accurate recall was more problematic. One respondent said he discovered the misuse in either 2003 or 2004, but he couldn't remember which year it was. An 86-year-old respondent said it occurred 36 months ago, but a conversation with her daughter revealed that it occurred 24 months ago, which meant the respondent had reverse-telescoped her discovery out of the reference period.

A couple of respondents came to the interview prepared with notes they had kept while dealing with the police, credit agencies, and other companies. These respondents did not have any trouble providing answers to this question.

Some respondents mentioned that it would be easier to recall the dates if the interview took place closer to the time of the identity theft. However, it was not always the respondents whose experiences occurred outside of the reference period who made these comments. We did observe that respondents who had experienced identity theft less recently or who had very complex situations did have difficulty in specifying a particular date.

Rounds 7 and 8

7b. How long ago did you make this first discovery that someone had misused your personal information?

Enter specific date:
_____*Month (01-12)*
_____*Day (01-31)*
_____*Year (2006-2008)*

OR
_____*Number of months ago*

IF DK: **Was it a year ago or less?**
1. *Yes*
2. *No*—> **Was it more than 2 years ago?**
    1. *Yes*
    2. *No*

Summary of Results:

In an attempt to elicit dates specific enough to code into the two time periods of major interest to data analysts (that is, the past year and the past two years), the sponsor requested that "Don't know" answers be followed up with probes about these two specific time periods.

Two respondents were asked this question in Rounds 7 and 8, and both provided a month and year. Since neither respondent gave a "don't know" response, the follow-up questions were not asked.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 7c:

We tested two different versions of this question.

Rounds 1 through 6

7c. How long had your personal information been misused before you discovered it?

___ *1. One day or less*
___ *2. More than a day, but less than a week*
___ *3. At least a week, but less than one month*
___ *4. 1 to 2 months*
___ *5. 3 to 5 months*
___ *6. 6 to 11 months*
___ *7. 1 year to 2 years*

Summary of Results:

Seventeen respondents were administered this question in Rounds 1 through 6. The responses ranged from "one day or less" to "6 to 11 months." Two respondents could not provide answers, giving a "don't know" response.

Some respondents found it fairly easy to come up with a response to this question, since banks or credit card companies immediately notified the respondents after the suspicious event. Other respondents initially did not know the exact answer, but made educated guesses as to the length of misuse based on the billing cycle of their credit cards, the dates of bad checks, or the amount of time before companies send unpaid debts to collection agencies. However, two respondents were

not even able to estimate how long someone had been misusing their personal information before they made the discovery.

When respondents gave answers such as "6 days" or "10 days," it took time for the interviewers to do the necessary mental calculations required to figure out which response category she should mark. In an effort to alleviate this problem, the sponsor added parenthesized timeframes to provide quick notations about where responses should be marked.

Rounds 7 & 8

7c. How long had your personal information been misused before you discovered it?

___ *1. One day or less (1-24 hours)*
___ *2. More than a day, but less than a week (25 hours-6 days)*
___ *3. At least a week, but less than one month (7-30 days)*
___ *4. 1 to 2 months (31-89 days)*
___ *5. 3 to 5 months*
___ *6. 6 to 12 months*
___ *7. More than 1 year but less than two years*

Summary of Results:

Two respondents were administered this question in Rounds 7 and 8.

Their responses of "a little over 30 days" and "6 weeks" and could easily be converted to the appropriate response category. However, we worry about cases in which longer periods of time are involved. The response categories in this question are not strictly continuous. The parenthesized expression after "1 to 2 months" attempts to clarify that the entire time period up to the three month mark (i.e., up to 89 days) should be reported there. However, these expressions are not intuitively clear, since 2 months is 60 days, not 89 days. Furthermore, the parenthesized specification is not included in the last three response categories

Although we did not encounter this problem is our testing, it also was possible that the misuse could have been going on for years before the respondent discovered it, even if this is out of the reference period for the survey. These response categories were not amenable to reporting out–of-scope misuses.

Final recommendation:

We recommend rewording response categories 4, 5, and 6 to be strictly continuous as follows: "*one month to less than three months,*" "*three months to less than six months,*" "*six months to less than one year*." For the direction of the response categories to be consistent, the last one should read "*1 year to less than 2 years*." We also recommend that a category "*two years or more*" be added to ensure that all possibilities are covered.

Sponsor's feedback:

Changes in wording of response categories adopted. Addition of new response category not adopted.

Question 7d:

We tested two different versions of this question.

Rounds 1 through 6

7d. How long ago was the most recent time someone misused your personal information?

Enter specific date:
____ *month (01-12)*
____ *day (01-31)*
____ *year (2006-2008)*

OR
____ *months ago*

Summary of Results:

Sixteen respondents were administered this question.

As with Q7b., some respondents reported dates (e.g., August 2005), while others reported in terms of elapsed time (e.g., 18 months ago). Responses ranged from "Summer 2003" to "February 2007," with the majority of responses falling in 2005 or 2006. Respondents also tended to report that the most recent misuse was around the same time that they first discovered the misuse, indicating these events were one and the same. Six respondents gave different answers to these two questions. Some of these respondents had experienced protracted misuse of personal information originating from a single theft, while other respondents experienced independent misuses.

Rounds 7 and 8

7d. How long ago was the most recent time someone misused your personal information?

IF DK: **Was it a year ago or less?**
1. *Yes*
2. *No—>* **Was it more than 2 years ago?**
    1. *Yes*
    2. *No*

Enter specific date:
____ *month (01-12)*
____ *day (01-31)*
____ *year (2006-2008)*

OR
____ *months ago*

Summary of Results:

After Round 6, changes were made to make this question consistent with the changes to Q7b.

Two respondents were administered this question in Rounds 7 and 8. One respondent reported a month and year. The other respondent said he couldn't give a specific answer. He provided a range of months, all of which were within the past year. Because none of the respondents provided a "don't know" response, we were not able to test the new probes.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 7e:

We tested two different versions of this question.

Rounds 1 through 3

7e. You just indicated that your personal information was misused at least once during the past year. How was it misused during the past year, that is, since _____?

(READ ANSWER CATEGORIES)

a. Someone used your existing credit card accounts?	**YES**	**NO**
b. Someone used your existing banking or other existing account?	**YES**	**NO**
c. Someone used your personal information to open NEW accounts?	**YES**	**NO**
d. Someone used your personal information for some other fraudulent purpose?	**YES**	**NO**

Summary of Results:

Three respondents were asked this question. Respondents whose most recent misuse was more than one year ago were skipped out of the question. Only two of the respondents should have been administered the question. However, it was also administered to one respondent whose misuses all occurred within the past year, because there was no instruction to skip him out of this unnecessary question. In a later round this skip instruction was added.

Respondents did not have a problem understanding the question. One respondent said she had received a notice within the last year that her information had been compromised, but that it had not been misused. She correctly answered "no" to the question. (Note: This response suggests that the respondent received a breach notice, but she responded "no" to the breach notice question later in the questionnaire.)

Rounds 4 through 8

7e. You just indicated that your personal information was misused at least once during the past year. Which incident(s) occurred during the past year? Was it the <autofill with all yes responses from Q1, including actual and unsuccessful attempts>...

(READ ANSWER CATEGORIES)

a. Attempted misuse of your existing credit cards?	**YES**	**NO**
b. Misuse of your existing credit cards?	**YES**	**NO**
c. Attempted misuse of your existing accounts?	**YES**	**NO**
d. Misuse of one of your existing accounts?	**YES**	**NO**
e. Attempted opening of a NEW account?	**YES**	**NO**
f. The opening of a NEW account?	**YES**	**NO**
g. Attempted misuse of your personal information for some other fraudulent purpose?	**YES**	**NO**
h. The use of your personal information for some other fraudulent purpose?	**YES**	**NO**

Summary of Results:

Between Rounds 3 and 4 the sponsor decided to collect this information for both actual and unsuccessful (attempted) misuses.

An explicit fill of the type of incidents the respondents reported in Q1 was added to this question, and additional "attempted" categories were included. The reference to banking accounts was deleted from parts c. and d. to decrease the wordiness of the questions.

One respondent in Rounds 4 through 8 was correctly administered this question, although following the skip instructions on a paper instrument proved challenging for the interviewers, and in three they asked the question inadvertently.

The respondent who was correctly asked this question couldn't answer it. He was unable to give a definitive answer about whether the information was misused in the past year or whether he only discovered it in the past year.

Final recommendation:

Since a., b., c., and d. all refer to existing accounts, we recommend that "other" be added to categories c. and d. so these categories will be mutually exclusive. These categories would read: "*Attempted misuse of your other existing accounts*" and "*misuse of one of your other existing accounts*."

Sponsor's feedback:

Recommendation accepted.

Question 7f:

This question was asked of respondents who reported multiple types of identity theft in Q1 (that is, during the past two years), and was used to determine which misuses the respondent felt was the most serious. This most serious incident was intended to be the focus for a subset of the supplement questions.

We tested four different versions of this question.

Rounds 1 through 3

7f. Now I would like you to think about ALL the ways you have told me your personal information had been misused during the past TWO years, that is, since _____, 20__?

Which misuse of your personal information, that you have discovered in the past TWO years, do you consider to be the most serious?

a. Misuse of your existing credit cards?
b. Misuse of one of your existing accounts?
c. The opening of a NEW account?
d. The use of your personal information for some other fraudulent purpose?
e. Blind response: All misuses were serious.

Summary of Results:

Four respondents were asked this question in Rounds 1 through 3. Two said "new account" and the other two said "existing account." Three respondents reported only one incident in the screener, which was, by default, the most serious incident.

Respondents generally understood the question and were able to answer it. However, one respondent incorrectly categorized the incidents that happened to her and gave an incorrect answer. She had two incidents of fraudulent charges on her debit card, and her answer reflected which of these two charges she thought was more serious. However, the two incidents she should have been comparing were the misuse of her debit card and the opening a new account in her name.

The other three respondents were able to give reasons for their selection of the most serious misuses. Some respondents chose successful misuses, rather than unsuccessful ones. In one case, a respondent reported that someone accessing her bank account was more serious than someone opening new accounts. In contrast, another respondent reported that someone opening a new account was more serious than someone withdrawing funds from her debit card while she was overseas.

Rounds 4 and 5

7f. You said <autofill from responses to Q1, including actual and unsuccessful attempts> happened in the past TWO years, that is since _____, 20__? Which of these do you consider to be the most serious?

a. Attempted misuse of your existing credit cards?
b. Misuse of your existing credit cards?
c. Attempted misuse of your existing accounts?
d. Misuse of one of your existing accounts?
e. Attempted opening of a NEW account?
f. The opening of a NEW account?
g. Attempted misuse of your personal information for some other fraudulent purpose?
h. The use of your personal information for some other fraudulent purpose?
i. Blind response: All misuses were serious.

Summary of Results:

In Rounds 4 and 5, the question was revised to be consistent with Q7e., which explicitly asks about both successful and unsuccessful misuses. Note that in the previous rounds, respondents did consider unsuccessful attempts, though the questionnaire did not allow them to choose them as most serious, and they did not in any case choose to identify an unsuccessful attempt as most serious.

Four respondents were asked this question. Four other respondents were not asked this question because they only reported one incidence of identity theft.

Three respondents reported misuses associated with "existing accounts" as the most serious incident. These misuses all involved access to bank accounts, and the respondents deemed this more serious than either opening new store accounts or misusing existing credit cards. One respondent reported that the use of personal information for other fraudulent purposes was the most serious incident. This "other misuse" was the use of her personal information to obtain medical care fraudulently.

Round 6

7f. You said <autofill from responses to Q1, including actual and unsuccessful attempts> in the past TWO years, that is since _____, 20__? Were all these incidents the result of the same theft of your personal information or was your personal information stolen more than once?

1. Same theft - Go to Q8
2. Multiple thefts - Ask Q7g

7g. Which of these do you consider to be the most serious?

(DO NOT READ CATEGORIES)

a. Attempted misuse of your existing credit cards?
b. Misuse of your existing credit cards?
c. Attempted misuse of your existing accounts?
d. Misuse of one of your existing accounts?
e. Attempted opening of a NEW account?
f. The opening of a NEW account?
g. Attempted misuse of your personal information for some other fraudulent purpose?
h. The use of your personal information for some other fraudulent purpose?
i. Blind response: All misuses were serious.

Summary of Results:

In Round 6, the sponsor decided that it was important to distinguish between respondents who had a single theft of personal information and those who had multiple thefts. They only wanted to collect information about the misuse the respondent considered to be the most serious when they had experienced multiple thefts. This change was not based on problems with the question wording itself, but instead was due to our observation that respondents could not separate the effects of one misuse (e.g., bank account) from another (e.g., opening new accounts in the later questions (Sections C through G) that elicited information about the most serious misuse,). For this revised question, if the respondent thought that the multiple misuses of their personal information resulted from a single event (e.g., as a result of a stolen wallet), then they would answer the later questions about their entire identity theft experience, since that was how they thought about it. However, if the respondent felt that the multiple misuses resulted from multiple "thefts" of their personal information (e.g., losing their wallet and responding to a scam e-mail), then the respondent would choose which of the resulting multiple misuses they thought was the most serious.

The revision for Round 6 asked a preliminary question about whether the respondent had been a victim of a single theft or multiple thefts. A follow-up question, with the same response categories as Q7f in the previous round, was asked only for respondents who indicated that they experienced multiple thefts.

Two respondents were asked this question in Round 6. They did not have any problems understanding the intended meaning of the question. Unfortunately, both of them indicated that their personal information had only been stolen once, so we were unable to test the new Q7g. in this context. Therefore, we did not have evidence as to whether the Round 5 question wording would solve the problem of focusing respondents' attention on the most serious misuse of their personal information in subsequent sections of the interview. Ultimately, the sponsor decided to separate these two questions, let respondents use their own frame of reference for answering the later questions, and ask the "most serious" question at the end of the questions for victims of successful identity thefts.

Rounds 7 and 8 (New 7f & Question 41a)

7f. You said that someone <autofill from responses to Q1, including actual and unsuccessful attempts> in the past TWO years, that is since _____, 20__? Were all of these incidents the result of the same theft of your personal information or was your personal information stolen more than once?

1. *Same theft*
2. *Multiple thefts - Go to Q10*
3. *Don't know*

Summary of Results:

In Rounds 7 and 8, Q7f. was worded the same way as in Round 6. Two respondents were administered this question. Both respondents reported that the incidents were part of the same theft. They did not have a problem with this question.

41a. You said <autofill from responses to Q1, including actual and unsuccessful attempts> happened in the past TWO years, that is since _____, 20__? Which of these do you consider to be the most serious?

a. Attempted misuse of your existing credit cards?
b. Misuse of your existing credit cards?
c. Attempted misuse of your existing accounts?
d. Misuse of one of your existing accounts?
e. Attempted opening of a NEW account?
f. The opening of a NEW account?
g. Attempted misuse of your personal information for some other fraudulent purpose?
h. The use of your personal information for some other fraudulent purpose?
i. Blind response: All misuses were serious.

41b. Why was <autofill from 41a> the most serious type of identity theft you experienced?

_____
_____
_____
_____

Summary of Results:

In Rounds 7 and 8, the question about most serious attempts was moved to Q41a., following the financial impact questions. In addition to this change, an open-ended follow-up question was added, which asked the respondent why he/she chose the misuse he/she reported in Q41a.

Two respondents were administered this question. One respondent reported that all of the misuses were serious. The other one said that opening new accounts was more serious than misusing existing accounts.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 8:

We tested three different versions of this question.

Rounds 1 through 4

8. Do you know anything about HOW your personal information was obtained?

___1. Yes - Ask Q9
___2. No – Skip to Q10

Summary of Results:

Eleven respondents were administered this question in Rounds 1 through 4. Four respondents answered, "yes," and seven respondents answered "no." However, two of the seven respondents answering "no" had some information about the incident. One respondent had a strong suspicion that it was her bank, which had lost the forms of some of its account holders. Another respondent suspected someone got his information through Internet hacking. Since the sponsors were interested in even this basic level of information, we revised the question for the next round of testing in an attempt to elicit respondents' reports of speculative information as well as known facts. The wording was revised to read: *"Do you have any idea of how your personal information was obtained, even if you are not completely certain?"*

Rounds 5 through 7

Read answer to Q7g = b or d or f or h or j: **The next series of questions I have will be about <autofill from Q.7g>. Please consider only <autofill from Q.7g> when answering these questions.**

8. Do you have any idea of HOW your personal information was obtained, <u>even if you are not completely certain?</u>

___1. Yes - Ask Q9
___2. No – Skip to Q10

Summary of Results:

Besides the change noted above, an introduction was added to the question. The introduction was administered to respondents who had reported multiple types of misuse in Q1 and had selected a most serious incident in Q7f (in Round 5) or Q7g. (in Rounds 6 and 7). This introduction was designed to encourage respondents to focus on the most serious incident in this and subsequent questions.

Eight respondents were administered this version of the question. All said "yes," even a respondent who said she "had a hunch" how it happened. The respondent suspected that someone stole her personal information when she gave her driver's license to a car salesman so he could make a copy of it when she was test-driving a new car. Another respondent first said "no," then changed his answer to "yes" because he knew a debit card machine was involved (since he only uses the misused card in debit card machines), and he heard that there is a way for someone to extract information from debit cards when they are used in the debit card machines. The other respondents who answered "yes" were certain or fairly certain about how their information was obtained. These results suggest that the rewording of the question was effective.

Round 8

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

___1. Yes - Ask Q9
___2. No – Skip to Q10

Summary of Results:

The Round 8 version of this question is the same as Round 7, except that the introduction was deleted. It was no longer necessary when we moved the choice of the most serious incident to later in the questionnaire.

Since both respondents in Round 8 reported only attempted misuses, we did not get to test this question without the introductory sentence.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 9:

We tested two different versions of this question.

Rounds 1 through 4

9. How do you think your personal information was obtained? (For example, was it lost or stolen from your wallet, stolen from your postal mail or garbage, or obtained in some other way?)

(DO NOT READ CATEGORIES)

(SELECT A SINGLE RESPONSE)

___1. I lost it/It was stolen from my wallet or checkbook
___2. Someone stole it from my postal mail
___3. Someone stole it from my garbage
___4. Someone stole it during a purchase or other transaction
___5. Someone changed my address at the post office
___6. Someone hacked into my computer
___7. I responded to a scam email
___8. Stolen from personnel files where I work
___9. From an office/company that had my personal information in its files
___10. Obtained in some other way - (specify) _____

Summary of Results:

Four respondents were administered this question. Seven respondents were not asked this question because they said "no" to the preceding question (Q8).

One respondent said that her boss lost copies of her driver's license and Social Security card, along with those of all the new employees at her job. Her personal information was not "taken" from the personnel files, because the copies were not in a paper or electronic file. They were out on someone's desk. She also she no longer worked there at the time of the interview. This response appropriately fits in category 9 ("from an office/company that had my personal information in my files." However, to cover situations where former employees' information may have been lost or stolen from personnel files, we changed the wording of category 8 to "*stolen from personnel files.*"

Two of the four respondents said their information was obtained in some other way. In one case, the offender was a boarder in the respondent's home, and he had access to her computer. She said

he did not hack into her computer, which implies some type of programming to break in. He just sat down at her computer and was able to find her passwords. The other respondent had responded to a scam telephone call in which someone pretended to be from her credit card company, checking up on alleged fraud, and asking for her personal information. Neither of these situations quite fit into the existing categories.

Rounds 5 through 8

9. How do you think your personal information was obtained? (For example, was it lost or stolen from your wallet, stolen from your postal mail or garbage, or obtained in some other way?)

(DO NOT READ CATEGORIES)

(SELECT A SINGLE RESPONSE)

___*1. I lost it/It was stolen from my wallet or checkbook*
___*2. Someone stole it from my postal mail*
___*3. Someone stole it from my garbage*
___*4. Someone stole it during a purchase or other transaction*
___*5. Someone changed my address at the post office*
___*6. Someone hacked into my computer*
___*7. I responded to a scam email*
___*8. Stolen from personnel files*
___*9. From an office/company that had my personal information in its files*
___*10. Obtained in some other way - (specify)* _____

Summary of Results:

Eight respondents were administered this question. Most of them said their information was stolen from their wallets or checkbooks.

Three respondents said their information was "obtained in some other way." One respondent, noted above, said her information was compromised when she left a copy of her driver's license with a car salesman while she test drove a new car. Later, she said someone also might have been stolen the information from files at the credit union where she obtained a car loan. Another respondent said his debit card information was extracted from an ATM machine.

It is clear that there is a plethora of ways in which personal information can be obtained, and the short list of categories in this questionnaire cannot capture them all. Interviewers may not be able to make an "on the spot" determination of the category into which a response falls. One respondent said that AOL gave out his password, which allowed someone to access his banking accounts. This response was initially recorded as "some other way." It may be recoded into "from an office/company that had my personal information in its files," using a very loose definition of "files." The sponsor may want to err on the side of caution and have things recorded as "other" and recoded using some defined criteria.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

SECTION C: VICTIM RESPONSE

Question 10:

We tested three different versions of this question.

Rounds 1 through 4

10. Did you talk to anyone at the credit card company, bank, or other company about the misuse of <your personal information/fill in the blank>?

___*1. Yes*
___*2. No*

Summary of Results:

Fourteen people were administered this version of the question. Eleven of them answered "yes;" they had talked to someone at a credit card company, bank, or other company about the misuse of their information. Three respondents answered, "no." One respondent asked "Did I speak to someone personally?" and was unsure how to answer, since she had spoken to someone on the telephone, rather than speaking to someone in person. She ultimately answered "yes," but was not sure this was a correct answer. In fact, it is a correct answer since the sponsor is interested in any kind of contact with one of these organizations.

One respondent answered "no," even though she had reported previously that she found out about the misuse during a phone call with a cell phone company. She had initiated the call for another purpose (to cancel her recently deceased son's cell phone account) when the representative informed her about the misuse. She indicated that she was not focused on whether the question was asking if they told her about the fraud or she stumbled upon it herself.

One respondent, who was a minor at the time of the misuse and had a joint credit card account with her parents, responded "no" to the question, although her parent did call the credit card company. This response seems to be a correct response, since her parent, as a joint account holder, also would be asked these questions in the supplement and would report the contact.

As a result of the potential misinterpretation of this question, as well as similar misinterpretations with Q11 detailed below, this question was reworded to broaden its scope. The new wording was*: Did you contact anyone at the credit card company, bank, or other company about the misuse of your <personal information/fill in the blank>?"*

Round 6

10. Did you <u>contact</u> anyone at the credit card company, bank, or other company about the misuse of <your personal information/fill in the blank>?

___*1. Yes*
___*2. No*

Summary of Results:

Only two respondents were administered this version of the question. Both respondents answered "yes" to the question. Neither one had an obvious problem with it.

Rounds 7 and 8

10. [For any of these incidents] Did you <u>contact</u> anyone at the credit card company, bank, or other company about the misuse of <your personal information/fill in the blank>?

___*1. Yes*
___*2. No*

Summary of Results:

Because of the changes introduced in Q7f in Round 6, an introductory phrase was added to this question, which served as a reminder for respondents to consider all identity theft episodes when answering this question. If in Q7f the respondent reported that his/her personal information was stolen more than once, the interviewer would read the bracketed text.

Two respondents were administered this version of the question. Both of them said "yes." We observed no obvious problems with this question.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 11:

We tested two different versions of this question.

Rounds 1 through 5

11. Did you talk to anyone at a credit bureau about the misuse of <your personal information/fill in the blank>?

___1. Yes
___2. No - Skip to Q15

Summary of Results:

Fourteen respondents answered this question in Rounds 1 through 5. Five respondents answered "yes," and nine respondents answered "no." However, two of these nine respondents gave incorrect responses, according to the sponsors' desired interpretation of this question, which included any kind of contact. One respondent said she went online and wrote a comment to add to her credit report. Another respondent said she called the credit bureau and her information was taken through an automated system. She interpreted "talk" to mean actually interacting with a phone representative.

As a result of these misinterpretations (and the misinterpretation reported for the previous question), the wording of this question was revised to read*: "Did you contact a credit bureau about the misuse of <your personal information/fill in the blank>?"*

It was clear at this point that respondents were not focusing their attention on the most serious misuse, which they were instructed to do in Q7f. When answering this question, one respondent talked about an incident that was not the one she had previously identified as the most serious. She mentioned misuses other than the most serious when answering other questions in this section too. This type of error contributed to the decision to move the "most serious" question from Q7g to Q41a, as reported previously.

Rounds 6 through 8

11. Did you <u>contact</u> a credit bureau about the misuse of <your personal information/fill in the blank>?

___1. Yes
___2. No - Skip to Q15

Summary of Results:

Four respondents were administered this version of the question. We observed no ambiguity with the intent of the question. Three respondents answered "yes" and one respondent answered "no."

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback.

Recommendation accepted.

Question 12:

We tested four different versions of this question.

Rounds 1 through 3

12. You just indicated that you contacted a credit bureau about the misuse of <your personal information/fill in the blank>. I am going to read a list of things that people sometimes do when they contact someone at a credit bureau after their <personal information/fill in the blank> is misused. Did you....

(READ ANSWER CATEGORIES)

a. Request your credit report?	**YES**	**NO**
b. Request corrections to your credit report?	**YES**	**NO**
c. Place an initial, or "90-day" fraud alert on your credit report?	**YES**	**NO**
d. Place a permanent, or "seven year" fraud alert on your credit report?	**YES**	**NO**
e. Send a police report to the credit bureau?	**YES**	**NO**
f. Place a freeze on your credit report, which prevents the credit bureaus from sending your credit report to anyone without your permission?	**YES**	**NO**
g. Do something else?	**YES**	**NO**

Summary of Results:

Two respondents were asked this version of the question in Rounds 1-3.

Both respondents placed a fraud alert on their credit report and did not seem to have a problem deciding if it was a 90-day (part c) or a seven-year (part d) fraud alert. Overall, they did not have a problem with the question.

One respondent answered in part e. that he had not sent a police report to the credit bureau because they told him to go to the FTC. He must have had this on his mind, because at part g., he reported that he contacted the FTC. This response is not in-scope for this question.

One respondent reported sending the police report number, but not the report itself, to the credit bureau. She was not sure how to answer the question.

Round 4

12. You just indicated that you contacted a credit bureau about the misuse of <your personal information/fill in the blank>. I am going to read a list of things that people sometimes do when they contact someone at a credit bureau after their <personal information/fill in the blank> is misused. Did you....

(READ ANSWER CATEGORIES)

a. Request your credit report?	**YES**	**NO**
b. Request corrections to your credit report?	**YES**	**NO**
c. Place an initial, or "90-day" fraud alert on your credit report?	**YES**	**NO**
d. Place a permanent, or "seven year" fraud alert on your credit report?	**YES**	**NO**
e. Send a police report <u>or incident number</u> to the credit bureau?	**YES**	**NO**
f. Place a freeze on your credit report, which prevents the credit bureaus from sending your credit report to anyone without your permission?	**YES**	**NO**
g. Do something else?	**YES**	**NO**

Summary of Results:

In Round 4, part e. of the question was changed to include reference to a report number. At the sponsor's request, we added the phrase "or incident number" after "police report." We then probed respondents about the term they used to describe a police report.

Only one respondent was administered this question in Round 4 (the others had not contacted a credit bureau). This respondent was not familiar with the term "incident number." She also committed a response error. She, like the one in Round 3, reported (in part g.) that she had contacted the FTC. This error may have occurred because, with the long list of items included in the question, she forgot that the stem of the question asked about actions she took when she contacted a credit bureau.

As a result of the two respondents who erroneously reported actions that did not involve a credit bureau, we revised the question to emphasize that all the actions referred to contact with a credit bureau. After Q12d., we repeated the stem of the question*: "When you contacted the credit bureau, did you … ."*

Round 5

12. You just indicated that you contacted a credit bureau about the misuse of <your personal information/fill in the blank>. I am going to read a list of things that people sometimes do when they contact someone at a credit bureau after their <personal information/fill in the blank> is misused. When you contacted the credit bureau, did you....

(READ ANSWER CATEGORIES)

a. Request your credit report?	**YES**	**NO**
b. Request corrections to your credit report?	**YES**	**NO**
c. Place an initial, or "90-day" fraud alert on your credit report?	**YES**	**NO**
d. Place a permanent, or "seven year" fraud alert on your credit report?	**YES**	**NO**

When you contacted the credit bureau, did you....

e. Send a police report <u>or incident number</u> to the credit bureau?	**YES**	**NO**
f. Place a freeze on your credit report, which prevents the credit bureaus from sending your credit report to anyone without your permission?	**YES**	**NO**
g. Do something else?	**YES**	**NO**

Summary of Results:

Only one respondent was administered this question in Round 5. As previously mentioned, most respondents in this round did not report contacting a credit bureau. Repeating the question stem in the middle of the question seemed to work for this respondent. We did not see the same memory issues as we did in the previous round. This respondent said "no" to all parts of the question.

However, this respondent was unable to answer either part c. or d. because, although she knew she had placed some type of freeze on her credit report, she did not know if it was a permanent (7-year) or temporary (90-day) freeze. This inability to answer the question suggests that respondents may not be familiar with the different types of credit report freezes.

When probed about the terminology in part e., she said she was not familiar with the term "incident report" -- "unless it means a police report." Clearly she was more familiar with the term "police report."

To increase reports of putting freezes on credit reports from respondents who don't know what type of freeze they initiated, we revised the question to read: "*Place a fraud alert on your credit report.*" Then a follow-up question was added: "Was *it a seven year fraud alert?"* This wording was suggested by the sponsor.

Rounds 6 through 8

12. When you contacted the credit bureau, did you....

(READ ANSWER CATEGORIES)

a. Request your credit report?	**YES**	**NO**	
b. Request corrections to your credit report?	**YES**	**NO**	
c. Place a fraud alert on your credit report?	**YES** - ask c.1		**NO**
IF D = YES: **c.1 Was it a seven year fraud alert?**		**YES**	**NO**

When you contacted the credit bureau, did you....

e. Send a police report <u>or incident number</u> to the credit bureau?	**YES**	**NO**
f. Place a freeze on your credit report, which prevents the credit bureaus from sending your credit report to anyone without your permission?	**YES**	**NO**
g. Do something else?	**YES**	**NO**

Summary of Results:

Three respondents were administered this question in Rounds 6-8.

Respondents in this round were able to report the type of fraud alert they placed on their credit report. One respondent placed a seven-year alert while two placed a 90-day alert.

One respondent said "yes" to part g –"doing something else". This was a legitimate response. He had contacted the credit bureau to ask a specific question. Two of the respondents reported later (Q24) that they had contacted the FTC. Neither one reported it here, suggesting that the reiteration of the question stem was successful at keeping the respondent's focus on actions they took with a credit bureau.

One of the respondents who reported that she requested a copy of her credit report may have made an error. She received a copy of her report because of a previous breach of her personal information. However she did not specifically request her report in response to her identity theft experiences. It is not clear if this response was correct or not.

Two of the respondents, when probed, said they were familiar with the term "incident report." Both worked in the criminal justice field and were familiar with the term. Both respondents thought that "police report" is a more common term and would be more familiar to the general population. Another respondent also suggested the term "complaint."

Final recommendation:

We recommend deleting the term "incident report" from part e. The question would read: "*Send a police report or police report number to the credit bureau*."

Sponsor's feedback:

Recommendation accepted.

Question 13:

We only tested one version of this question.

13. After you told a credit bureau that <your personal information had been misused/fill in the blank>, how satisfied were you with the credit bureau's response? Were you very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?

(DO NOT READ ANSWER CATEGORIES)

(IF THE RESPONDENT STATES THAT THEY CONTACTED MULTIPLE CREDIT BUREAUS, INSTRUCT THE RESPONDENT TO THINK ABOUT THEIR TOTAL EXPERIENCE WITH THE CREDIT BUREAUS)

___1.Very Satisfied – Skip to Q15
___2. Somewhat Satisfied – Skip to Q15
___3. Somewhat Dissatisfied - Ask Q14
___4. Very Dissatisfied - Ask Q14
___5. Neither satisfied nor dissatisfied - Skip to Q15

Summary of Results:

Seven respondents were administered this question. The responses ranged from "very satisfied" to "very dissatisfied." Respondents did not seem to have any problem with this question. One respondent had recall issues. She said she couldn't remember how she felt about the credit bureau's response. This response was coded as "Neither satisfied nor dissatisfied." However, this response possibly should have been captured as "don't know."

Final recommendation:

No changes.

Question 14:

We only tested one version of this question.

14. Why were you dissatisfied with the credit bureau's response?

(DO NOT READ ANSWER CATEGORIES)

(MARK ALL THAT APPLY)

___1. My credit report was not corrected
___2. It was hard to communicate with the credit bureau
___3. I could not place a fraud alert
___4. I could not obtain a credit report
___5. I could not place a freeze
___6. The credit reporting bureaus would not accept my police report
___7. Some other reason - (specify) _____

Summary of Results:

One respondent was administered this question, which was a follow-up for respondents who indicated they were dissatisfied with the credit bureau's response.. This respondent reported that her "credit report was not corrected." "They said they would red flag any account with my name on it, but it didn't happen."

Final recommendation:

No changes.

Question 15:

We tested one version of this question.

15. Did you contact any law enforcement agencies, such as the police or sheriff, to report the misuse of <your personal information/fill in the blank>?

___1. Yes - Ask Q16
___2. No - Skip to Q23

Summary of Results:

Seventeen people were asked this question. For one respondent, the question was inadvertently omitted. Twelve respondents reported that they contacted law enforcement agencies, and five of them said they did not.

Respondents were not limiting their report to the most serious misuse. One respondent mentioned both of the incidents of identity theft she experienced, rather than just the most serious. This error is additional evidence that respondents were not using the correct frame of reference when answering this question series.

Final recommendation:

No changes.

Question 16:

We tested two different versions of this question.

Rounds 1 through 4

16. Was it your local law enforcement or another law enforcement agency?

___*1. Local law enforcement*
___*2. Another law enforcement agency*

Summary of Results:

Four respondents were administered this question in Rounds 1 through 3. Three of them said they contacted their local law enforcement agency. One respondent said she contacted both a local and another law enforcement agency. However, this was not a correct response. The other agency she contacted was www.consumer.gov, which is the FTC hotline. She was not able to differentiate between government agencies and law enforcement agencies.

To eliminate respondents' confounding reports of contacting the FTC or other government agencies when answering this question, we added another response category, "*other government agency*," for the next round of testing.

Rounds 5 through 6

16. Was it your local law enforcement or another law enforcement agency?

___*1. Local law enforcement*
___*2. Another law enforcement agency*
___*3. Other government agency*

Summary of Results:

Eight respondents were asked this question in Rounds 5 through 8. For one respondent it was inadvertently omitted.

Five respondents in these rounds said they reported their identity theft to their local law enforcement agency. Three other respondents said they reported it to both a local enforcement agency and another law enforcement agency. The "other" law enforcement agencies reported included:

- the security office at Nordstroms, which deals with theft and credit card fraud.
- the police in the jurisdiction where the credit card fraud occurred (outside her home jurisdiction). Finally The third respondent said she responded
- a federal authority. Further probing revealed that this respondent was referring to the FTC. This misreport suggests two things: (1) respondents may have legitimately contacted authorities in more than one geographic location; and (2) it may not be possible to disentangle reports of the FTC from the "other law enforcement agency" category, since respondents do not seem to realize the difference. At least one respondent thought that the consumer.gov hotline was run by the Secret Service. This confusion is something that the sponsor will need to keep in mind when analyzing the data.

No one reported "other government agency."

Final recommendation:

We recommend that a series of follow-up questions (Q17-22) be added for the respondent to report about their experiences with both types of law enforcement agencies.

Sponsor's feedback:

Recommendation accepted.

Question 17:

We tested one version of this question.

17. Did <the local law enforcement agency/that other law enforcement agency> take a police report from you about the misuse of <your personal information/fill in the blank>?

___1. Yes - Ask Q18
___2. No - SKIP to Q19

Summary of Results:

Twelve respondents were asked this question. The question was inadvertently omitted for one respondent.

Nine respondents said the law enforcement agency took a police report. Three respondents reported that the agency did not take a police report. When answering this question, one of the respondents, who had already reported the misuse of her personal information to local law enforcement and a federal agency (i.e., FTC), reported that she contacted an additional "other law enforcement agency." She also reported the misuse in the jurisdiction where the credit card fraud occurred.

No one had problems understanding the question. The only issue we observed was that there was no procedure for asking and recording information about the additional law enforcement agencies that the respondent contacted.

Final recommendation:

We recommend that a series of follow-up questions (Q17-22) be added for the respondent to report about their experiences with more than one law enforcement agency.

Sponsor's feedback:

Recommendation accepted.

Question 18:

We tested one version of this question.

18. Did you get a copy of the police report?

___*1. Yes*
___*2. No*

Summary of Results:

This question was administered to nine respondents. Seven respondents got a copy of their police report, and two respondents did not get a copy. We did not observe any problems with understanding or answering this question.

Final recommendation:

No changes.

Question 19:

We tested one version of this question.

19. How satisfied were you with the law enforcement agency's response when you reported the misuse of <your personal information/fill in the blank>? Were you very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?

(DO NOT READ ANSWER CATEGORIES)

(ENTER A SINGLE RESPONSE)
___*1. Very Satisfied – Skip to Q21*
___*2. Somewhat Satisfied – Skip to Q21*
___*3. Somewhat Dissatisfied - Ask Q20*
___*4. Very Dissatisfied - Ask Q20*
___*5. Neither satisfied nor dissatisfied - Skip to Q22*

Summary of Results:

Twelve respondents were administered this question. Everyone seemed to be able to provide an answer. The responses ranged from "very satisfied" to "very dissatisfied." One respondent reported, "neither satisfied nor dissatisfied," after she saw it as a response option on the interviewer's questionnaire

Final recommendation:

No changes.

Question 20:

We tested one version of this question.

20. Why were you dissatisfied with the law enforcement agency's response?

(DO NOT READ ANSWER CATEGORIES)

(MARK ALL THAT APPLY)
- ___*1. Police didn't or couldn't do anything*
- ___*2. Police only filled out a report*
- ___*3. Police didn't see it as a crime*
- ___*4. Police said the crime did not fall in their jurisdiction*
- ___*5. Police gave me no information on what I should do about the crime*
- ___*6. Police never got back in contact with me/never learned outcome*
- ___*7. Didn't feel my concerns/complaints were taken seriously*
- ___*8. Police unable to catch the offender*
- ___*9. Other (Specify)* _____

All responses 1-9 - Skip to Q22

Summary of Results:

Seven respondents were administered this question. We recorded eight responses across these respondents, since multiple responses were allowed. Two respondents reported in each of the following categories: police didn't or couldn't do anything; police said the crime did not fall in their jurisdiction; didn't feel my concerns/complaints were taken seriously; and other.

Two respondents also indicated that they were dissatisfied for "other" reasons. One said the police "did not have time to deal with" her report of identity theft and they seemed to indicate that "it wasn't a big deal." This response likely should have been recoded into the "didn't feel my concerns/complaints were taken seriously" category. However, the respondent did not think 'didn't feel my concerns/complaints were taken seriously' adequately captured her feelings.

No other issues were encountered with this question.

Final recommendation:

No changes.

Question 21:

We tested one version of this question.

21. Why were you satisfied with the law enforcement agency response?

(DO NOT READ ANSWER CATEGORIES)

___1. Police took a report
___2. Police gave me information on what to do - Skip to Q24
___3. Police did everything that they could
___4. Police took the crime seriously
___5. Police caught the offender
___6. Police kept me informed
___7. Other (specify) _____

Summary of Results:

Three respondents were administered this question. One of them said the, "police took a report," and, "they knew what to do (category 1)." Another respondent said the "police took a report" and "they told me what I should do and who I should call." It is not clear whether this response should be coded in category 1 or 2. Multiple responses are not explicitly allowed, and the skip instructions differ depending which category is chosen. The third respondent was very vague when assessing her level of satisfaction. She said she could not remember any negative interactions ("shouting at them or getting mad or anything"). This type of reaction seems to be an "other" response.

Final recommendation:

We recommend that multiple responses be allowed here and that the skip instruction after category 2 be deleted. In combination with the revised wording of Q22. below, this change will have the same effect as the original intent of this question, but without the current potential for confusion.

Sponsor's feedback:

Recommendation accepted.

Question 22:

We tested two different versions of this question.

Rounds 1 through 5

22. Did the law enforcement agency provide you with any additional information, such as a pamphlet or prevention material, on what to do when you've experienced identity theft?

___1. Yes - Ask Q24
___2. No - Skip to Q24

Summary of Results:

Seven respondents were administered this question in Rounds 1 through 5. Five of them said "no" to the question and two said "yes." The respondent who reported in Q21. that "police took a report" and "they told me what I should do and who I should call" was asked this question. Because she had previously indicated that the police provided her with "next-steps" information, she was understandably confused about how to answer this question. As a result of this confusion, the question was revised for the next round to read: *"Did the law enforcement agency provide you with any additional printed information, such as a pamphlet or prevention material, on what to do when you've experienced identity theft?"*

Rounds 6 through 8

22. Did the law enforcement agency provide you with any additional printed information, such as a pamphlet or prevention material, on what to do when you've experienced identity theft?

___1. Yes - Ask Q24
___2. No - Skip to Q24

Summary of Results:

Four respondents were administered this question in Rounds 6 through 8. Two respondents said "yes" and two said "no."

The revision to this question seems to be successful at alleviating the ambiguity and awkwardness observed in Q21. above. With this question change, there is no need to keep the skip instruction in Q21., and multiple responses could be recorded.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 23:

We tested one version of this question.

23. I'd like to learn more about why people who experience identity theft do not report it to law enforcement. Why did you decide not to contact a law enforcement agency?

(DO NOT READ ANSWER CATEGORIES)

(MARK ALL THAT APPLY)

DIDN'T KNOW I COULD
a. Didn't know that I could report it
b. Didn't know what agency was responsible for identity theft crimes

NO LOSS
c. I didn't lose any money

HANDLED IT ANOTHER WAY
d. Reported it to someone else such as credit card company/bank or other organization
e. Took care of it myself

DIDN'T THINK THE POLICE COULD HELP
f. Didn't think police would do anything
g. Didn't want to bother police/not important enough
h. Didn't find out abut the crime until long after it happened/too late for police to help
i. Couldn't identify the offender or provide much information that would be helpful to the police

PERSONAL REASONS
j. I was afraid to report it
k. The person responsible was a friend or family member and I didn't want to get them in trouble
l. I was embarrassed
m. Too inconvenient/didn't want to take the time

OTHER
n. Other (specify) _____

Summary of Results:

This question was administered to five respondents. There were six responses, since it was a Mark-All-That-Apply question. Three responses fit into the pre-coded categories, and three responses did not fit.

One of the "other" responses was part of a multiple response. The respondent had reported her stolen credit card to the credit card company and "had made enough phone calls dealing with the credit card companies." She also did not want to bother calling the police to report her identity theft. Another respondent didn't call the police because his card was not physically stolen {his number was taken from the ATM machine). The respondent, who did not have a very good grasp of the interview experience, explained a situation that had occurred prior to her in-scope experiences and was related to theft of documents rather than the misuse of her personal information. She did not want to make any accusations because she was not sure if people working in her house had taken the documents.

Final recommendation:

No changes.

Question 24:

We tested four different version of this question.

Round 1

24. Next, I'm going to read you a list of other people and organizations that someone might contact when their personal information is misused. Which of the following people or organizations, if any, did you contact? Did you contact.....

(READ ANSWER CATEGORIES)

a. A lawyer or other legal professional?	**YES**	**NO**
b. A State or local government consumer affairs agency, such as the State Attorney General's office?	**YES**	**NO**
c. A consumer agency, such as the Better Business Bureau or the National Consumer League?	**YES**	**NO**
d. The government agency that issued the lost or stolen identification such as your driver's license?	**YES**	**NO**
e. Your credit monitoring service or identity theft insurance company?	**YES**	**NO**
f. The Federal Trade Commission?	**YES**	**NO**
g. Some other group or organization?	**YES (specify)** _____	**NO**

Summary of Results:

We asked one respondent this question in Round 1. This respondent had a broader definition of legal professional than was intended. It included anyone in the legal system, including police, judges, and state legal professionals who handle identity thefts. Since this definition would result in an overreport of contacts with legal professionals, we decided to revise the question to delete "other legal professionals."

Rounds 2 & 3

24. Next, I'm going to read you a list of other people and organizations that someone might contact when their personal information is misused. Which of the following people or organizations, if any, did you contact? Did you contact.....

(READ ANSWER CATEGORIES)

a. <u>A lawyer?</u>	**YES**	**NO**
b. A State or local government consumer affairs agency, such as the State Attorney General's office?	**YES**	**NO**
c. A consumer agency, such as the Better Business Bureau or the National Consumer League?	**YES**	**NO**
d. The government agency that issued the lost or stolen identification such as your driver's license?	**YES**	**NO**
e. Your credit monitoring service or identity theft insurance company?	**YES**	**NO**
f. The Federal Trade Commission?	**YES**	**NO**
g. Some other group or organization?	**YES (specify)** _____	**NO**

Summary of Results:

Six respondents were administered the Round 2 version of this question. We observed several issues with this version.

Two respondents were unsure how to answer part a. because they had received unpaid legal help from people they knew. One person responded, "yes," to the question, since she assumed that this level of assistance was relevant. The other respondent could not provide an answer. She said she had a conversation about her incident with a person who happens to be a lawyer, but that she did not make an appointment and did not pay a fee.

The wording of part d. was awkward, since it assumes that the respondent has lost some type of identification. For many of our respondents this was not the case, and they did not know how to answer. The question was left blank for one respondent.

In two of these six interviews, respondents were unsure about what was included in part b. Specifically, they wondered if this option included the FTC or www.consumer.gov. One of these respondents said "no" to b. and "yes" to f. The other respondent said "no" to both questions. She knew that she had contacted consumer.gov, but she did not know that it is part of the FTC website.

One respondent answered "yes" to "g. -- Some other group or organization." She reported that she had notified the Post Office, since someone had stolen a replacement credit card from her mail. This person had been using a credit card that she did not even know existed because she had never received it.

To address these issues, we made several changes in the question for Round 3.

- We changed the wording of part a. from "contact a lawyer" to "hire a lawyer." This change necessitated taking the word "contact" out of the question stem and adding it as the first word in parts b.-g.
- We revised the wording of part d. to make it relevant for all respondents. The wording was revised to read*: "Contact an organization or company that issues documents like drivers' licenses, social security cards, or insurance cards?"*
- We re-ordered the sequence of questions to move part f. up to follow part c. This change made the connection between these two questions more explicit.

Rounds 4 & 5

24. Next, I'm going to read you a list of other people and organizations that someone might contact when their personal information is misused. Which of the following people or organizations, if any, did you contact? Did you…

(READ ANSWER CATEGORIES)

a. Hire a lawyer?	**YES**	**NO**
b. Contact a State or local government consumer affairs agency, such as the State Attorney General's office?	**YES**	**NO**
c. Contact the Federal Trade Commission?	**YES**	**NO**
d. Contact a consumer agency, such as the Better Business Bureau or the National Consumer League?	**YES**	**NO**
e. Contact an organization or company that issues documents like driver's licenses, social security cards, or insurance cards?	**YES**	**NO**
f. Contact your credit monitoring service or identity theft insurance company?	**YES**	**NO**
g. Contact some other group or organization?	**YES (specify)** _____	**NO**

Summary of Results:

Eight respondents were administered this version of the question.

The revised wording of part e. did not cause a problem. Several respondents in this round responded ”yes” to this question and no one left it blank. We also did not observe any confusion.

The revised version of part a. worked well. One respondent correctly reported “yes” because she enrolled in Prepaid Legal Services, specifically Identity Theft Shield. She initially could not decide how to answer the question because she did not go to a specific law firm and speak with a lawyer face-to-face. However, she eventually decided that she should say “yes.”

The revised wording of part c. worked well. Two respondents said “yes.” One of these respondents initially wondered about reporting contacting the FTC in part b. and decided not to. The next asked about the FTC, and it was clear where her response should go.

Rounds 6 through 8

24. Next, I'm going to read you a list of other people and organizations that someone might contact when their personal information is misused. Which of the following people or organizations, if any, did you contact? Did you

(READ ANSWER CATEGORIES)

a. Hire a lawyer?	**YES**	**NO**
b. Contact a State or local government consumer affairs agency, such as the State Attorney General's office?	**YES**	**NO**
c. Contact the Federal Trade Commission?	**YES**	**NO**
d. Contact a consumer agency, such as the Better Business Bureau or the National Consumer League?	**YES**	**NO**
e. Contact <u>an agency</u> or company that issues documents like driver's licenses, social security cards, or insurance cards?	**YES**	**NO**
f. Contact your credit monitoring service or identity theft insurance company?	**YES**	**NO**
g. Contact some other group or organization?	**YES (specify)** _____	**NO**

Summary of Results:

For the remaining rounds of pretesting, one of the survey sponsors requested that the wording of part e. be revised. Instead of "*Contact an organization or company that issues documents like driver's licenses, social security cards, or insurance cards,*" it read "*Contact an agency or company that issues documents like driver's licenses, social security cards, or insurance cards.*"

Four respondents were administered this version of the question.

There were no problems with the revised wording of this question. Three of the four respondents said "yes." One respondent, however, reported contacting Social Security in response to category g. He apparently did not realize that it should have been reported in category e.

One other respondent reported something in part g. She said she contacted the Banking and Securities Commission. She thought about it when she answered part d., but she decided it didn't belong there.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

SECTION E: VICTIM IMPACT

In this section, there was one global problem common to all questions. As with Section C, respondents were instructed to think only about the "most serious" misuse when answering questions in this section. These questions were structured to allow the "automatic fill" of this most serious misuse, which we added when reading the question. For example, if a respondent chose the misuse of a bank account as the most serious misuse, the question would read, "Did the misuse of your *bank account*…?"

As with Section C, it became apparent during the retrospective probing, as well as during the questionnaire itself, that respondents were not successful at limiting their focus to the most serious misuse. This lack of focus was problematic because respondents most likely were misreporting the emotional and physical impact of that particular misuse. It did not seem possible for respondents to partition the different emotional and physiological experiences associated with each misuse of personal information.

As noted previously (see Q7f), changing the location of the "most serious incident" question and not restricting respondents' answers in this and later sections to a particular misuse of information addressed this problem.

On the following pages are the cognitive testing results for each individual question in Section E.

Question 25:

We tested one version of this question.

25. The misuse of personal information affects people in different ways. Next I would like to ask you some questions about how the misuse of <your personal information/fill in the blank> may have affected you.

Did the misuse of <your personal information/fill in the blank> lead you to have significant problems with your job or schoolwork, or trouble with your boss, coworkers, or peers?

___*1. Yes*
___*2. No*

Summary of Results:

This question was administered to 19 respondents. Only one respondent answered in the affirmative. She believed cleaning personnel at her job stole her credit card. After the respondent reported these suspicions to her company, the cleaning staff no longer acted friendly toward her.

We did not observe any problems with this question. In general, respondents were able to understand and answer it. However, one respondent took time to consider the term "significant." This respondent indicated that she did miss some work and was somewhat distracted when trying to resolve her identity theft experiences. She ultimately decided that while her identity theft experience was disruptive to her work life, this disruption was not "significant." The respondent said that the disruption wasn't "to the point of losing my job."

This question will not be applicable to some respondents. An 86-year-old respondent answered "no" to this question because she was not working when she experienced identity theft. Although this response is not an error, it also is not accurate. The respondent didn't have the opportunity to experience these types of problems. Because this question is not applicable to respondents who are not in school or do not work, the data will not paint an accurate picture of how often people experience these type of problems. This group of respondents will "dilute" the prevalence rate of these types of problems.

Final recommendation:

If sponsors do not want to commingle the responses of non-workers and non-students, to whom this question does not apply, with the responses of workers and students, then we recommend adding a skip in the instrument based on information previously reported about the person's work status.

Sponsor's feedback:

Recommendation accepted.

Question 26:

We tested one version of this question.

26. Did the misuse of <your personal information/fill in the blank> lead you to have significant problems with family members or friends, including getting into more arguments or fights than you did before, not feeling you could trust them as much, or not feeling as close to them as you did before?

___1. Yes
___2. No

Summary of Results:

We did not observe any problems with this question. All of the respondents were able to understand and answer it. However, it is worth noting that none of the respondents answered in the affirmative. In fact one respondent offered, "No, it had the opposite effect," meaning that she felt closer to friends and family during her identity theft experiences.

*Final Recommendation***:**

No changes.

Question 27:

We tested one version of this question.

27. How distressing was the misuse of <your personal information/fill in the blank> to you? Was it not at all distressing, mildly distressing, moderately distressing, or severely distressing?

(DO NOT READ ANSWER CATEGORIES)

(ENTER A SINGLE RESPONSE)
__*1. Not at all distressing - Skip to Q32*
__*2. Mildly distressing - Skip to Q32*
__*3. Moderately distressing - Go to Check Item K*
__*4. Severely distressing - Go to Check Item K*

Summary of Results:

This question was administered to 19 respondents. Three respondents reported that their experience was "mildly distressing;" five reported that their experience was "moderately distressing," and eleven reported that their experience was "severely distressing." No one reported that their experience was "not at all distressing."

Although respondents were able to understand this question, they most likely were not limiting their report to the "most serious" misuse of their personal information. This reporting error was no longer an issue once respondents were no longer limited to reporting on the most serious misuse.

Final recommendation:

No changes.

Question 28:

We tested one version of this question. In Round 6, we added a transition word (underlined in the question text) at the beginning of the question to make it flow better from the previous question. The lack of a transition word did not cause any problems for the respondents. The addition of this transition also did not alter the question meaning, and therefore, for brevity's sake, we present this question as a single version of this question.

28. <u>Still</u> thinking about your distress associated with the misuse of <your personal information/fill in the blank> did you feel any of the following ways for a month or more? Did you feel....

(READ ANSWER CATEGORIES)

a. Worried or anxious?	**YES NO**
b. Angry?	**YES NO**
c. Sad or depressed?	**YES NO**
d. Vulnerable?	**YES NO**
e. Violated?	**YES NO**
f. Like you couldn't trust people?	**YES NO**
g. Unsafe?	**YES NO**
h. Some other way?	**YES** -- specify **NO**
	_____

Summary of Results:

The question was administered to the 16 respondents who indicated that their identity theft experiences were at least moderately distressing or that they experienced significant problems with other people.

Respondents tended to report experiencing more than one of these feelings. One respondent said yes to part f ("like you couldn't trust people"), but indicated that it was distrust in organizations, not individual people. Six respondents chose part h (feeling "some other way"), specifying what they felt that was not captured in the existing response options. There seemed to be no common theme to these responses, and therefore, we do not recommend the addition more response categories. The responses in this category were:

- Surprised -- "How could this happen to me?"
- Cautious
- Bewildered
- Frustrated
- Driven to justice -- "payback"

We did not observe any comprehension problems with this question. Respondents were attending to the duration and onset of feelings when answering this question. They were able to restrict their report to feelings that lasted for at least one month and only report feelings that they experienced as a result of identity theft experiences in the last two years.

However, respondents did have trouble limiting the focus of their answers. They indicated that they were focusing on all of their identity theft experiences in the last two years when answering this question and not just the most serious misuse. However, this issue was no longer problematic when respondents did not have to focus on the most serious misuse.

Final recommendation:

No changes.

Question 29:

We tested two different versions of this question.

Rounds 1 through 4

29. Did you experience any of the following physical problems for a month or more? Did you experience.....

(READ ANSWER CATEGORIES)

a. Headaches?	**YES**	**NO**
b. Trouble sleeping?	**YES**	**NO**
c. Changes in your eating or drinking habits?	**YES**	**NO**
d. Upset stomach?	**YES**	**NO**
e. Fatigue?	**YES**	**NO**
f. High blood pressure?	**YES**	**NO**
g. Muscle tension or back pain?	**YES**	**NO**

Summary of Results:

The nine respondents in these rounds who indicated that they found the misuse of their personal information to be at least "moderately distressing" were administered this version of the question. Six of them did not report experiencing any physical symptoms. Three respondents reported experiencing at least one of these symptoms. Many respondents reported multiple symptoms.

We did not observe any problems with this question Respondents were attending to the reference period. They were able to report symptoms that they experienced for a month or more. In fact, some respondents would answer no, adding "not for a month or more." Respondents also were able to restrict their report to symptoms they experienced only as a result of the misuse of their personal information.

Although we did not observe it, we were concerned about the potential problem that respondents may answer "yes" to this question because they experienced the symptoms prior to their identity theft incident. To prevent this error from happening, we added a reference to the misuse of person information in the question.

Rounds 5 through 8

29. Did you experience any of the following physical problems associated with the <misuse of your personal information/fill in the blank> for a month or more? Did you experience.....

(READ ANSWER CATEGORIES)

a. Headaches?	**YES**	**NO**
b. Trouble sleeping?	**YES**	**NO**
c. Changes in your eating or drinking habits?	**YES**	**NO**
d. Upset stomach?	**YES**	**NO**
e. Fatigue?	**YES**	**NO**
f. High blood pressure?	**YES**	**NO**
g. Muscle tension or back pain?	**YES**	**NO**

Summary of Results:

Seven respondents were administered this version of the question. Six of them reported experiencing at least one of these symptoms. One respondent did not report experiencing any of these symptoms. .

We did not observe any problems with this question. As with the previous version, respondents were able to understand and answer this question and limit their focus to physical symptoms that last one month or longer.

However, respondents most likely were not limiting their report to the "most serious" experience. We observed potential problems with respondents misreporting on their global identity theft experiences and not just the most serious misuse. This problem was no longer an issue in Round 8, when respondents were not restricted only to considering the most serious misuse.

Final recommendation:

No changes from the Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 30/28a:

We tested three different versions of this question. In the first three rounds, this question was intended to reference both physical and emotional symptoms. However, there is an ambiguous frame of reference in this question because it does not specify the type of problems on which the respondent should focus (i.e., physical or emotional). Based on these early pretesting results, we modified this question to refer only to physical problems and added identical follow-up questions (28a & 28b) after Q28.

Rounds 1 through 3

30. Did you seek any kind of professional help for these problems?

___*1. Yes -- Ask Q31*
___*2. No* -- Skip to Q32

Summary of Results:

Five respondents were administered this version of the question. Four of them answered "yes." One respondent refused to answer the question. This reticence may suggest that some respondents will find this question to be sensitive. However, the respondent who declined to answer this question seemed uncomfortable providing details on her experiences and consistently provided vague answers. Other respondents did not seem to echo this same reticence, and therefore, we did not suggest changes to the questionnaire.

The lack of a frame of reference confused some respondents. They were not sure if this question referred to the physical symptoms they reported in the previous question, the emotional experiences they reported in another question, or something else. For example, one respondent asked for clarification before answering because she was not sure how to answer. She initially interpreted the question to be about any actions she might have taken to resolve her identity theft experiences (such as calling credit bureaus or canceling cards), but assumed the question must have been talking about physical symptoms in the previous question. Both interpretations were wrong, because both physical and emotional problems are in scope for the question.

Because of this misinterpretation, we revised the question to explicitly refer to both physical and emotional consequences.

Round 4

30. Did you seek any kind of professional help for the feelings or physical problems you experienced as a result of the <misuse of your personal information/ fill in the blank>?

___*1. Yes -- Ask Q31*
___*2. No -- Skip to Q32*

Summary of Results:

Three respondents were administered this version of the question. All of the respondents answered "no."

We observed no problems with this question. Despite the fact that this question version was not problematic, we felt that the treatment question should be asked immediately after each of the

feeling/symptom questions. Thus, we created two similar questions, one for emotional feelings (Q28a) and one for physical problems (Q30).

Round 5 through 8

28a. Did you seek any kind of professional help for the feelings you experienced as a result of the <misuse of your personal information/ fill in the blank>?

___*1. Yes -- Ask 28b*
___*2. No -- Skip to Q29*

Summary of Results:

Seven respondents were asked this question. Only one respondent answered "yes."

We observed no problems with this question. All of the respondents were able to understand and answer this question.

Final recommendation:

No changes to the Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Rounds 5 through 8

30. Did you seek any kind of professional <u>or medical</u> help for the physical problems you experienced as a result of the <misuse of your personal information/ fill in the blank>?

___*1. Yes -- Ask Q31*
___*2. No -- Skip to Q32*

Summary of Results:

This version was administered to five respondents. No one answered "yes" to this question. One respondent preferred not to answer it.

The re-sequencing of this question cleared up respondent's confusion for the frame of reference. We did not observe any problems.

Final recommendation:

No changes to the Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 31/28b:

We tested one version of this question. In Rounds 1 through 4, this question referred to both physical and emotional reactions to identity theft. In Rounds 5 through 8, this question was added after the emotional experiences question, becoming Q28b.

31/28b. What kind of professional help did you seek?

(DO NOT READ ANSWER CATEGORIES)

(MARK ALL THAT APPLY)
___*a. Counseling*
___*b. Medication*
___*c.Visited doctor or nurse*
___*d. Visited ER/ hospital/clinic*
___*e. Other specify* _____

Q28b Summary of Results:

This question was administered to one respondent (none of the other respondents reported seeking professional help in Q28a). Before and during her identity theft experiences, this respondent regularly saw a therapist. However, once she discovered her identity theft, she also talked about this experience during her sessions.

There is a potential problem with the response options. The respondent indicated that she got help from, "a therapist -- a "Clinical Psychologist." This response was coded as "e -- Other", since the respondent provided a very specific response that was not one of the existing options.

Q28b Final Recommendation:

Since seeing a therapist is qualitatively different from seeing a counselor, and may be a common source of help for respondents, we recommend modifying category a. to reflect visits to both a counselor and a therapist: It would read: *"a. Counseling/therapy."*

Sponsor's Feedback:

Recommendation accepted.

Q31 Summary of Results:

We were not able to test Q31. None of our respondents indicated that they sought treatment for physical symptoms.

Q31 Final Recommendation:

This question is a follow-up to Q30. However, the wording of Q31 is inconsistent with the parent question. The response options in this question also should be consistent with the response option in Q28b (a parallel question on emotional effects). To make the wording consistent, we recommend the following changes:

> *31. What kind of professional or medical help did you seek?*
> *___a. Counseling/therapy*

Sponsor's Feedback:

Recommendation accepted.

SECTION F: 0FFENDERS

Question 32:

We tested two different versions of this question.

Rounds 1 through 4

32. Do you know, or have you learned, anything about the person(s) who misused <your personal information/fill in the blank>?

__1. Yes - Ask Q33
__2. No - Skip to INTRO, Section G, Financial Impact on page 9

Summary of Results:

This question was administered to 11 respondents. Only one respondent answered "yes."

Respondents adopted a conservative response threshold. They seemed to have a very strict definition of "know anything" and were reluctant to respond in the affirmative to this question. Some respondents knew the names or addresses associated with some of the misuse, but were reluctant to "incriminate" people. They were not sure knowing names or addresses constituted "knowing anything."

To encourage respondents to consider speculative or uncertain information when answering this question, we revised the wording to read: *"Do you know, or have you learned, anything at all about the person(s) who misused <your personal information/fill in the blank>?"*.

Rounds 5 through 8

32. Do you know, or have you learned, anything at all about the person(s) who misused <your personal information/fill in the blank>?

__1. Yes - Ask Q33
__2. No - Skip to INTRO, Section G, Financial Impact on page 9

Summary of Results:

Eight respondents were administered this question. Five of them answered "yes."

One respondent answered in the affirmative because she had seen the thieves on security surveillance. However, some respondents still demonstrated reluctance when answering this question. This reluctance was due to individual definitions of what constitutes "knowing" something about the identity thief. Although one respondent saw the person who stole her wallet, she wasn't sure that constituted "knowing." Another respondent who also had her wallet stolen expressed the same reluctance. She knew "how" her wallet was stolen -- by someone she didn't know -- but not "who" stole it. Respondents seemed to interpret this question to be asking about some level of personal relationship with the identity thief, rather than to be asking if it was "anonymous" (someone they did not know at all) or more "personal" (a friend, family member, employee, etc).

Respondents also may not answer "yes" if they believe the information is not veridical. One respondent had names and addresses for the people that had applied for credit under his name. However, this respondent answered "no" to this question because he was sure this information probably was not real or accurate. He figured the identity thief or thieves were using aliases and fake addresses. If a respondent has doubts about the truthfulness of the information he or she has, changes to the questionnaire most likely will not influence this evaluation.

Final recommendation:

No changes to Round 8 questionnaire. However, the sponsor should be aware that the information obtained in this question may not be accurate.

Sponsor's feedback:

Recommendation accepted.

Question 33:

We tested one version of this question. This question was only asked of respondents who answered "yes" to Q32 (the respondent knew something about the person who misused their personal information).

33. Was the person who misused <your personal information/fill in the blank> someone you knew or had seen before, or a stranger?

__1. Knew or had seen - Ask Q34
__2. Stranger -- Skip to INTRO, Section G, Financial Impact on page 10

Summary of Results:

Seven respondents were administered this question. One respondent indicated that she knew the identity thief. All other respondents answered "no."

We observed no problems with this question. Respondents were able to understand and answer it.

Final recommendation:

No changes.

Question 34

We tested one version of this question. This question was asked only of respondents who reported in Q33 that they knew the person who misused their personal information.

34. How well do you know this person? For example, was the person a family member, friend, acquaintance, salesperson, or somebody else?

(DO NOT READ ANSWER CATEGORIES)

RELATIVE
___a. Spouse (ex-spouse)
___b. Parent or step-parent
___c.Brother or sister
___d. Child or step-child
___e. Other relative (specify) _____

NONRELATIVE WELL KNOWN
___f. Boyfriend or girlfriend (ex-boyfriend or ex-girlfriend)
___g. Friend or ex-friend
___h. Housemate
___i. Neighbor
___j. Co-worker
___k.Someone working in my home (babysitter, housecleaner, etc.)

NONRELATIVE NOT WELL KNOWN
___l. Casual acquaintance
___m. Salesperson
___n. Waiter

NONRELATIVE OTHER
___o. Other non-relative (specify) _____

Summary of Results:

Only one respondent was asked this question. This respondent indicated that she "knew" the person who had misused her personal information. She defined "someone you knew" as "someone I had personal interaction with, either over the phone or face-to-face."

The respondent thought this was a multiple choice question. She originally said, "acquaintance," because she thought the example categories in the question were all-inclusive. After the interviewer clarified that this was an open-ended question, the respondent then chose "housemate," since it was a tenant who misused her personal information. This error was most likely the result of the content of the exampled text.

Final recommendation:

While we do not have any recommendations for change, sponsors should be aware that the ambiguous nature of the "example" sentence may create the potential for respondent confusion and inaccurate responses.

SECTION G: FINANCIAL IMPACT

Question 35:

We tested one version of this question.

> ***Read only if more than one type of incident was reported in Q1:*** **Earlier you told me someone misused <fill all types reported in screener>. I would like you to think about all of these types of misuses during the last TWO years.**
>
> **35. Since _____, 20____, what is the approximate total dollar value of what someone obtained while misusing your personal information? Include the value of goods, services, credit, loans, cash, and anything else the person may have obtained.**
>
> *RECORD THE ESTIMATED AMOUNT.*
> *$_____.00*
> *(IF OVER $1,000, PROBE: I just want to verify that the total amount is (INSERT AMOUNT RESPONDENT INDICATED)*
> *IF response = $0, skip to Q. 37.*

Summary of Results:

This question was administered to 19 respondents. Responses reported ranged from $40 to more than $80,000.

Three respondents provided potentially problematic responses:

- One respondent provided a "don't know" response. This respondent seemed reluctant to provide information about her experiences throughout the interview. She declined to answer other questions during the interview. However, it is unclear if she had no knowledge of the dollar amount involved or if she just did not want to provide that information.

- Two other respondents may not have experienced actual identity theft. Both respondents reported that no one obtained any money. One respondent had only experienced attempted identity theft, but problems with an early version of the screener question led to a misreporting of the experience as actual identity theft. The other respondent may not have experienced either actual or attempted identity theft. She reported what may have been a clerical error in administrative records as an instance of identity theft. Her health insurance company had a different address on file and did not have her listed in the correct state. This

may have been a "paperwork error" that led to the wrong state being entered. However, this respondent thought it might have been identity theft. She had no other experiences.

For the most part, respondents were able to understand that the question was asking about the amount of money the identity thieves "took." They included the appropriate items in their calculations, such as the amount of new credit, withdrawals from accounts, fraudulent charges, and other new accounts, when answering this question,.

However, some respondents seemed unwilling or unable to provide a detailed and accurate estimate of the exact dollar amount. They understood what to include, but seemed "over-taxed." They gave rough estimates rather than engage in the cognitive processes necessary to recall and tally the actual amount.

Final Recommendation:

The complicated introduction to this question is no longer necessary. It was necessary when respondents were asked to focus on the most serious misuse in the previous section. However, they are no longer focusing on just one incident, and the introduction is making this question wordy. We recommend deleting the introduction and rephrasing the question stem to read: *"Thinking about all of the types of misuses of your personal information during the last TWO years, that is, since _____, 20__, what is the …"*

Sponsor's feedback:

Recommendation accepted.

Question 36:

We tested three different versions of this question.

Rounds 1 through 3

36. Of this total, how much, if anything, did you personally lose?

RECORD THE ESTIMATED AMOUNT.
$_____.00

(IF "NONE," PROBE: Just to confirm, you didn't have to pay anything?)

Summary of Results:

This question was administered to seven respondents. They generally understood and were able to answer this question. Respondents understood that they should report any fraudulent charges, withdrawn money, or non-refundable fees. However, we did observe some problems.

Two respondents answered this question incorrectly because they included other costs that should be reported in a later question (Q38). One of them provided a dollar amount associated with evicting the tenant who had stolen and misused her personal information. The other respondent provided the dollar amount associated with making phone calls to clear up the misuse of her personal information.

The term "personally lose" was problematic. Although most respondents understood that the intent of the question was to report what money they were not able to recover, "personally lose" seemed to be the wrong word choice to describe this money. For one respondent, who had her car stolen, the term seemed to imply the intangible or the invaluable things that someone might have lost --like the personal items in her car. For another respondent, "personally lose" also connoted the emotional costs of her identity theft experience. The use of this term may have been what led to the two reporting errors.

Because "personally lose" seemed to evoke a powerful and incorrect context for this question, we revised the question to focus participants' attention back to the dollar amount of fraudulent use in the previous question.

Rounds 4 & 5

36. Of this <autofill from Q.35>, how much, if anything, did you personally lose?

RECORD THE ESTIMATED AMOUNT.
$_____.00

(IF "NONE," PROBE: Just to confirm, you didn't have to pay anything?)

Summary of Results:

This version of the question was administered to eight respondents. Only one respondent reported having lost money. Her bank did not refund approximately $200 in bank fees.

We observed no problems with this question. Respondents understood that this question was asking about unrecoverable funds or charges and answered accordingly.

Although we did not observe any difficulty with this question, we wanted to clarify more specifically the source of the dollar amount respondents should be considering. We revised the question to read: *"Of this <autofill from Q. 35> that they obtained, how much of that money did you personally lose*?"

Rounds 6 through 8

36. Of this <autofill from Q.35> that they obtained, how much of that money did you personally lose?

RECORD THE ESTIMATED AMOUNT.
$_____.00

(IF "NONE," PROBE: Just to confirm, you didn't have to pay anything?)

Summary of Results:

This question was administered to four respondents. Three of them reported that they did not lose any money. One respondent reported charges that she was still disputing with her credit card company.

We did not observe any problems with this version of the question. Respondents did not have any problems understanding or answering it.

Final recommendation:

No changed to the Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 37/40:

We tested one version of this question wording, but we moved the question's location between Rounds 3 and 4. The question numbers reflects its location in Rounds 1-3 (Q37) and Rounds 4 and 5 (Q40) . The question was eliminated at Round 6.

37/40. Has the misuse of your personal information stopped?

___1. Yes -- Ask Q31
___2. No -- Skip to Q32

Summary of Results:

Fourteen respondents were administered this question. We did not record any problems with this question.

However, respondents tended to qualify their responses. A number of respondents added, "as far as I know," hedging their "yes" responses. This hedging most likely reflects the ongoing victimization

associated with identity theft. The respondents may have issues that they have yet to discover, or someone may misuse their information again in the future. The nature of this crime makes it impossible to definitively conclude that the misuse had permanently stopped.

Final recommendation:

Delete the question.

Sponsor's feedback:

Recommendation accepted.

Question 38/37:

We tested two versions of this question. In the first three rounds this question was Q38; in Rounds 4 it was Q37. In Round 4 we also added an introduction (the parenthesized text) to serve as a clarifying transition between this question and the previous question (Q36, reported losses).

Rounds 1 through 6

38/37. (Other than the costs you already told me about,) How much, IF ANY, additional costs did you incur? Include costs for things such as legal fees, payment of any fraudulent debts, and any miscellaneous expenses, such as postage, phone calls, or notary fees. Do not include lost wages.

RECORD THE ESTIMATED AMOUNT.
$_____.00
(IF OVER $1,000, PROBE: I just want to verify that the total amount is (INSERT AMOUNT RESPONDENT INDICATED)

Summary of Results:

This version of the question was administered to 17 respondents. Six of them reported paying a variety of additional costs, including costs for phone calls, postage, police report fees, notary fees, photocopies, driver's license reissuing fees, gas, credit protection fees, and fees for a home security system. Eleven respondents did not report incurring any additional costs.

There may have been one response error based on a respondent's incorrect judgment about what costs should be included. This respondent left out the costs associated with evicting her tenant and making repairs after the tenant caused property damage. The respondent did not think of these as additional costs.

Between Rounds 6 and 7, the sponsor requested that bounced check fees be included in the costs included in the supplementary instruction.

Rounds 7 & 8

38/37. (Other than the costs you already told me about,) How much, IF ANY, additional costs did you incur? Include costs for things such as legal fees, bounced check fees, and any miscellaneous expenses, such as postage, phone calls, or notary fees. Do not include lost wages.

RECORD THE ESTIMATED AMOUNT.
$_____.00
(IF OVER $1,000, PROBE: I just want to verify that the total amount is (INSERT AMOUNT RESPONDENT INDICATED)

Summary of Results:

Two respondents were administered this version of the question. Both respondents reported minimal additional costs.

There was one potential response error. One respondent included the cost of "forty hours of vacation time." He did not indicate a specific dollar value. This respondent took approximately one week of paid vacation from work to resolve his identity theft experiences. Although the question explicitly states that the respondent should exclude lost wages, paid time does not fall under this category. The respondent reported these hours as a representation of the cost in time of his identity theft experiences.

Final recommendation:

No changes from Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 38 (Rounds 6 through 8):

We tested only one version of this question, which was added in Round 6.

38. Have you been successful in clearing up all of the financial and credit problems associated with the misuse of your personal information?

1. *Yes - Ask Q39*
2. *No - Skip to Q40*
3. *Don't Know - Skip to Q40*

Summary of Results:

When we deleted the question that asked if the misuse of personal information had stopped (Q37/Q40), we added this question, which asks if the respondents if they had been able to clear up all their financial and credit problems.

Four respondents were asked this question. Three of them answered "yes." Only one respondent, who was still disputing some credit card charges, indicated that she was still working to resolve financial and credit issues.

We observed no problems with this question.

Final recommendation:

No changes.

Question 39/38:

We tested three different versions of this question.

Rounds 1 through 3

39. How long did it take you to clear up the financial problems associated with the misuse of your personal information?

___a. One day or less
___b. More than a day, but less than a week
___c. At least a week, but less than one month
___d. 1 to 2 months
___e. 3 to 5 months
___f. 6 to 11 months
___g. 1 year to 2 years

Summary of Results:

This question was administered to seven respondents, who were able to understand and answer it. They gave estimates ranging from two weeks to several months.

However, the question contained a problematic presupposition. In these early rounds of pretesting this question was asked of all respondents. However, it sounded awkward for respondents who were still in the process of clearing up their problems.

To address this problem, we changed the question wording to acknowledge and allow for the fact that respondents' issues might not all be resolved. We revised the question to read: "*How long has*

it taken you so far to clear up the financial or credit problems associated with the misuse of your personal information?"

Rounds 4 & 5

38. How long has it taken you so far to clear up the financial or credit problems associated with misuse of your personal information?

___a. One day or less
___b. More than a day, but less than a week
___c. At least a week, but less than one month
___d. 1 to 2 months
___e. 3 to 5 months
___f. 6 to 11 months
___g. 1 year to 2 years
___h. 2+ years

Summary of Results:

This question was administered to eight respondents. Their answers ranged from less than a day more than a year.

We observed no problems with this question. Respondents were able to understand and answer this question. However, the blind response options were not very informative for interviewers when respondents reported the number of days or weeks it took to clear up financial problems rather than the number of months. As with Q7c, the sponsor added parenthesized time frames to provide quick notations about where responses should be marked.

Rounds 6 through 8

39. How long did it take you to clear up the financial and credit problems associated with the misuse after you discovered it?

___ a. One day or less
(1-24 hours)
___ b. More than a day, but less than a week
(25 hours-6 days)
___ c. At least a week, but less than one month
(7-30 days)
___ d. 1 to 2 months
(31-89 days)
___ e. 3 to 5 months
___ f. 6 to 11 months
___ g. 1 year to 2 years
___ h. 2+ years

Summary of Results:

Three respondents were administered this question. Their responses ranged from one month to more than three months. We observed no problems with this question. Respondents were able to understand and answer this question.

Final recommendations:

We recommend rewording response categories 4, 5, and 6 to be strictly continuous, as follows: "one month to less than three months," "three months to less than six months," "six months to less than one year." For the direction of the response categories to be consistent, the last one should read "1 year to less than 2 years." We also recommend that a category "two years or more" be added to ensure that all possibilities are covered.

Sponsor's feedback:

Recommendation accepted.

Question 40/39:

We tested three different versions of this question.

Rounds 1 through 3

40. During this <auto-fill response from Q39> period, how many hours did you spend clearing up problems?

_____ *Number of hours*

Summary of Results:

This question was administered to seven respondents. Their responses ranged from spending less than one hour to spending more than two-hundred hours clearing up problems. They included time spent making phone calls, filing police reports, obtaining credit reports, and any other miscellaneous activities necessary to resolve identity theft issues. One respondent reported the unique experience of attending a support group. Her employer had lost copies of employee social security cards and drivers' licenses. As a result, a large number of employees experienced identity theft. These employees met and discussed their identity theft experiences and how to address them.

Respondents' estimates may be inaccurate. Some respondents provided very rough calculations. They seemed to find it difficult to retrieve and add up all of the hours spent resolving issues. Their estimates may be biased or quite inaccurate, especially for long, drawn out experiences or remote isolated experiences.

In order to clarify that respondents should report hours spent clearing up the financial and credit consequences of identity theft, the sponsors requested a change in the wording of this question to read: *"During this <fill response from Q39> period, how many hours did you spend clearing up financial or credit problems?"*.

Round 3 through 5

39. During this <fill response from Q38> period, how many hours did you spend clearing up financial or credit problems?

_____ *Number of hours*

Summary of Results:

Eight respondents were administered this version of the question. Their responses ranged from less than one hour to more than eight hundred hours. Respondents included similar activities in their estimates as respondents in Rounds 1 and 2 included (with the exception of the support group).

We observed no global problems with this question. However, one respondent, an 86-year-old woman, had recall issues when attempting her calculations. The interviewer probed based on her limited responses, and the respondent eventually arrived at a number. She had spent hundreds of hours clearing up her problems and was unable to do the estimation and mathematical calculation required for an accurate answer.

The interviewers found that this question was awkward to administer with the autofill option. The wording of the response options from Q38 didn't flow naturally into the next question. As a result, we revised the question to delete the autofill.

Rounds 6 through 8

With the addition of Q38 in Round 6, the question was revised to reference the period of time spent clearing up financial problems for respondents who reported in Q38 that they were successful at clearing up these problems. This bracketed text did not identify to the specific period of time reported in Q39, but simply referred to that period.

40. [During that period,] How many hours have you spent clearing up financial or credit problems?

_____ *Number of hours*

Summary of Results:

Four respondents were asked this question. Their answers ranged from 20 to 120 hours. Respondents who answered this question reported similar actions in their estimates as respondents

in the previous rounds, such as time spent making phone calls to various companies and agencies and writing and notarizing letters.

We again observed that some respondents were reluctant to go through the necessary mental calculations. It is worth noting that some respondents will only provide rudimentary guesses about the number of hours they spent clearing up issues.

The interviewers felt that even the newly-inserted, brief, bracketed text was awkward and did not flow well from the previous question.

Final recommendation:

We recommend deleting this bracketed text, and substituting different verb tense when the respondent has answered "yes" to Q38 as follows: *"How many hours <have you spent/did you spend> clearing up financial or credit problems?"*

Sponsor's feedback:

Recommendation accepted.

Question 41:

We tested three different versions of this question.

Round 1

41. Next I have some general questions about any other problems that you might have experienced as a result of the misuse of your personal information.

Other than anything we have already talked about, what types of problems, IF ANY, have you experienced as a result of the misuse of your personal information? For example, have you been turned downed for a loan?

(DO NOT READ ANSWER CATEGORIES)

(MARK ALL THAT APPLY)

CREDIT RELATED
a. Had to repeatedly correct the same information on your credit reports
b. Had credit problems, such as being turned down for a credit card, or having a card rejected
c. Been turned down for a loan or had to pay higher rates
d. Had banking problems, such as being turned down for a checking account, or having checks bounce

OTHER LIFE EVENTS
e. Had phone or utilities cut off or been denied new service
f. Been turned down for insurance or had to pay higher premiums
g. Been turned down for a job/lost a job
h. Had a debt collector or collections department contact me
i. Had a lawsuit filed or a judgment entered against me
j. Been the subject of an arrest or criminal proceeding

OTHER
k. Had some other type of problems? - (specify)
_____
_____

Summary of Results:

Only one respondent was asked this question. Initially this respondent indicated that she did not experience any other consequences, but on further probing, the respondent indicated that credit bureaus call when she applies for credit.

Although only one respondent answered the question, it was clear to us that respondents would have no frame of reference for what types of answers were in-scope for this question. Without examples to establish the response context, respondents most likely would continue not to report any of these

common consequences. To address this problem, we revised the question to ask specifically about the types of problems of interest to the sponsor.

Rounds 2 through 4

41. Next I have some general questions about any other problems that you might have experienced as a result of the misuse of your personal information.

Other than anything we have already talked about, have you experienced any of the following problems? Have you…

(READ ANSWER CATEGORIES)

a. Had credit related problems, such as having to repeatedly correct the same information on your credit report, being turned down for credit or loans, or having to pay higher rates?	**YES NO**
b. Had banking problems, such as being turned down for a checking account or having checks bounce?	**YES NO**
c. Had Debt Collectors or collections departments contact you?	**YES NO**
d. Had utilities cut off or been denied new service?	**YES NO**
e. Been turned down for a job or lost a job?	**YES NO**
f. Had legal problems, such as having a lawsuit filed against you or being the subject of an arrest or criminal proceedings?	**YES NO**
g. Had some other type of problems?	**YES** (specify) _____ **NO**

Summary of Results:

Ten respondents were asked this version of the question. Seven of them did not report experiencing any of these problems. Three respondents reported experiencing at least one problem.

The multiple choice version of this question was successful in capturing the diversity of additional problems respondents had experienced.

This question was too long and wordy. One respondent originally reported credit problems in part a. Because of the wordy stem and long response options, the respondent had forgotten that this question referenced the misuse of her personal information. She misreported the credit problems because she thought this question was asking about general financial problems. The respondent has had credit problems in the past.

We revised the question to remind respondents of the point of the question. Between part b and part c we reiterated: "As a result of the misuse of your personal information…"

Rounds 5 through 8

41. Other than anything we have already talked about, have you experienced any of the following problems as a result of the misuse of your personal information? Have you…

(READ ANSWER CATEGORIES)

a. Had credit related problems, such as having to repeatedly correct the same information on your credit report, being turned down for credit or loans, or having to pay higher rates? **YES NO**

b. Had banking problems, such as being turned down for a checking account or having checks bounce? **YES NO**

As a result of the misuse of your personal information, have you...

c. Had Debt Collectors or collections departments contact you? **YES NO**

d. Had utilities cut off or been denied new service? **YES NO**

e. Been turned down for a job or lost a job? **YES NO**

f. Had legal problems, such as having a lawsuit filed against you or being the subject of an arrest or criminal proceedings? **YES NO**

g. Had some other type of problems? **YES** (specify) _____ **NO**

Summary of Results:

Eight respondents were administered this version of the question. Three of them did not report experiencing any of these problems. Five respondents reported experiencing at least one problem.

We observed no problems with this version of the question.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 42:

We tested one version of this question. It was omitted for the final round of cognitive testing at the sponsor's request.

Rounds 1 through 7

42. In your opinion, what was the hardest part of your experiences with the misuse of your personal information?

(RECORD VERBATIM. PROBE FOR CLARIFICATION. IF RESPONDENT IS UNSURE, ENCOURAGE BEST GUESS)

_____
_____
_____
_____
_____
_____

Summary of Results:

Eighteen respondents were administered this question. Respondents were able to verbalize the most difficult aspect of their identity theft experiences.

Final recommendation:

Because this question was deleted, we have no recommendations.

SECTION H: ATTEMPTED IDENTITY THEFT MODULE

This module contains a subset of the questions in Sections B-G, modified to apply to attempted identity theft.

We interviewed four respondents who experienced attempted identity theft. Although these questions did not receive much testing, they were modified each time changes were made to the parallel questions in sections B through G. We completed one interview in Round 1, one interview in Round 7, and two interviews in Round 8. We include only the versions of questions from these rounds of testing.

Round 1

INTRO: Now, I would like to ask you some questions about the attempted misuse of your personal information to commit identity theft during the last 2 years.

Question 43:

We tested two different versions of this question.

Round 1

43. How did you FIRST find out someone had attempted to misuse your personal information? When answering this question, please think only about when you found out about the attempted misuse, not when you think your personal information was stolen…

(DO NOT READ ANSWER CATEGORIES)

(MARK ALL THAT APPLY)
DISCOVERED BY RESPONDENT
___ *a. I applied for credit, a bank account or loan, telephone service, employment, or government benefits, etc. and had problems.*
___ *b. I checked my credit report*

NOTIFIED BY FINANCIAL INSTITUTION
___ *c. I received a bill that I did not owe.*
___ *d. Credit card company or bank contacted me about suspicious activity on my account.*
___ *e. A credit monitoring service contacted me.*

NOTIFIED BY OTHER PARTY
___ *f. A law enforcement agency notified me.*
___ *g. A company/agency that had my personal information notified me.*

OTHER
___ *h. Had something else happen - Specify* _____

Summary of Results:

One respondent was administered this version of the question. She reported that "a credit card company or bank contacted me about suspicious activity on my account."

No problems were observed with this question.

Rounds 7 & 8

43. How did you FIRST find out someone had attempted to misuse your personal information? When answering this question, please think only about when you found out about the attempted misuse.

(DO NOT READ ANSWER CATEGORIES)

(MARK ALL THAT APPLY)
DISCOVERED BY RESPONDENT
___ *a. I applied for credit, a bank account or loan, telephone service, employment, or government benefits, etc. and had problems.*
___ *b. I checked my credit report*

NOTIFIED BY FINANCIAL INSTITUTION
___ *c. I received a bill that I did not owe.*
___ *d. Credit card company or bank contacted me about suspicious activity on my account.*
___ *e. A credit monitoring service contacted me.*

NOTIFIED BY OTHER PARTY
___ *f. A law enforcement agency notified me.*
___ *g. A company or agency notified me.*

OTHER
___ *h. Had something else happen - Specify* _____

Summary of Results:

Three respondents were administered this version of the question. We were able to code all three responses into the pre-existing categories. One respondent provided a response that fit into a category revised after Round 2. The respondent received a rejection letter from one of the credit bureaus for a credit card from a fashion retail store.

No problems were observed with this question.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 44:

We tested two different versions of this question.

Round 1

44. Do you know anything about HOW your personal information was obtained?

1. Yes - Ask Q45
2. No - Skip to Q46

Summary of Results:

One respondent was administered this version of the question. Her response was "no."

We observed no problems with this version.

Rounds 7 & 8

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

1. Yes - Ask Q45
2. No - Skip to Q46

Summary of Results:

Three respondents were administered this version of the question. One respondent said "yes" and two respondents said "no."

We observed no problems with this version..

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 45:

We tested two different versions of this question.

Round 1

45. How do you think your personal information obtained? (For example, was it lost or stolen from your wallet, stolen from your postal mail or garbage, or obtained in some other way?)

(DO NOT READ ANSWER CATEGORIES)

(ENTER A SINGLE RESPONSE)
___a. I lost it/It was stolen from my wallet or checkbook
___b. Someone stole it from my postal mail
___c. Someone stole it from my garbage
___d. Someone stole it during a purchase or other transaction
___e. Someone changed my address at the post office
___f. Someone hacked into my computer
___g. I responded to a scam email
___h. My employer
___i. An office/company that had my personal information in its files
___j. Obtained some other way - (specify) _____

Summary of Results:

No one was administered this question, so we were unable to test it.

Rounds 7 & 8

45. How do you think your personal information obtained? (For example, was it lost or stolen from your wallet, stolen from your postal mail or garbage, or obtained in some other way?)

(DO NOT READ ANSWER CATEGORIES)

(ENTER A SINGLE RESPONSE)
___a. I lost it/It was stolen from my wallet or checkbook
___b. Someone stole it from my postal mail
___c. Someone stole it from my garbage
___d. Someone stole it during a purchase or other transaction
___e. Someone changed my address at the post office
___f. Someone hacked into my computer
___g. I responded to a scam email
___h. Stolen from personnel files
___i. An office/company that had my personal information in its files
___j. Obtained some other way - (specify) _____

Summary of Results:

One respondent was administered this version of the question. She said she "responded to a scam email."

We did not observe any problems with this version of the question.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 46:

We tested two different versions of this question.

Round 1

46. Did you talk to anyone at the credit card company, bank, or other company about the attempted misuse of your personal information?

1. Yes
2. No

Summary of Results:

One respondent was administered this version of the question. She said "yes."

We did not observe any problems with this version of the question.

Rounds 7 & 8

46. Did you contact anyone at the credit card company, bank, or other company about the attempted misuse of your personal information?

1. Yes
2. No

Summary of Results:

Two respondents were administered this version of the question. One of them said "yes" and the other respondent said "no."

We did not observe any problems with this version of the question.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 47:

We tested two different versions of this question.

Round 1

47. Did you talk to anyone at a credit bureau the attempted misuse of your personal information?

1. Yes -- Ask Q48
2. No --Skip to Q49

Summary of Results:

One respondent was administered this version of the question. She answered "no."

We did not observe any problems with this version of the question.

Rounds 7 & 8

47. Did you contact anyone at a credit bureau the attempted misuse of your personal information?

1. Yes -- Ask Q48
2. No --Skip to Q49

Summary of Results:

Three respondents were administered this version of the question. One of them said "yes" and two respondents said "no."

We did not observe any problems with this version of the question.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 48:

We tested two different versions of this question.

Round 1

48. You just indicated that you contacted a credit bureau about the attempted misuse of your information. I am going to read a list of things that people sometimes do when their personal information is misused. Did you...

(READ ANSWER CATEGORIES)

a. Request your credit report?	**YES**	**NO**
b. Request corrections to your credit report?	**YES**	**NO**
c. Place an initial, or "90-day" fraud alert on your credit report?	**YES**	**NO**
d. Place a permanent, or "seven year" fraud alert on your credit report?	**YES**	**NO**
e. Send a police report to the credit bureau?	**YES**	**NO**
f. Place a freeze on your credit report, which prevents the credit bureaus from sending your credit report to anyone without your permission?	**YES**	**NO**
g. Do something else?	**YES**	**NO**

Summary of Results:

No one was administered this question, so we were unable to test it.

Rounds 7 & 8

48. When you contacted the credit bureau, did you....

(READ ANSWER CATEGORIES)

a. Request your credit report?	**YES**	**NO**	
b. Request corrections to your credit report?	**YES**	**NO**	
c. Place a fraud alert on your credit report?	**YES** - ask c.1		**NO**
IF D = YES: **c.1 Was it a seven year fraud alert?**		**YES**	**NO**

When you contacted the credit bureau, did you....

e. Send a police report <u>or incident number</u> to the credit bureau?	**YES**	**NO**
f. Place a freeze on your credit report, which prevents the credit bureaus from sending your credit report to anyone without your permission?	**YES**	**NO**
g. Do something else?	**YES**	**NO**

Summary of Results:

One respondent was administered this version of the question. She had recall issues in responding to it. She did not know if she had requested a copy of her credit report. She also knew she placed a fraud alert on her credit report, but she did not know if it was a 7-year alert.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

<u>Question 49:</u>

We tested one version of this question.

49. Did you contact any law enforcement agencies, such as the police or sheriff, to report the attempted misuse of your personal information?

1. Yes -- Ask Q50
2. No --Skip to Q54

Summary of Results:

Four respondents were administered this question. All of the respondents said “no.”

We did not observe any problems with this version of the question.

Final recommendation:

No changes.

Question 50:

We tested two different versions of this question.

Round 1

50. Was it your local law enforcement or another law enforcement agency?

1. Local law enforcement
2. Another law enforcement agency

Summary of Results:

No one was administered this question, so we were unable to test it.

Rounds 7 & 8

50. Was it your local law enforcement or another law enforcement agency?

1. Local law enforcement
2. Another law enforcement agency
3. Other government agency

Summary of Results:

No one was administered this question, so we were unable to test it.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor’s feedback:

Recommendation accepted.

Question 51:

We tested one version of this question.

51. Did this law enforcement agency take a police report from you about the attempted misuse of your information?

___1. Yes - Ask Q52
___2. No - SKIP to Q53

Summary of Results:

No one was administered this question, so we were unable to test it.

Final recommendation:

No changes.

Question 52:

We tested one version of this question.

52. Did you get a copy of the police report?

___1. Yes
___2. No

Summary of Results:

No one was administered this question, so we were unable to test it.

Final recommendation:

No changes.

Question 53:

We tested one version of this question.

53. Did the law enforcement agency provide you with any additional information, such as a pamphlet or prevention material, on what to do when you've experienced identity theft?

___1. Yes - Skip to Q55
___2. No - Skip to Q55

Summary of Results:

No one was administered this question, so we were unable to test it..

Final recommendation:

To make this wording consistent with the parallel question in Section C (Q22), we recommend the following wording change:

53. *Did the law enforcement agency provide you with any additional printed information, such as a pamphlet or prevention material, on what to do when you've experienced identity theft?*

Sponsor's feedback:

Recommendation accepted.

Question 54:

We tested one version of this question.

54. I'd like to learn more about why people who experience identity theft do not report it to law enforcement. Why did you decide not to contact a law enforcement agency?

(DO NOT READ ANSWER CATEGORIES)

(MARK ALL THAT APPLY)

DIDN'T KNOW I COULD
a. Didn't know that I could report it
b. Didn't know what agency was responsible for identity theft crimes

NO LOSS
c. I didn't lose any money
d. It was an attempt/thief was not successful

HANDLED IT ANOTHER WAY
e. Reported it to someone else such as credit card company/bank or other organization
f. Took care of it myself

DIDN'T THINK THE POLICE COULD HELP
g. Didn't think police would do anything
h. Didn't want to bother police/not important enough
i. Didn't find out abut the crime until long after it happened/too late for police to help
j. Couldn't identify the offender or provide much information that would be helpful to the police

PERSONAL REASONS
k. I was afraid to report it
l. The person responsible was a friend or family member and I didn't want to get them in trouble.
m. I was embarrassed
n. Too inconvenient/didn't want to take the time

OTHER
o. Other (specify) _____

Summary of Results:

Four respondents were administered this question. Since this was a Mark-All-That-Apply question, two of these respondents provided more than one response

One of the responses was coded into the "other" category. The respondent said she didn't have the time to report her identity theft to the police.

Final recommendation:

No changes.

Question 55:

We tested two different versions of this question.

Round 1

55. I'm going to read you a list of people and organizations that someone might contact when someone attempts to misuse their personal information. Which of the following people or organizations, if any, did you contact? Did you contact.....

(READ ANSWER CATEGORIES)

a. A lawyer or other legal professional?	**YES**	**NO**
b. A State or local government consumer affairs agency, such as the State Attorney General's Office?	**YES**	**NO**
c. A consumer agency, such as the Better Business Bureau or National Consumer League?	**YES**	**NO**
d. The government agency that issued the lost or stolen identification such as your driver's license?	**YES**	**NO**
e. Your credit monitoring service or identity theft insurance company?	**YES**	**NO**
f. The Federal Trade Commission?	**YES**	**NO**
g. Some other group or organization? (specify)_____	**YES**	**NO**

Summary of Results:

One respondent was administered this version of the question.

The wording of part d. was awkward and the question was not asked by the interviewer. She answered "yes" to part e.

Rounds 7 & 8

55. Next, I'm going to read you a list of other people and organizations that someone might contact when someone attempts to misuse their personal information. Which of the following people or organizations, if any, did you contact? Did you

(READ ANSWER CATEGORIES)

a. Hire a lawyer?	**YES**	**NO**
b. Contact a State or local government consumer affairs agency, such as the State Attorney General's office?	**YES**	**NO**
c. Contact the Federal Trade Commission?	**YES**	**NO**
d. Contact a consumer agency, such as the Better Business Bureau or the National Consumer League?	**YES**	**NO**
e. Contact an agency or company that that issues documents like driver's licenses, social security cards, or insurance card?	**YES**	**NO**
f. Contact your credit monitoring service or identity theft insurance company?	**YES**	**NO**
g. Contact some other group or organization?	**YES (specify)** _____	**NO**

Summary of Results:

Three respondents were administered this version of the question. None of them reported contacting any of these people or organizations.

Final recommendation:

No changes to Round 8 questionnaire.

Sponsor's feedback:

Recommendation accepted.

Question 56:

We tested one version of this question.

56. Do you know, or have you learned, anything about the person who attempted to misuse your personal information?

___1. Yes -- Ask Q57
___2. No -- Skip to Q59

Summary of Results:

Two respondents were asked this question. Both of them said "no." We did not observe any problems with this question.

Unfortunately, a problem with the skip instruction for this question went undetected until Round 8. As a result of this error, two of the respondents who experienced attempted identity theft were not asked any of the other questions in this section.

Final recommendation:

The wording of this question is inconsistent with the parallel question in Section F (Q32). To make this wording consistent, we recommend the following change:

*56. Do you know, or have you learned, anything **at all** about the person who attempted to misuse your personal information?*

Sponsor's feedback:

Recommendation accepted.

Question 57:

We tested one version of this question.

57. Was the person who attempted to use your personal information someone you knew or had seen before, or a stranger?

___1. Yes -- Ask Q58
___2. No -- Skip to Q59

Summary of Results:

No one was administered this question, so we were unable to test it.

Final recommendation:

No changes.

Question 58:

We tested one version of this question.

58. How well do you know this person? For example, was the person a family member, friend, acquaintance, salesperson, or somebody else?

(DO NOT READ ANSWER CATEGORIES)

RELATIVE
___a. Spouse (ex-spouse)
___b. Parent or step-parent
___c.Brother or sister
___d. Child or step-child
___e. Other relative (specify) _____

NONRELATIVE WELL KNOWN
___f. Boyfriend or girlfriend (ex-boyfriend or ex-girlfriend)
___g. Friend or ex-friend
___h. Housemate
___i. Neighbor
___j. Co-worker
___k.Someone working in my home (babysitter, housecleaner, etc.)

NONRELATIVE NOT WELL KNOWN
___l. Casual acquaintance
___m. Salesperson
___n. Waiter

NONRELATIVE OTHER
___o. Other non-relative (specify) _____

Summary of Results:

No one was administered this question, so we were unable to test it.

Question 59:

We tested one version of this question.

59. How much money did you personally pay out of pocket as a result of the attempted misuse of your personal information? Include costs for things such as legal fees, or payment of any fraudulent debts. Also include miscellaneous expenses such as postage, phone calls, and notary fees. Do not include lost wages.

RECORD ESTIMATED AMOUNT.
$_____.00

*(**IF OVER $1,000, PROBE**: I just want to verify that the total amount is (**INSERT AMOUNT RESPONDENT INDICATED**).*

Summary of Results:

This question was administered to two respondents (this question was inadvertently skipped for two respondents). Both respondents indicated that they did not have any out-of-pocket costs.

We did not observe any problems with this question. Both respondents were able to understand and answer this question.

Recommendations:

No changes.

Question 60:

We tested two versions of this question.

Round 1

60. How much time have you spent clearing up credit, financial, and other problems caused by the attempted theft of your information?

(DO NOT READ ANSWER CATEGORIES)

(ENTER A SINGLE RESPONSE)
___*a. One day or less*
___*b. More than a day, but less than a week*
___*c. At least a week, but less than one month*
___*d. 1 to 2 months*
___*e. 3 to 5 months*
___*f. 6 to 11 months*
___*g. 1 year to 2 years*

Summary of Results:

We did not test this version of the question due to a skip pattern error.

Rounds 7 & 8

60. How long has it taken you so far to clear up financial or credit problems caused by the attempted theft of your information?
(DO NOT READ ANSWER CATEGORIES)

(ENTER A SINGLE RESPONSE)
___*a. One day or less*
___*b. More than a day, but less than a week*
___*c. At least a week, but less than one month*
___*d. 1 to 2 months*
___*e. 3 to 5 months*
___*f. 6 to 11 months*
___*g. 1 year to 2 years*
___*h. 2+ years*

Summary of Results:

Two respondents were administered this version of the question. Both respondents reported that they had cleared up all consequences in a week or less.

We did not observe any problems with this question.

Final recommendation:

This question wording is inconsistent with its parallel question (Q39) and the terminology used throughout the questionnaire. To make this question consistent, we recommend the following wording change:

60. How long has it taken you so far to clear up financial or credit problems caused by the attempted misuse of your personal information?

Sponsor's feedback:

Recommendation to reword response categories accepted. New response category not accepted.

Question 61:

We tested two different versions of this question.

Round 1

61. During this <auto-fill response from Q60> period, how many hours did you spend clearing up problems?

_____ *Number of hours*

Summary of Results:

We were unable to test this version of the question due to a skip pattern error

Rounds 7 & 8

61. During that period, how many hours have you spent clearing up financial or credit problems?

_____ *Number of hours*

Summary of Results:

Two respondents were administered this version of the question. One respondent initially misinterpreted it. He seemed to think this question was asking about time spent *after* clearing up all of the original problems. The interviewer probed with the appropriate reference period and the respondent answered correctly. He said, "2 hrs."

Both respondents included time to make phone calls in their responses.

Final recommendation:

We recommend deleting the introductory clause in this question to be consistent with our recommendation for its parallel question (Q40):

61. How many hours have you spent clearing up financial or credit problems?

Question 61a:

This question was added at Round 5 to capture details on the respondents' identity theft experiences. Initially, we thought this detailed information would be useful for reconciling inconsistent reports in the screening section of the questionnaire. However, the significant changes to the first screen question seemed to resolve the response errors. The sponsors decided to keep this question to collect data for their own research purposes.

61a. Now I'd like you to tell me, in your own words, about all of your experiences with the misuse of your personal information.

You mentioned <autofill from Q1 > Can you tell me about that, in your own words?

REPEAT UNTIL ALL CATEGORIES FROM Q1 HAVE BEEN ASKED.

Summary of Results:

We observed no problems with this question. Respondents were able to summarize their experiences. Because this question was so lengthy, it was not administered to all respondents. It is also worth noting that the interviewers found capturing respondent's summaries to be quite onerous. It was difficult to record all of the details as the respondents were relating their story. Because respondents are likely to provide long and disconnected recaps of their experiences, interviewers may not be able to capture much detailed information. They may also abandon this question in the interest of maintaining the respondent's cooperation with the remainder of the survey.

Final recommendation:

Since this question is so time-consuming, we recommend that is be moved to the very end of the questionnaire. This will prevent loss of information in Section I if respondents break off at this point.

SECTION I: RISK AVOIDANCE

This section of the questionnaire went through significant changes across all 8 rounds of pretesting. Question numbers in this section changed as we combined some of the questions.

Rounds 1 through 3

Questions 62 through 66:

We tested two significantly different versions of Q62. In the first three rounds this question was first in a series of questions (Q62 through Q66) on risk avoidance activities.

INTRO: Finally, I'd like to ask some questions about actions that people may take to try to avoid identity theft. For each of these actions, I'd like you to tell me whether or not this is something you do or do not do.

62. Have you checked your credit report in the past year?

1. Yes
2. No

Summary of Results:

Eight respondents were administered this question. Two of them answered "no," and the remaining six respondents answered "yes."

One respondent answered "no" because she had ordered a copy of her credit report but had not yet received it. She has not actually "seen" the report to "check it over", and knows nothing of its content.

Respondents were familiar with the term credit report . Most respondents were able to give a definition of the term. They defined it as a record of all lines of credit and loans that their payment histories and balances.

63. Have you regularly changed passwords on any of your accounts?

1. Yes
2. No

Summary of Results:

Eight respondents were administered this version. Three of them said "yes," and five said "no."

One respondent focused on the word "regularly," which respondents were free to interpret as they chose. He indicated that he changes his passwords, but not "regularly." He ultimately answered

"no." It was unclear how often he changes passwords on his accounts. Different interpretations of regularity will lead to different responses across respondents.

The term "accounts" was too ambiguous. One respondent immediately asked, "Which accounts?" Respondents had different interpretations of this term. When we asked them of what types of accounts they were thinking, some respondents thought this term was referring to any type of account, including e-mail accounts, online banking accounts, or any type of miscellaneous online "account" that requires logging in with a username and password (such as online retailers, Amazon, or eBay). Other respondents thought "accounts" was referring only to financial accounts, such as online banking. We did not specifically probe the kinds of accounts for which respondents had changed passwords, so it is not clear if this ambiguity led to any response errors. We also did not know if the sponsors wanted respondents to only focus on a certain type of accounts.

Respondents had a clear understanding of the term "password." Respondents largely defined passwords in terms of online account access, as a required "security code" or "protection code" for accessing personal information online.

64. Have you ever purchased credit monitoring services or identity theft insurance?

1. Yes
2. No

Summary of Results:

Eight respondents were asked this version of the question. Two of them said "yes," and five said "no." One respondent did not answer this question.

It is not clear whether respondents had a correct interpretation of "identity theft insurance." One respondent referred to "anti-theft" insurance that she got when she opened a new credit card account. The respondent indicated that this insurance came with the card, but covered all three of her existing credit cards.

Another respondent, who answered "no," said she had purchased "insurance" through her credit card company. She responded to an advertisement offer she saw on the envelope she used to mail back her statement. This insurance seems to only cover this credit card, protecting her from fraudulent charges if the respondent loses the card or it is stolen. Given this description, her response was most likely correct.

Finally, although it did not lead to a response error, one respondent had a misconception of credit monitoring services. The respondent had actually purchased credit monitoring services through her bank. She answered this question correctly. However, she also considered placing a fraud alert on her credit report to be "purchasing credit monitoring services."

65. Do you regularly shred or destroy documents that contain personal identifying information?

1. Yes
2. No

Summary of Results:

Eight respondents were asked this version of the question. Seven of them indicated that they regularly shred documents. One respondent indicated that she did not.

We did not observe any problems with this version of the question.

66. Do you use any type of security software program on your computer to protect it against unwanted access over the internet (for example, a firewall)?

1. Yes
2. No

Summary of Results:

Eight respondents were asked this version of the question. Five of them indicated that they had security software. Three respondents indicated that they did not, have security software.

Although respondents had a hard time providing a formal definition of the term "firewall," this difficulty generally was not symptomatic of any misconceptions of the term. Respondents were able to elucidate a firewall's function: to prevent unwanted access to a computer. However, one respondent didn't think a firewall protected a computer "over the internet." She was familiar with the term firewall but wasn't completely sure she knew what it was. This respondent was positive that her computer did not have any sort of protection in the form of a firewall or anti-virus software. Another respondent indicated that she only used her son-in-law's computer and assumed that he "had everything on it," and therefore, answered in the affirmative. It is not possible to know if this is a response error.

Rounds 4 through 8

In rounds 4 through 8, Q62 became a combination of the Q62 through Q66 series. We tested two different versions of this combined question series (Rounds 4 & 5; Rounds 6-8). In Round 4 we also added two different preambles to this question -- one preamble for respondents who have experienced identity theft and one for all other respondents.

Question 62:

Rounds 4 & 5

62. ***Read if any "yes" in Q1b. or Q1d. or Q1f. or Q1h.or Q1j (victim):*** **The next set of questions ask about actions, that people may take to try to avoid identity theft. During the last 12 months, even if this was before your identity theft, have you...**

Read if "no" in Q1b and Q1d. and Q1f. and Q1h. and Q1j. (not a victim):
Next, I'd like to ask some questions about actions that people may take to try to avoid identity theft. For each of these actions, I'd like you to tell me whether or not this is something you do or do not do. During the last 12 months, have you...

a. checked your credit report?	**YES**	**NO**
b. changed passwords on any of your accounts?		
c. purchased credit monitoring services or identity theft insurance?	**YES**	**NO**
d. shredded or destroyed documents that contained personal identifying information?	**YES**	**NO**
e. checked your banking or credit card statements for unfamiliar charges?	**YES**	**NO**
f. used any type of security software program on you computer to protect it against unwanted access over the internet (for example, a firewall)?	**YES**	**NO**

Summary of Results:

All of the 8 respondents in these rounds indicated taking at least one of these actions in the past 12 months.

One respondent pointed out that all of these activities were "typical to his household." He kept reiterating that he regularly performed these actions, and not just as a result of his identity theft experiences. This respondent seemed to have missed the reference frame of the intro, which states these activities may be independent of identity theft experiences.

Respondents in these rounds generally understood the term "credit report," and also defined it as a record of credit history. However, one respondent had a misconception of the term. She confused credit report with a credit card statement. She has a joint credit card account with her father, who checks over the statement. She thought checking over the monthly statement was the same as checking a credit report. We did not find out if she has ever seen her actual credit report.

We again observed that the term "accounts" was too ambiguous. One respondent asked us to clarify what types of accounts he should consider. Because of this ambiguity, respondents also adopted diverse interpretations of the term, which included bank accounts, e-mail, accounts, and other miscellaneous online accounts. We did not ask participants to indicate for which accounts they had changed passwords, so we do not know if there were any response errors. However, based on

communication with the sponsors, we determined that "financial accounts" was the desired reference category.

These respondents also had similar definitions for passwords, and tended to view PINs as passwords. In these rounds, two respondents did not think a PIN was a password. As one of these respondent said, "They wouldn't call it a PIN if it were a password, right?"

We again observed some ambiguity with the concept of a firewall. Respondents knew the function of a firewall (to prevent unwanted access to a computer), but had some difficulty providing a formal definition. However, in this round, the unfamiliarity of this concept may have lead one respondent to commit a response error. She answered "no," but she was not certain she was correct. She didn't know the difference between a firewall and anti-virus software, and was answering "conservatively," based on of her uncertainty.

Because "accounts" was ambiguous, and respondents were not adopting the desired interpretation, we revised the question to clarify the type of accounts that are in scope:

b. changed passwords on any of your financial accounts?

Rounds 6 through 8

62. ***Read if any "yes" in Q1b. or Q1d. or Q1f. or Q1h.or Q1j (victim):*** **The next set of questions ask about actions, that people may take to try to avoid identity theft. During the last 12 months, even if this was before your identity theft, have you...**

Read if "no" in Q1b and Q1d. and Q1f. and Q1h. and Q1j. (not a victim):
Next, I'd like to ask some questions about actions that people may take to try to avoid identity theft. For each of these actions, I'd like you to tell me whether or not this is something you do or do not do. During the last 12 months, have you...

a. checked your credit report?	**YES**	**NO**
b. changed passwords on any of your financial accounts?		
c. purchased credit monitoring services or identity theft insurance?	**YES**	**NO**
d. shredded or destroyed documents that contained personal identifying information?	**YES**	**NO**
e. checked your banking or credit card statements for unfamiliar charges?	**YES**	**NO**
f. used any type of security software program on you computer to protect it against unwanted access over the internet (for example, a firewall)?	**YES**	**NO**

Summary of Results:

All seven respondents in these rounds reported engaging in at least one of these activities in the last 12 months.

We observed two different response errors. First, one respondent indicated that she did not have security software. She misheard the question, thinking it asked if she had *purchased* the security software. This respondent already had security software that she had purchased more than twelve months ago.

Second, one respondent erroneously answered in the affirmative for checking her credit report. She recently secured a mortgage to purchase a home. The mortgage company ran a credit check. She thought this question was asking if anyone has run a credit check on her credit history, rather than asking if she herself had looked over her own credit report.

Respondents continued to have difficulty defining a firewall, sometimes having a tenuous grasp on its function. However, it seems that this difficulty is not based on the ambiguity of the terms, but rather is based on people's average degree of technological savvy. People may not be aware of how their computer works and exactly what types of programs they have. Modifications to this question will not change respondents' lack of knowledge. Further, respondents generally knew whether or not they had a firewall, even though they could not define the term.

Question 67/63:

We tested one version of this question.

67/63. Do you know if you can get a free credit report from the national credit bureaus every year?

1. Yes
2. No

Summary of Results:

Three respondents said "yes" and 19 said "no." Due to interviewer error, one respondent was not asked this question. Interestingly, some respondents spontaneously offered that it was possible to get this free credit report when they indicated that they had checked their credit report within the last year (Q62).

There may have been one response error. A respondent answered "yes," but then went on to describe pop-up ads for free credit report. In the interest of time, the interviewer did not probe this response. However, it does not seem that this respondent was thinking of the law that allows consumers to get a free credit report. He seemed to be thinking of promotions from banks, credit bureaus, and credit monitoring services. Although the misconception technically did not lead to a response error (because the question does not specify that it is referencing this federal law), the respondent did not base his response on the correct information.

Question 68/64:

We tested four different versions of this question. This question was extremely problematic. Despite significant revisions across all of the rounds of cognitive testing, respondents were misinterpreting the intended meaning of this question. The result of this misinterpretation was an indeterminate number of response errors.

Round 1

68. Have you ever been notified by a company, government agency, or other organization of a breach involving your personal information, such as an account number or your social security number?

1. Yes
2. No

Summary of Results:

Two respondents answered this version of the question. Both of them incorrectly answered "yes." Although they had different definitions of the term "breach" (a "broken promise" or "broken security line"), they both committed the same response error. They interpreted this question to be asking about how someone got a hold of the information that resulted in their respective identity theft experiences.

We revised the question to be more specific and to provide an example that would differentiate this question from the actual misuse the respondent experienced (if it was not the result of a breach).

Rounds 2 & 3

68. Has a company, government agency, or some other organization that has your personal information on file ever informed you of a "security" breach involving this personal information? For example, has a company ever notified you that its computer system was hacked and your personal information was stolen, or that one of its laptops containing your personal information had been lost or stolen?

1. Yes
2. No—Go to END

Summary of Results:

Two of the six respondents in these rounds of pretesting indicated that they had received a breach notification.

Although these respondents in this round seemed to understand the reference to the term "breach," we observed two misinterpretations. First, one respondent, who answered "no" to this question, thought that it was only asking about a definitive breach of her account information. She received a

letter from a retail store indicating that her account *may* have been stolen. This respondent answered "no" because she wasn't sure her account information actually was breached. Second, a respondent answered "no" because her breach involved hard copies (photocopies) of her personal information. An employer had lost a stack of photocopies of drivers' licenses and Social Security cards. The respondent thought this question was only asking about electronic copies of personal information.

Because of these response errors, we revised the question to include different formats of information and potential loss or left.

Rounds 4 & 5

64. Has a company, government agency, or some other organization that has your personal information on file ever informed you of a "security" breach involving this personal information? For example, have you ever been notified that paper or electronic files containing your personal information may have been lost, stolen, or posted on a publicly available website?

1. Yes
2. No – Go to Q66

Summary of Results:

Three of the eight respondents in these rounds indicated that their personal information had been breached.

One respondent who answered this version of the question had the same misconception of the term "breach" as respondents who answered the first version of this question. She erroneously answered "yes" because she thought the "breach" referenced the actual theft of their personal information.

Although the majority of the respondents seemed to give the correct answer, we saw evidence that they were not interpreting this question correctly. Respondents tended to think that this question was only about breaches where the personal information was actually lost or stolen, and not just potentially lost or stolen. If a respondent receives a letter indicating that the information was not definitively compromised, there is a potential for the respondents to answer this question incorrectly.

The term "breach" seemed to be problematic for respondents. It did not adequately communicate the intended meaning of this question and was potentially confusing. We revised the question to delete the term and to simplify the question wording.

Rounds 6 through 8

64. Has a company, government agency, or some other organization that has your personal information on file ever notified you that paper or electronic files containing your personal information may have been lost, stolen, or posted on a publicly available website?

1. Yes
2. No – Go to Q66

Summary of Results:

Five of the seven respondents who were asked this version of the question indicated that they had received this type of notification. Two respondents indicated that they had not received this type of notification.

In these rounds of cognitive testing we did not see the same misinterpretation of "breach." However, we did observe one new misinterpretation of this question. One respondent thought this question was asking about websites selling or giving people's e-mail or other personal information to third party vendors. He also thought this question was referring to the firewall protection warnings that pop-up when someone accesses a secure or unsecured website. This warning indicates that information can be seen by third parties. Although this misinterpretation did not lead to a response error (the respondent had no reason to believe anyone had gotten a hold of his personal information this way), it signifies the highly problematic nature of this question.

Final recommendation:

We recommend that this question be deleted.

Sponsor's feedback:

The recommendation was not adopted.

Question 69/65:

We tested two different versions of this question.

Round 1 through 5

69/65. Did this breach notification indicate that your social security number was included in the information that was breached?

1. Yes
2. No

Summary of Results:

Only respondents who indicated that they had received a breach notification in the previous question were asked this question. Six respondents were administered this question. Five of them indicated that their SSN was not part of this breached information, and one respondent said she didn't know.

The DK response was a potential response error. The respondent indicated that the breach letter did not explicitly state that that her SSN was part of the breached information. However, the respondent was skeptical that this omission meant that her Social Security Number had not been exposed.

We observed no other problems with this question.

Although this question was not problematic, because it is a follow-up to Q64, we revised it to reflect the changes in language to the parent question. Namely, we deleted the term "breach."

Rounds 6 through 8

65. Did this notification indicate that your social security number was included in the information that was lost, stolen, or posted on a publicly available website?

1. Yes
2. No

Summary of Results:

Three of the four respondents who were asked the question answered "no" to this question and the remaining respondent answered "don't know." This respondent had received two such notifications but could not remember if they mentioned his Social Security Number.

We observed no problems with this version of the question.

Final recommendation:

We recommend that the question be deleted, since we recommend deleting its parent question (Q64).

Sponsor's feedback:

The recommendation was not adopted.

Question 66:

At the sponsor's request, this question was added in Round 4. We tested one version of this question.

66. My final question has to do with your Internet activity. During the past 12 months, have you used the Internet to purchase anything online?

1. Yes
2. No

Summary of Results:

Fifteen respondents were administered the question. Thirteen of them indicated that they had made online purchases in the last 12 months. Two respondents said they had not.

There may have been one response error. One respondent answered in the affirmative, but added that she did not actually make the online purchases. Her son uses her credit card to make online purchases. If the sponsors intend for the respondent to answer only about their own behavior, then this is a response error. However, if the sponsors are concerned only about the "vulnerability" of the respondents account information, then this is a correct answer. The respondent's account number is vulnerable when her son uses it.

Final recommendation:

No changes.

Question 67:

At the sponsor's request, this question was added in Round 6, as a follow-up to Q66. We tested one version of this question in the final three rounds.

67. About how many times during the past year have you purchased something online?

If R offers a range: Of that <range>, what is your best estimate?

_____ Number of times

Summary of Results:

Respondents reported making online purchases between 3 and 50 different times in the past year.

The probe worked well for this question. Some respondents were vague in their estimates, giving ranges. When prompted to pick a specific value, respondents were able to make the mental

calculation. However, it is worth noting that because respondents may have a hard time remembering or calculating the number of online purchases, this question may yield inaccurate estimates.

Final recommendation:

No changes.