Synovate
1650 Tysons Blvd
Suite 110
McLean VA
22102

Tel 703 790 9099
Fax 703 790 9181
www.synovate.com

synovate
Research reinvented

Federal Trade Commission – 2006 Identity Theft Survey Report

Prepared for Federal Trade Commission

Prepared by Synovate

November, 2007

Table of Contents

Executive Summary

Identity theft (ID theft) is an issue that continues to plague consumers, businesses, and law enforcement. To provide greater insight into the prevalence and cost of ID theft, the Federal Trade Commission (FTC) has sponsored its second ID theft survey of US adults. The specific objectives of the survey were to:

- Estimate the prevalence of ID theft victimization
- Measure the impacts of ID theft on the victims
- Identify actions taken by victims
- Explore measures that may help victims of future cases of ID theft

The study was conducted through telephone interviews using a Random-Digit-Dialing (RDD) sampling methodology. This system was designed to obtain a random sample of U.S. adults age 18 and older. A total of 4,917 interviews were conducted between March 27 and June 11, 2006.

Table 1: Prevalence of ID Theft in 2005, by Category of Misuse

	Percent of Adult Population[1]	**Number of Persons (millions)[2]**
New Accounts & Other Fraud	0.8 % (0.5 % - 1.2%)	1.8 (1.2 – 2.8)
Misuse of Existing Non-Credit Card Account or Account Number	1.5 % (1.1% - 2.1%)	3.3 (2.4 – 4.6)
Misuse of Existing Credit Card or Credit Card Number	1.4 % (1.0 % - 2.1%)	3.2 (2.1 – 4.6)
Total Victims in 2005	3.7 % (3.0% - 4.6%)	8.3 (6.6 – 10.3)

[1] Figures in parentheses are 95% confidence intervals.

[2] Based on U.S. population age 18 and over of 222.94 million as of July 1, 2005. (http://www.census.gov/popest/states/asrh/tables/SC-EST2005-01Res.xls (visited August 15, 2006)).

The Prevalence of ID Theft

- A total of 3.7 percent of survey participants indicated that they had discovered they were victims of ID theft in 2005. This result suggests that approximately 8.3 million U.S. adults discovered that they were victims of some form of ID theft in 2005.[3] (See Table 1.)

- In this report, victims of ID theft are classified as belonging to one of three categories based on the most serious problem the victim reported. Each of these categories represents a form of identity theft as it is defined by federal law. The survey confirmed prior data indicating that the magnitude of harm to consumers, as a general matter, correlates with the kind of ID theft suffered by the victim. In order of the magnitude of harm, from least to most, the three categories are: "Existing Credit Card Only," "Existing Non-Credit Card Account," and "New Accounts & Other Frauds."

- For the calendar year 2005:

  - 1.4 percent of survey participants, representing 3.2 million American adults, reported that the misuse of their information was limited to the misuse of one or more of their existing credit card accounts in 2005.[4] These victims were placed in the "Existing Credit Cards Only" category because they did not report any more serious form of identity theft.

  - 1.5 percent of participants, representing 3.3 million American adults, reported discovering in 2005 the misuse of one or more of their existing accounts other than credit cards—for example, checking or savings accounts or telephone accounts—but not experiencing the most serious form of identity theft. These victims were placed in the "Existing Non-Credit Card Accounts" category.

  - 0.8 percent of survey participants, representing 1.8 million American adults, reported that in 2005 they had discovered that their personal information had been misused to open new accounts or to engage in types of fraud other than the misuse of existing or new financial accounts in the victim's name. These victims were placed in the "New Accounts & Other Fraud" category, whether or not they also experienced another type of identity theft.

This consumer survey may not capture all types of identity theft or their associated costs. Situations in which someone creates a fictitious identity by combining personal information from one or more consumers with invented information, rather than using the identity of an existing individual, may not have been captured. This form of fraud, called synthetic ID theft, is not always detectable by the consumer(s) whose information was used.

[3] The difference between the 3.7% overall prevalence figure found in this survey and the 4.6% rate in the FTC's 2003 survey is not statistically significant using standard statistical analysis.

[4] Identity theft is defined both by statute (ID Theft Act, 18 U.S.C. § 1028(a)(7), 1029(e)) and by FTC rule (16 C.F.R. § 603.2), and includes the misuse or attempted misuse of any identifying information – such as the SSN, biometric data, or an existing credit card account number - to commit fraud.

Table 2: Costs of ID Theft, Misuse Discovered Since 2001

	New Accounts & Other Frauds	Existing Non-Credit Card Accounts	Existing Credit Cards Only	All ID Theft
Value of Goods and Services Obtained by Identity Thieves				
Median	$1,350	$457	$350	$500
90th Percentile	$15,000	$3,800	$4,000	$6,000
95th Percentile	$30,000	$6,000	$7,000	$13,000
Victims' Out-of-Pocket Expenses				
Median	$40	$0	$0	$0
90th Percentile	$3,000	$900	$132	$1,200
95th Percentile	$5,000	$1,200	$400	$2,000
Hours Victims Spent Resolving Their Problems				
Median	10	4	2	4
90th Percentile	100	44	25	55
95th Percentile	1,200	96	60	130
Sample size n =	138	164	257	559

- Table 2 presents various measures of the costs of ID theft. Rather than average values, the table uses median values (the point at which half the victims fell above the number and half below). A minority of ID thefts result in much greater harm than the typical case. Because these large values have a significant impact on the average value, the median better represents the typical experience. To capture the experiences of those who suffer the most serious harm, the table also reports values for the 90th percentile and 95th percentile of harms reported.

Financial Value Obtained by Thief

- The median value of goods and services obtained by the identity thieves for all categories of ID theft was $500. Ten percent of victims reported that the thief obtained $6,000 or more, while 5 percent reported that the thief obtained at least $13,000 in goods and services. (See Table 2.)

- Where the identity thieves opened new accounts or committed other frauds (the "New Accounts & Other Frauds" category), the median value of goods and services obtained by the thieves was $1,350. Ten percent of these victims reported that the thief obtained $15,000 or more in goods and services; in the top 5 percent, the thief obtained at least $30,000 in goods and services. Victims in the New Accounts & Other Frauds category were three times as likely to report that the thieves obtained more than $5,000 as victims in the other two categories of ID theft (23% vs. 7%).

- Where the ID theft was limited to the misuse of existing accounts – either credit card or non-credit card – the median value of goods and services obtained was less than $500. However, much higher amounts were obtained in some cases. Ten percent of victims in the "Existing Credit Card Only" category reported that the thief obtained $4,000 or more in goods and services. In the "Existing Non-Credit Card Accounts" category, the comparable figure was $3,800.

The Costs of ID Theft to Victims

- In more than 50 percent of ID thefts, victims incurred no out-of-pocket expenses. (Out-of-pocket expenses include any lost wages, legal fees, any payment of fraudulent debts, and miscellaneous expenses such as notarization, copying, and postage.) [5] In the New Accounts & Other Frauds category, the median value of out-of-pocket expenses was $40.

- However, some victims do incur substantial out-of-pocket expenses. Ten percent of all victims reported out-of-pocket expenses of $1,200 or more. For the New Accounts & Other Frauds category, the top 10 percent of the victims incurred expenses of at least $3,000, and the top 5 percent incurred expenses of at least $5,000. One-quarter of victims in the New Accounts & Other Frauds category reported paying out-of-pocket expenses of at least $1,000.

- Victims of all types of ID theft spent hours of their time resolving the various problems that result from ID theft. The median value for the number of hours spent resolving problems by all victims was 4. However, 10 percent of all victims spent at least 55 hours resolving their problems. The top 5 percent of victims spent at least 130 hours.

[5] In most cases, victims are not legally responsible for the cost of fraudulent transaction by identity thieves using their personal information. A variety of laws limit consumers' liability in these situations. Such laws include the Truth in Lending Act, 15 U.S.C. § 1601 et seq., implemented by Regulation Z, 12 C.F.R. § 226; see especially 15 U.S.C. § 1643; 12 C.F.R. § 226.12(b) (limits consumer liability for unauthorized credit card charges to a maximum of $50), and the Electronic Fund Transfer Act, 15 U.S.C. § 1693 et seq., implemented by Regulation E, 12 C.F.R. § 205; see especially 15 U.S.C. § 1693g; 12 C.F.R. § 205.6(b) (limits consumer liability for unauthorized electronic fund transfers depending upon the timing of consumer notice to the applicable financial institution). Consumer liability for losses associated with checking account fraud and loan fraud are typically limited by state statute or common law, although consumers are sometimes held liable.

- Victims in the New Accounts & Other Frauds category spent the greatest amount of time resolving problems. In the top 10 percent in this category, victims reported spending 100 hours or more resolving problems. The top 5 percent reported spending at least 1,200 hours.

- Almost one-quarter of all victims were able to resolve any problems experienced as a result of ID theft within one day of discovering that their personal information had been misused. This refers to the amount of time that passed from when they discovered the crime to when their problems where resolved, not to the number of hours spent resolving their problems.

- Thirty-seven percent of victims reported experiencing problems other than out-of-pocket expenses or the expenditure of time resolving issues as a result of having their personal information misused. The problems victims reported include, among other things, being harassed by collections agents, being denied new credit, being unable to use existing credit cards, being unable to obtain loans, having their utilities cut off, being subject to a criminal investigation or civil suit, being arrested, and having difficulties obtaining or accessing bank accounts.

- Victims of New Accounts & Other Frauds were more than twice as likely to report having one or more of these other types of problems (68%) than were victims in the Existing Non-Credit Card Accounts category (32%,) and four times as likely as victims in the Existing Credit Cards Only category (17%).

Comparison to the 2003 ID theft survey

The FTC conducted a similar telephone survey of consumers in 2003, the first national survey to measure the prevalence and cost of identity theft. Based on the knowledge gained from conducting and analyzing the 2003 survey, FTC staff changed certain elements of the survey methodology for the 2006 survey, to more accurately capture consumers' identity theft experiences. Because of these methodological changes, estimates of the losses from ID theft in the two surveys cannot be directly compared.

- **Prevalence.** The 2003 survey found that 4.6% of the survey population had experienced ID theft during the one year period before the survey was conducted. The 2006 survey found that 3.7% of the survey population had experienced ID theft during 2005. The difference between the rates is not statistically significant.[6] Given the sample sizes and the variances within the samples, one cannot conclude that the apparent difference between the two figures is the result of a real decrease in ID theft rather than a result of random variation.

- **Average amount obtained by the thief.** Both the 2003 and 2006 surveys asked victims for their best recollection of the amount of money obtained by the thief. In the 2006 survey, the average amount obtained by the thief was $1,882, whereas the average was $4,789 in the 2003 survey.

  Although these results appear to show a dramatic change in the amount obtained by the thief, some of this difference may be explained by several changes in the survey methodology. First, in the 2003 survey, the amounts reported by victims were only recorded as falling within a specified range – *e.g.,* between $100 and $499. In estimating the average amount obtained by thieves, each individual response was assumed to be equal to the mid-point of the specified range selected by that individual. For example, if the consumer chose the category "$100 - $499," the value used in the estimate was $300. In contrast the 2006 survey recorded the **actual** values reported by victims. This difference between using actual values versus the mid-point of a range of values could lead to differences in the results.[7]

  Second, the average value is highly influenced by a small number of "outlier" victims who claimed to have suffered exceptionally large losses. (See Table 2, above.) In estimating average and total amounts obtained by identity thieves, this report excludes the responses of two individuals whose extremely high estimates were suspect.[8] No such exclusions were made in the 2003 survey report.

---

[6] It should also be noted that, prior to asking whether they had experienced ID theft, the 2006 survey asked participants whether they had been notified that a company, government agency, or other organization had lost their personal information. Questions about breach notices were not included in the 2003 survey, and this change may affect participants' responses in unknown ways.

[7] To test this proposition, the 2006 "actual value" responses were put into the ranges used in 2003. For most of the ranges, the average of "actual value" responses was lower than the midpoint of the range.

[8] In one instance, a person who was interviewed claimed to be a victim of ID theft and reported that the thief had obtained goods or services worth $999,999. However, a closer reading of the entire interview record indicated that this person was describing the theft of intellectual property, rather than ID theft. In the second instance, the person reported that the value obtained by the thief was $485,000. While this person did appear to be describing ID theft, the record seemed

Third, the 2006 report adopted a new way to account for instances where more than one individual may have been victimized by a single theft of personal information because the misuse involved accounts that were jointly held by two people. In the 2003 report, the total amount obtained by the thief was attributed to each of the victims, whereas in the 2006 report, the total was divided amongst the victims (*e.g.,* attributing half of the loss to each of two joint victims).

Although we believe that these methodological changes improve the reliability of the estimated values, they tend to cause lower estimates as compared to the 2003 survey. Thus, the differences in the estimates between 2003 and 2006 may, at least in part, be due to the changes in methodology as opposed to changes in consumers' actual experiences. We cannot, therefore, be confident that the difference between the 2003 and 2006 estimates represents an actual drop in the average amount obtained by identity thieves.

- **Total amount obtained by thieves.**

  Similarly, the estimate of total losses from ID theft in the 2006 survey - $15.6 billion - is considerably lower than the estimate of $47.6 billion in the 2003 survey. This reflects lower estimates of both the prevalence of ID theft and the average loss per incident. As discussed above, however, some of these differences result from the changes in survey methodology. Thus, we cannot determine whether total losses have actually dropped significantly between 2003 and 2006.

- **Average consumer out-of-pocket expenses.**

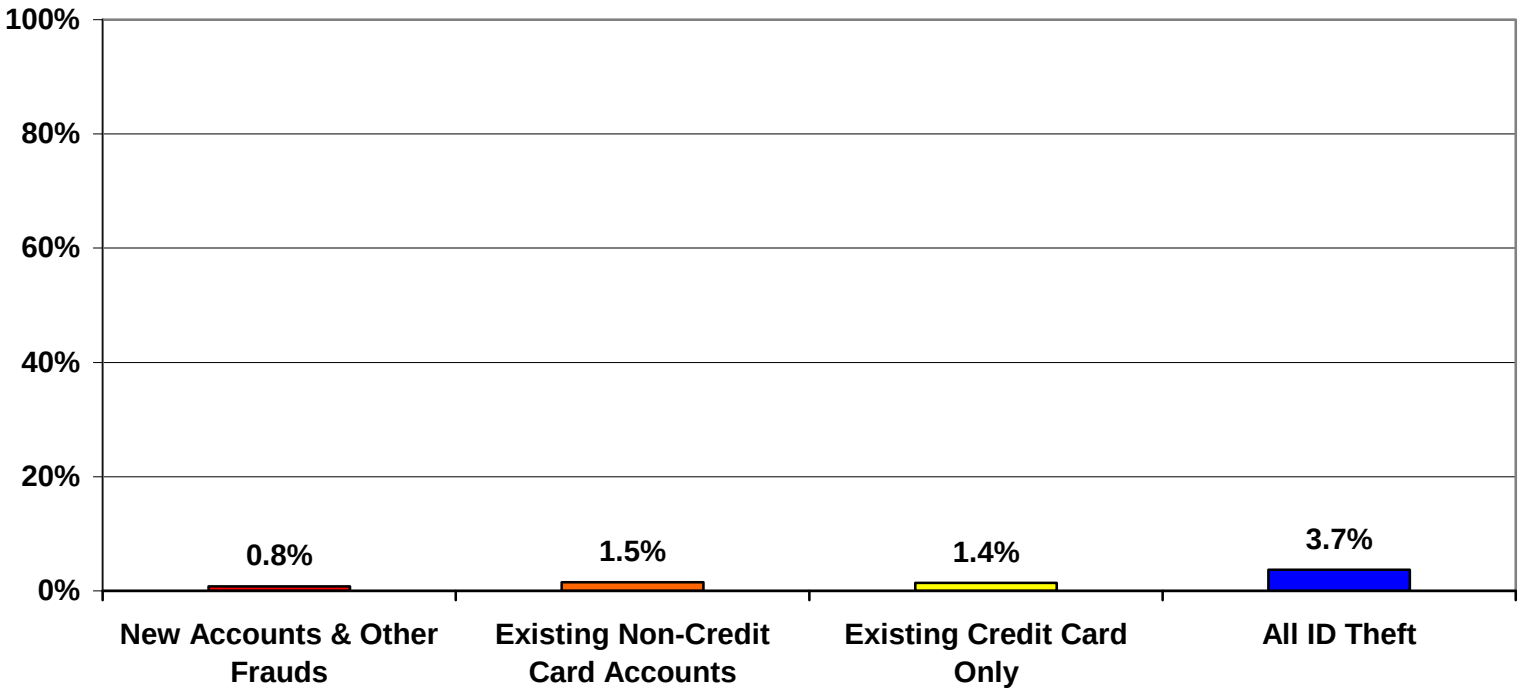
  The 2003 survey found that victims had, on average, out-of-pocket expenses of $500. In the 2006 survey, the average victim loss was $371. The same methodological differences that pertain to the amount the thief obtained also apply to these average loss estimates, that is, measuring loss as a range versus actual amount and how we accounted for joint victims.

---

inconsistent with the loss of this much money. If this value were to be included in the calculation, the estimated average loss per victim would be $3,370, and the estimated total loss would be $27.9 billion.

Prevalence of Identity Theft

Figure 1 - Q1 / Q7 / Q8 / Q9 / Q15 - Prevalence of Identity Theft in 2005[1]



- 3.7% of respondents (3.0% - 4.6%)[2] said they became aware of being a victim of ID theft during 2005. This suggests that 8.3 million American adults (6.6 million – 10.3 million) discovered they were ID theft victims in 2005.[3]

---

[1] In computing prevalence figures for 2005, individuals who reported that they had discovered that their personal information was being misused since the beginning of 2006 were eliminated from the sample. While these people discovered that their information was being misused in 2006, there is no way to know whether or not they had discovered a separate incident of ID theft in 2005.
See Appendix B for a discussion of the effect of consumers who declined to participate in or who began but did not complete the survey.

[2] Figures in parentheses are 95% confidence intervals. As with any survey, this study is subject to sampling error. While a survey of all adults in the U.S. might give results that differ somewhat from the figures reported here, there is a 95% probability that the figure would lie within the range of values represented by the figures in parentheses.

[3] In some cases, the misuse of an individual's personal information included the misuse of jointly held accounts. In these cases, the estimates of the prevalence of ID theft may include both account holders as victims. This seems appropriate since both individuals are likely to have been negatively impacted by the misuse. In other places in the report, the experiences of both victims are combined as a single victim response. In particular, when asked about the out-of-pocket expenses incurred and the time spent resolving problems, interviewees were asked to include the total amount of money or time expended by both themselves and the other individual included on the joint account.

In addition, because the data reported here are the results of a survey of consumers, the data may not capture situations in which someone creates a new identity, rather than using the identity of an existing individual, and uses that fictitious identity to obtain goods or services, i.e. synthetic identity fraud. Whether such instances of synthetic identity fraud will be captured in a consumer survey will depend on whether the actions have been attached to a real person – perhaps the individual whose Social Security number was used in creating the fictitious identity.

Categorizing ID Theft

- This report classifies ID theft victims in one of three categories: New Accounts and Other Frauds, Existing Non-Credit Card Accounts, and Existing Credit Cards Only. They are placed in the category that includes the most serious type of ID theft they reported. ID theft is considered more serious if it causes the victim more harm, measured by factors such as the amount of time it takes to recover, the out-of-pocket expenses incurred, and the additional problems they experience.

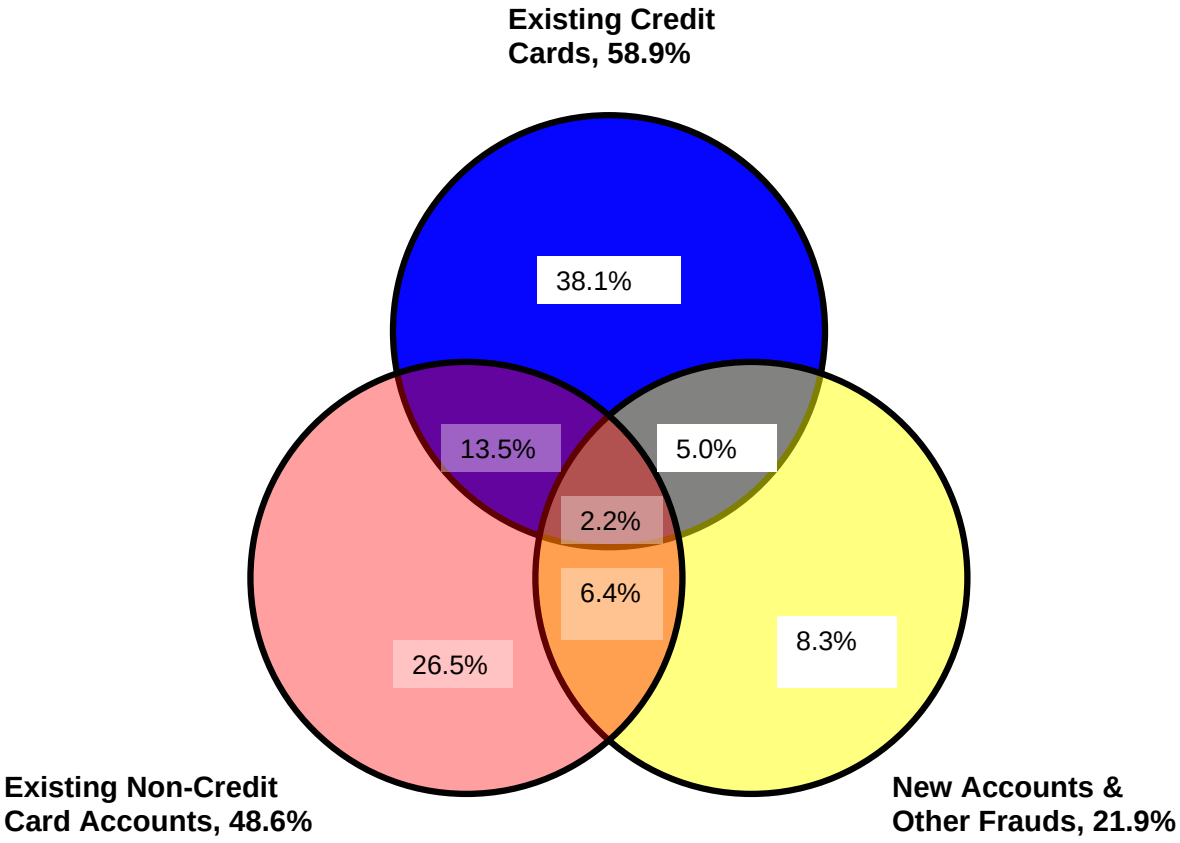
- The "New Accounts & Other Frauds" category is considered to be the most serious, followed by the "Existing Non-Credit Card Accounts" category. "Existing Credit Cards Only" is considered the least serious type of victimization. Placing victims in only one category means that, for example, victims who reported that a new account had been opened using their information and also that one of their existing non-credit card accounts had been misused are placed in the "New Accounts & Other Frauds" category, not in the "Existing Non-Credit Card Accounts" category.

- 1.4% of respondents (1.0% - 2.1%) fall into the category labeled "Existing Credit Cards Only." This category includes victims who reported the misuse of only their existing credit cards and no other misuse of their personal information.

- 1.5% of respondents (1.1% - 2.1%) fall into the category of ID theft that includes the misuse of existing accounts other than a credit card, "Existing Non-Credit Card Accounts."

- 0.8% of respondents (0.5% - 1.2%) fall into the category labeled "New Accounts & Other Frauds." This category includes victims whose personal information had been used to open new accounts (for example, new credit card or bank accounts, telephone or wireless service, or loans) or commit other frauds (for example, the thief giving the victim's name and identifying information when charged with a crime, renting an apartment or a house, or obtaining medical care).

Figure 2 - Display of 2005 ID Theft Victim Overlap Among Categories

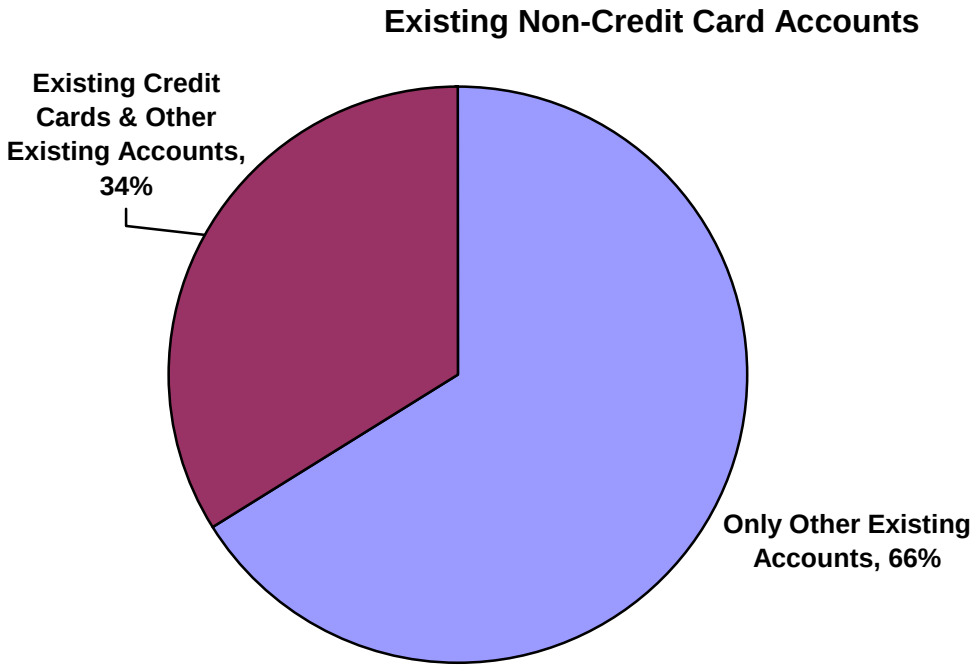


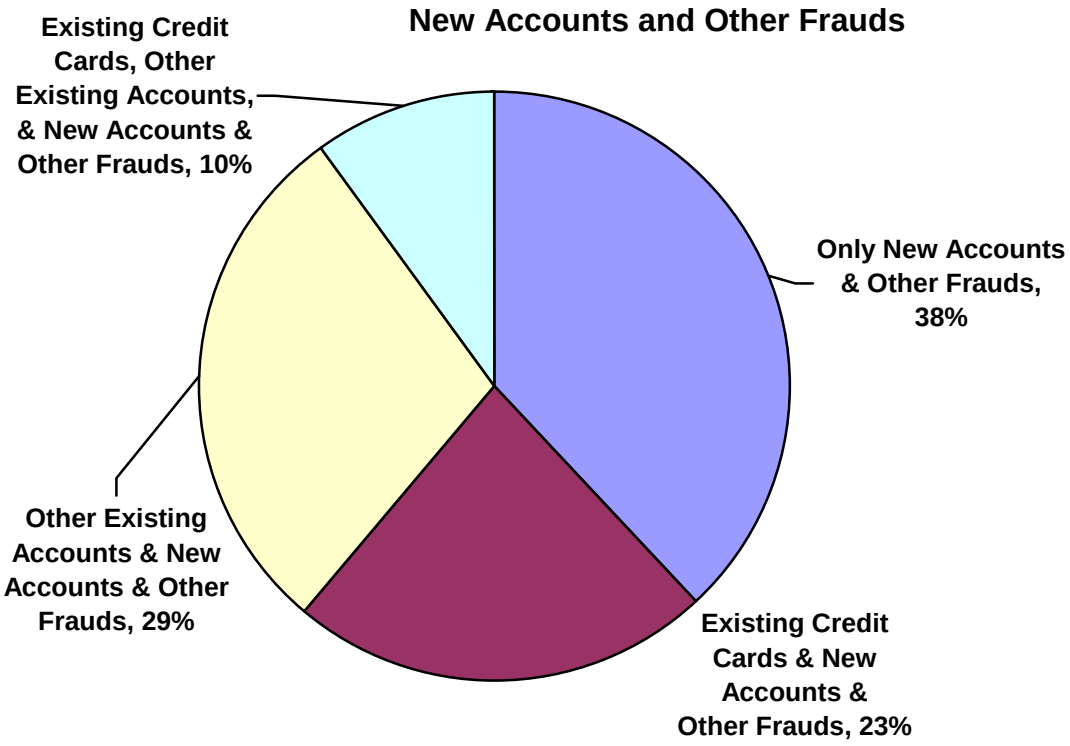
- For most purposes, this report groups victims according to the most serious form of ID theft that they suffered. However, many victims suffer multiple types of ID theft, and this diagram illustrates the overlap in types.
- 58.9% of all victims experienced the misuse of an existing credit card.
- A total of 48.6% of victims experienced the misuse of existing accounts other than existing credit card accounts.
- 21.9% of victims had their personal information used to open a new account or commit some other kind of fraud.
- For 38.1% of all victims (1.4% of all respondents), the misuse of an existing credit card was the only form of ID theft suffered.
    - Approximately one-third of victims who experienced the misuse of an existing credit card also experienced another type of ID theft. Therefore, these victims are counted in one of the other two, more serious, categories of ID theft.

- Victims who experienced the misuse of existing accounts other than credit card accounts are included in the Existing Non-Credit Card Accounts category (1.5% of all respondents), unless new accounts were opened or other frauds were committed using their information.
    - 13.5% of victims experienced both the misuse of existing non-credit accounts and the misuse of existing credit accounts, but not new accounts or other frauds.

- All victims whose personal information was used to open new accounts or commit other frauds are included in the New Accounts & Other Frauds category. That is, all of the 21.9% of victims in the yellow circle of the diagram (0.8% of all adult Americans) are included in this category. This category includes:
    - 6.4% of victims who, in addition to new accounts or other frauds, had existing non-credit card accounts, but not existing credit card accounts, misused.
    - 5.0% of victims who, in addition to new accounts or other frauds, had existing credit card accounts, but not existing non-credit card accounts, misused.
    - 2.2% of victims who had both existing credit and non-credit card accounts misused, in addition to new accounts and other frauds.

Figure 3 - Display of Breakout of 2005 ID Theft Victims within Categories



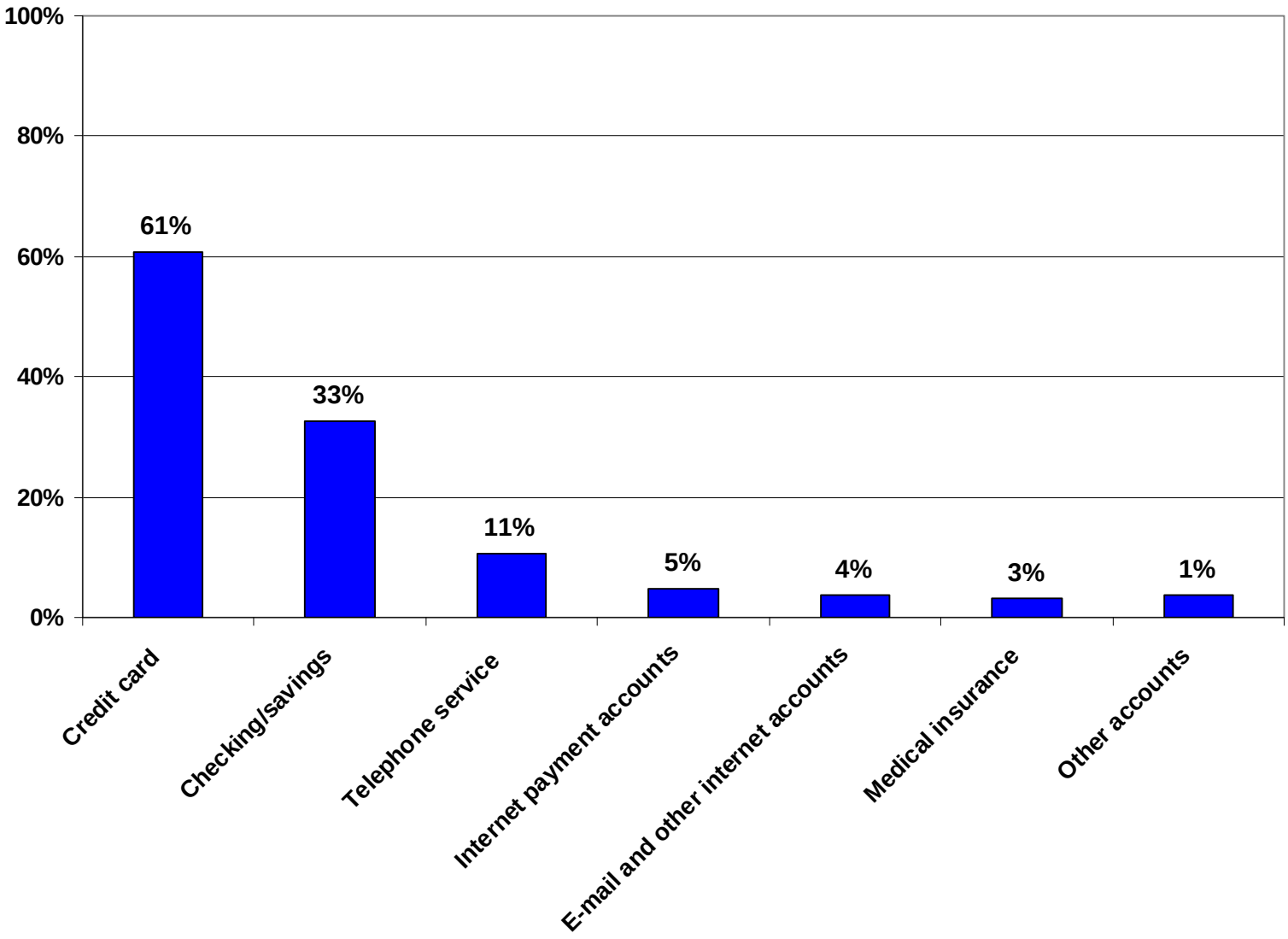


- As mentioned above, each victim is classified as belonging to only one of the categories of ID Theft, based on the most serious problem the victim reported. Some victims in the two more serious categories have had their information misused in ways that relate to more than one category.

- Approximately 34% of victims in the “Existing Non-Credit Card Accounts” category also experienced the misuse of an existing credit card account.

- Similarly, 62% of those who discovered that they had experienced “New Accounts & Other Frauds” ID Theft in 2005 also experienced the misuse of an existing credit card or other account: 23% experienced the misuse of an existing credit card, 29% experienced the misuse of an existing non-credit card account, and 10% experienced both the misuse of existing credit cards and the misuse of existing non-credit card accounts.

Figure 4 – Q1 / Q29 - Existing Accounts Misused[4]



The figures on this and the succeeding pages are based on the responses of all survey participants who reported discovering the misuse of their personal information between the beginning of 2001 and when they were interviewed—a total of 559 individuals. The data in Figures 1-3 are based only on those who discovered the misuse of their information in 2005.

- Eighty-five percent of all ID theft victims reported that one or more of their existing accounts had been misused.[5] This figure includes both credit card and non-credit card accounts.

[4] The figures on this and the succeeding pages are based on the responses of all survey participants who reported discovering the misuse of their personal information between the beginning of 2001 and when they were interviewed—a total of 559 individuals. The data in Figures 1-3 are based only on those who discovered the misuse of their information in 2005.

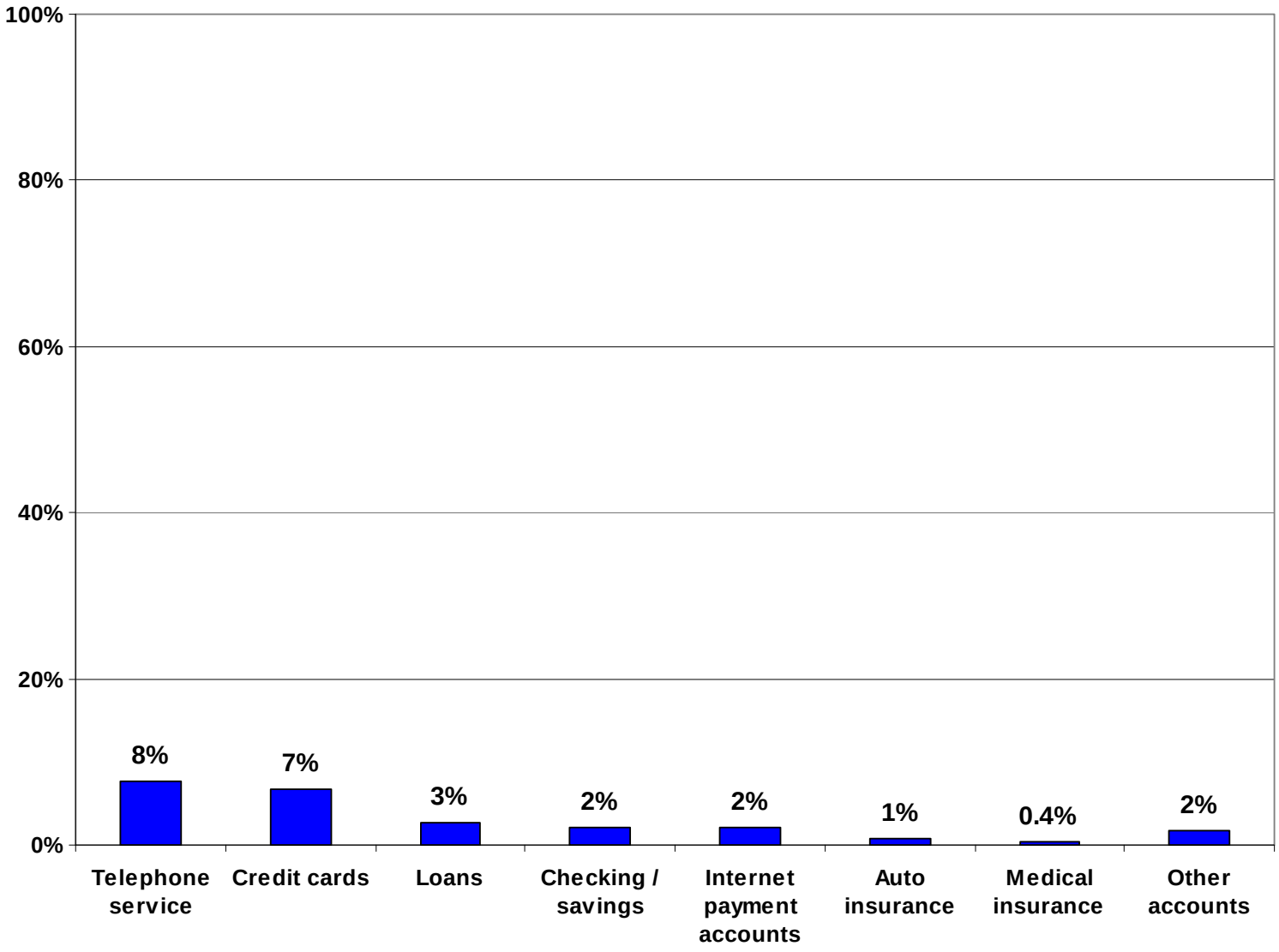
[5] Victims were asked what types of existing accounts were misused by the thief. The percentages for each category of misuse reflect each discrete misuse reported by the victim. Unlike in Figure 1, victims can be counted in more than one response category in this graph.

- Sometimes identity thieves take additional steps to facilitate their unauthorized use of the victim's existing accounts. They may change the billing or mailing address in order to conceal their unauthorized use, or add their names as authorized users to obtain a card in their name from the card issuer. These types of actions are known as "account takeover."

    - Account takeover was reported by 9% of victims who experienced existing credit card misuse and 11% of victims who experienced existing non-credit card account misuse.[6] Because new account fraud involves the creation of an entirely new account rather than the misuse of an existing one, account takeover does not apply to that type of identity theft.

[6] The data on takeovers of existing credit card accounts is based on the responses to question 5a of 379 individuals who indicated that their existing credit card accounts had been misused between 2001 and the time they were interviewed. The data on takeovers of existing non-credit card accounts are based on the responses to question 5b of 217 individuals who indicated that one or more of their existing non-credit card accounts had been misused.

Figure 5 - Q32 / Q33 – New Accounts Opened By Identity Thieves[7]



- Seventeen percent of all ID theft victims said the thief used their personal information to open at least one new account.[8]
- The two most common type of accounts victims reported thieves opening were telephone service accounts (including both landline and wireless phone accounts) and credit card accounts (8% and 7% of all victims, respectively).

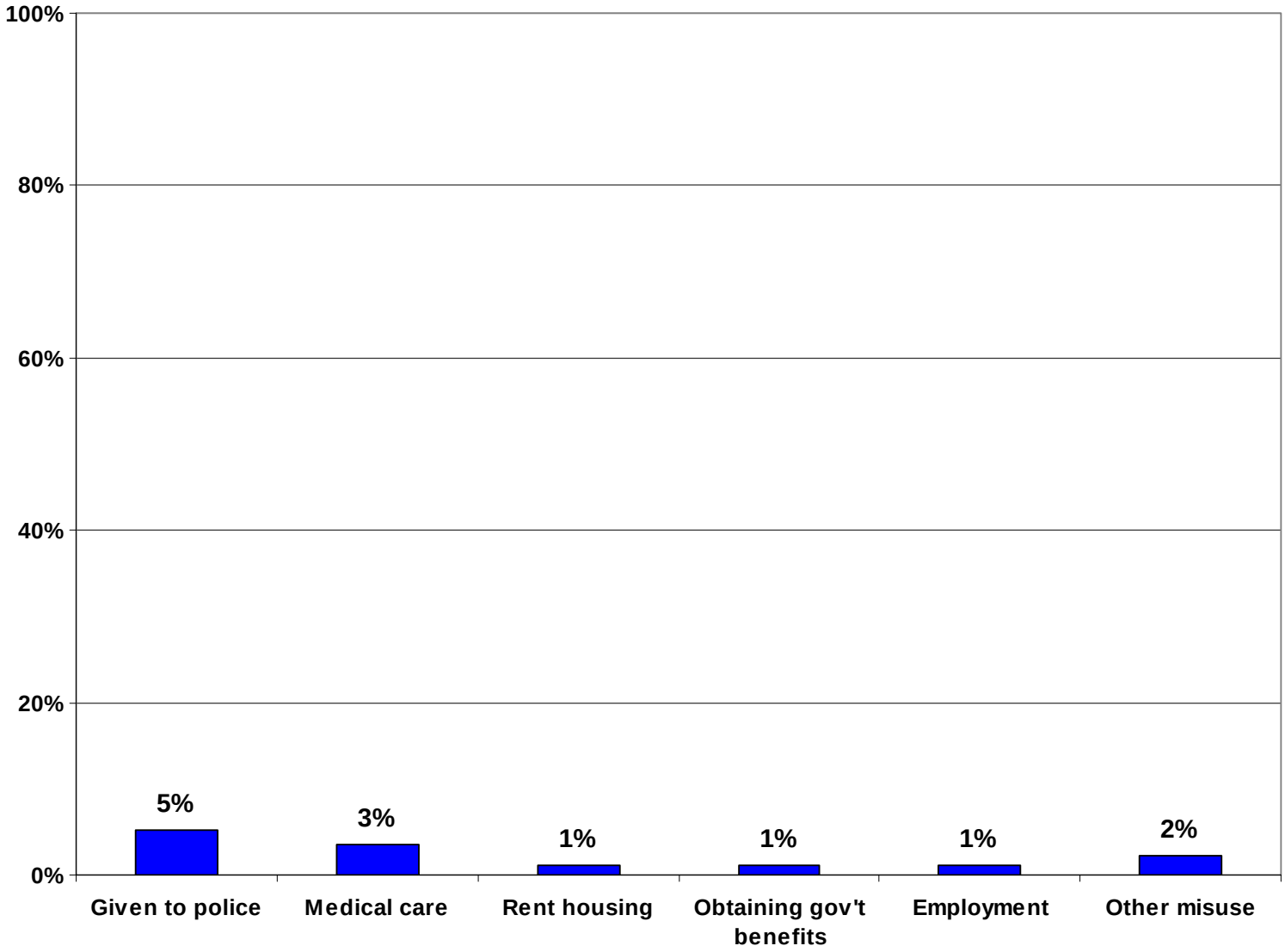
[7] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed.

[8] Victims were asked what types of accounts were opened. This graph shows several specific types of accounts they mentioned. The percentages reflect each time a victim mentioned that type, and, unlike in Figure 1, a victim can be counted more than once.

- Just over half of victims who reported that new accounts were opened said that a single new account was opened.[9]
- One-quarter of victims who had new accounts opened reported that 3 or more accounts were opened.

[9] These figures are based on the responses of 94 individuals who indicated that new accounts had been opened using their personal information.

Figure 6 - Q34 – Other Misuses of Personal Information[10]

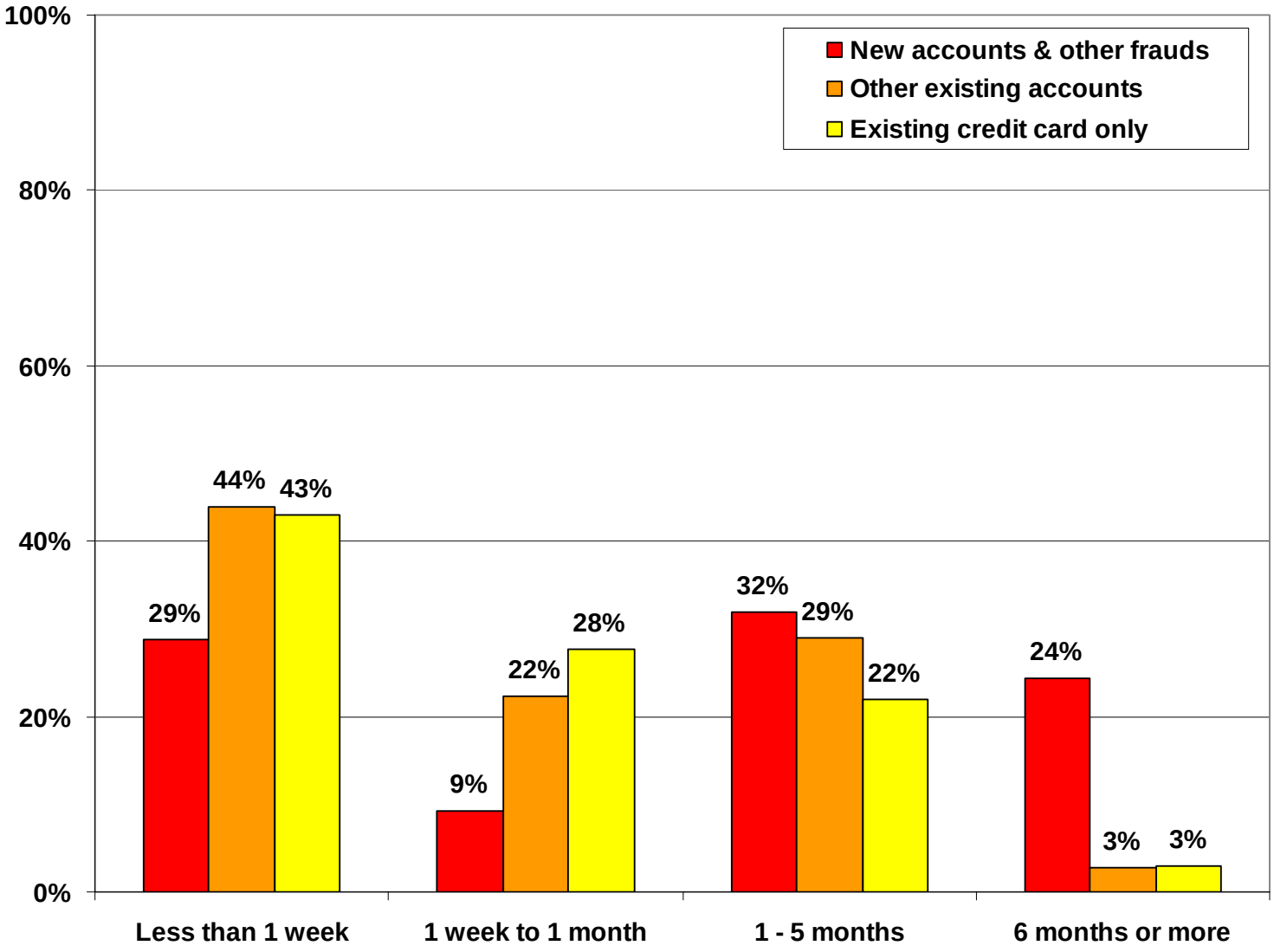


- Twelve percent of victims reported one or more misuse other than accessing new or existing financial accounts in the victim's name, and specified what type(s) of fraudulent activities were committed. The most common forms of non-account misuse were:
    - Five percent of victims said that they were aware that their name and/or personal information were given to the police when the thief was stopped or charged with a crime.
    - Three percent of victims said the thief had obtained medical treatment, services, or supplies using their personal information.

[10] Based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed.

Time Considerations

Figure 7 - Q16 – Length of Time to Discover Misuse[11]



- Nearly 40% of all ID theft victims discovered the misuse of their information within one week of the start of the misuse.
- However, the discovery period was significantly different depending on the type of fraud experienced:
    - Victims in the Existing Credit Cards Only (22%) and the Existing Non-Credit Card Accounts (21%) categories were about twice as likely as those in the New Accounts & Other Frauds (10%) category to find out about the misuse the day it started.

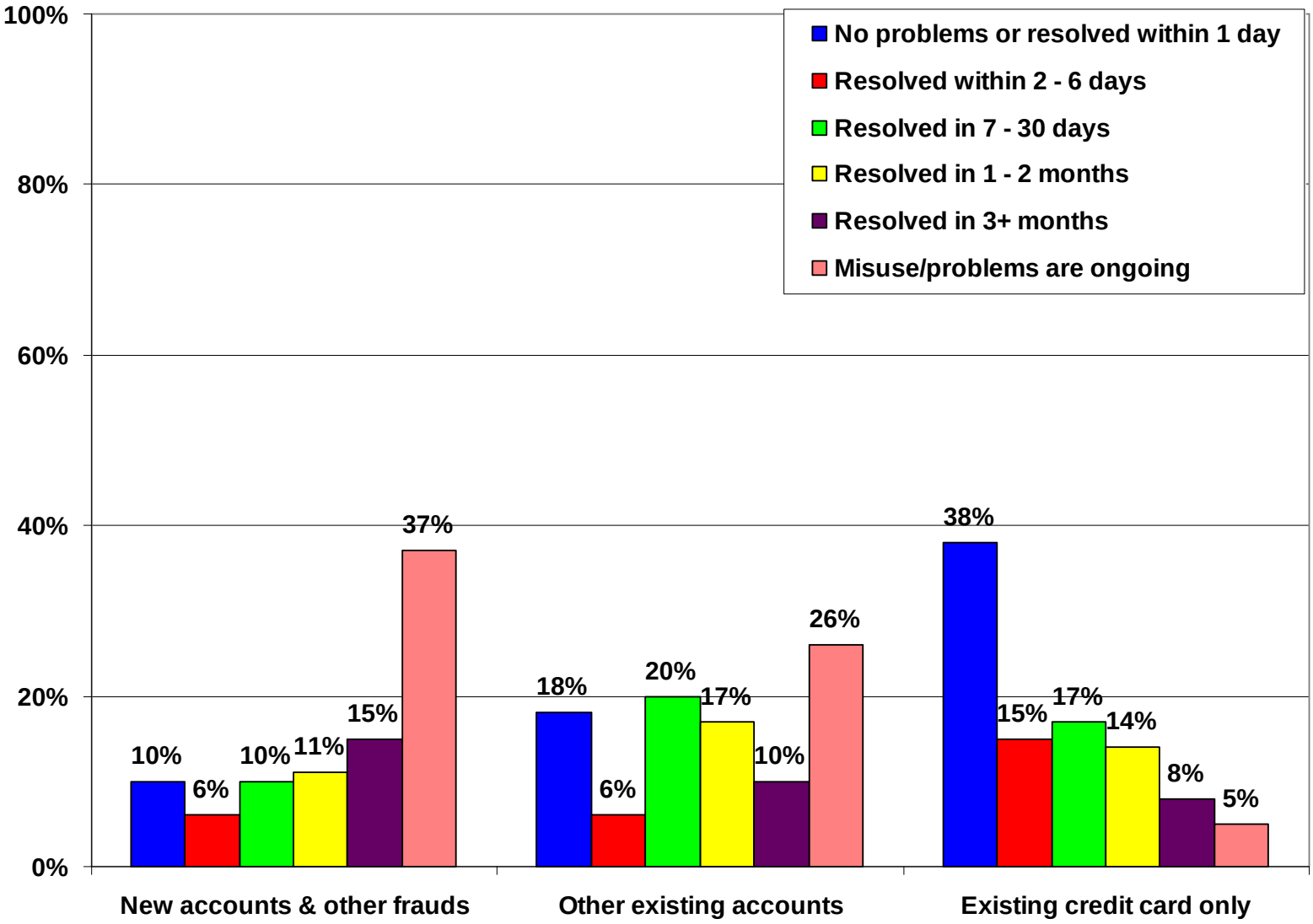
[11] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed. Figures for Existing Credit Cards Only, Existing Non-Credit Card Accounts, and New Accounts & Other Frauds are based on the responses of the 257, 164, and 138 individuals, respectively, who indicated that they had experienced these types of ID theft during this period of time.

  - Nearly one-quarter (24%) of New Accounts & Other Frauds victims did not find out about the misuse of their information until at least 6 months after it started – compared to just 3% of Existing Credit Cards Only and Existing Non-Credit Card Accounts victims.
  - In the Existing Credit Cards Only and Existing Non-Credit Card Accounts categories, the median amount of time that elapsed before victims discovered that their personal information was being misused was between 1 week and 1 month. For the New Accounts & Other Frauds category, the median value was between 1 and 2 months.

- Where discovery of the misuse occurred more quickly, victims reported lower out-of-pocket losses and thieves obtained less:[12]
  - Thirty percent of those who discovered that their personal information was being misused 6 months or more after it started had to spend $1,000 or more, compared to 10% of those who found the misuse within 6 months.
  - Sixty-nine percent of those who discovered the misuse within 6 months spent fewer than 10 hours compared to 32% of those who took 6 months or more to discover it.
  - Thirty-one percent of those who discovered the misuse of their information 6 months or more after it started reported that the thief obtained $5,000 or more, compared to 10% of those who found out in less than 6 months.

[12] Figures for those who discovered the misuse less than 6 months after it began are based on 485 observations; figures for those who discovered the misuse 6 or more months after the misuse began are based on 50 observations.

Figure 8 - Q17 / Q19 / Q20 – Problem Resolution[13]



- Almost one-quarter of all victims (23%) said that either they had no problems or they were able to resolve any problems experienced as a result of being a victim of ID theft within one day of discovering that their personal information was being misused.
    - While 38% of victims in the Existing Credit Cards Only category either had no problems or were able to resolve any problems within one day, only 10% of victims in the New Accounts & Other Frauds category were able to do so.
- Eleven percent of all victims said that it had taken 3 or more months to resolve their problems after they discovered that their information was being misused.

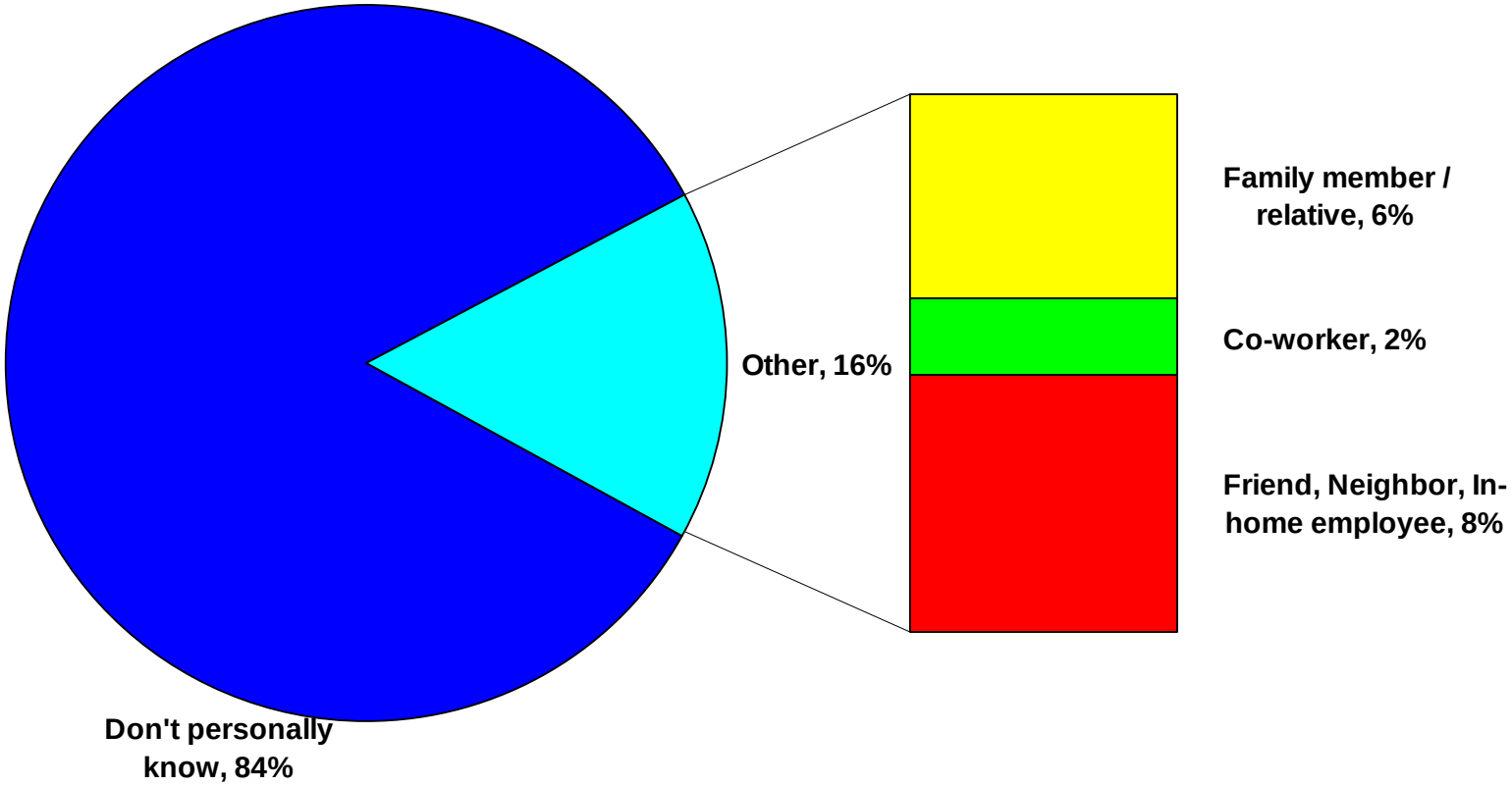
[13] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed. Figures for Existing Credit Cards Only, Existing Non-Credit Card Accounts, and New Accounts & Other Frauds are based on the responses of the 257, 164, and 138 individuals, respectively, who indicated that they had experienced these types of ID theft during this period of time.

  - While 15% of victims in the New Accounts & Other Frauds category took 3 months or longer to resolve the problems, only 8% of victims in the Existing Credit Cards Only category took this long to resolve problems.

- Twenty-one percent of all victims indicated that they were either continuing to experience problems related to the misuse of their information or that the misuse was continuing.
  - This was the case for 37% of those who had experienced New Accounts & Other Frauds ID theft, as compared to only 5% of victims in the Existing Credit Card Only category.

Offenders' Means of Access

Figure 9 - Q23 – Personal Relationship with Thief[14]



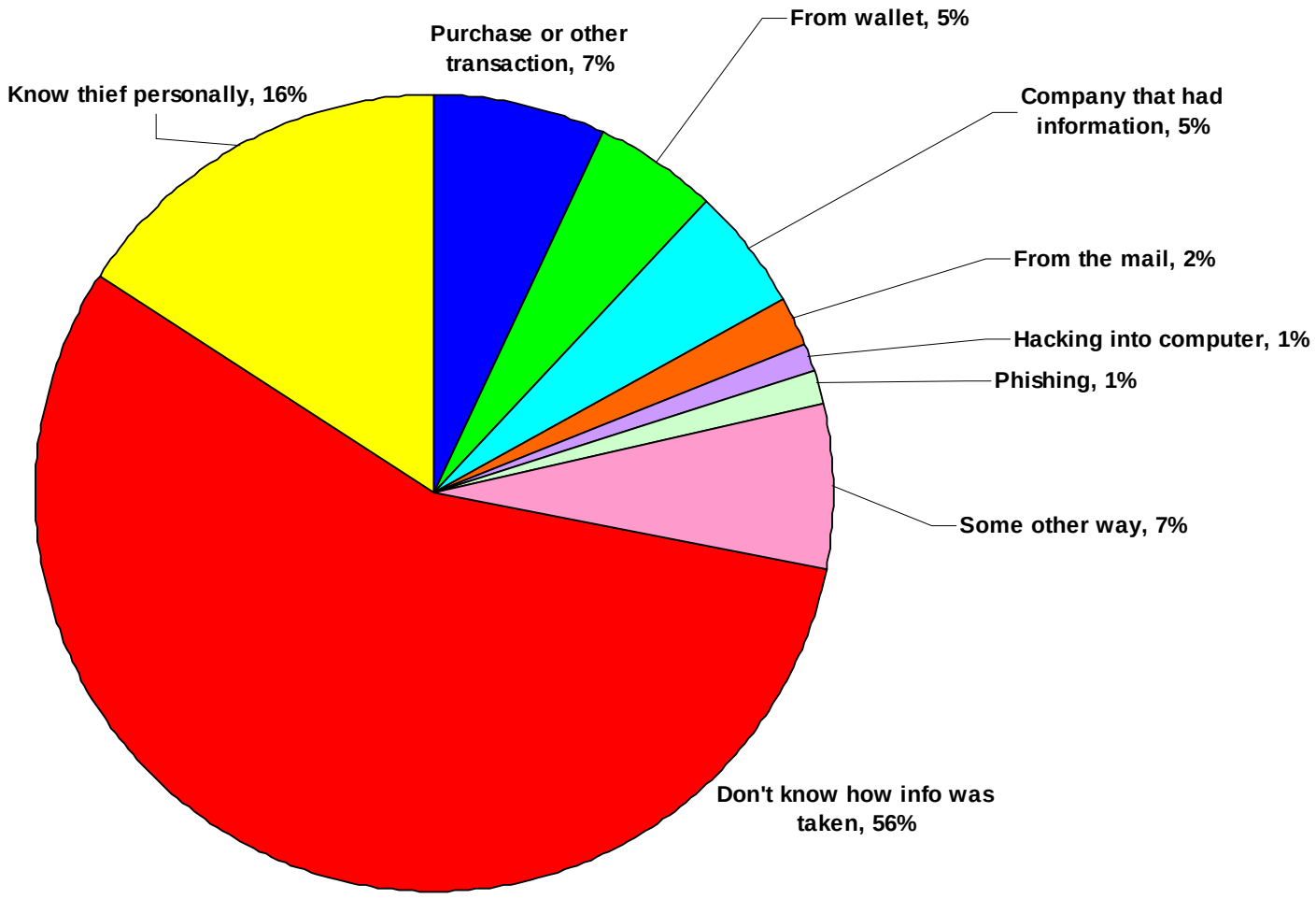
- ID theft victims generally are either unaware of the identity of the thief or do not personally know the thief. Over three-quarters of all ID theft victims (84%) reported that he or she did not personally know the thief, regardless of whether they had information about the thief's identity.
- Sixteen percent of all victims said that they personally knew the thief:
  - Six percent of victims knew that a family member or relative was the thief.
  - Eight percent of victims knew that a friend, neighbor, or in-home employee was the thief.
  - Two percent of victims reported that someone known to the victim from the workplace was the thief.

[14] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed.

- Victims in the New Accounts & Other Frauds (24%) and the Existing Non-Credit Card Account (21%) categories were nearly 5 times as likely to know the thief personally as victims in the Existing Credit Card Only category (5%).[15]

[15] Figures for Existing Credit Cards Only, Existing Non-Credit Card Accounts, and New Accounts & Other Frauds are based on the responses of the 257, 164, and 138 individuals, respectively, who indicated that they had experienced these types of ID theft between 2001 and the date they were interviewed.

Figure 10 - Q23 / Q25 / Q26 / Q27 – How Information Was Obtained[16]



- The majority of victims (56%) did not know how their information was stolen. Forty-three percent of victims were aware of who took their information or how it was taken.[17]
- Among those who knew how their information was taken, the most common factor was that their information was stolen by someone they personally knew. Sixteen percent of all victims indicated that their information was taken by someone they personally knew.

[16] Based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed.

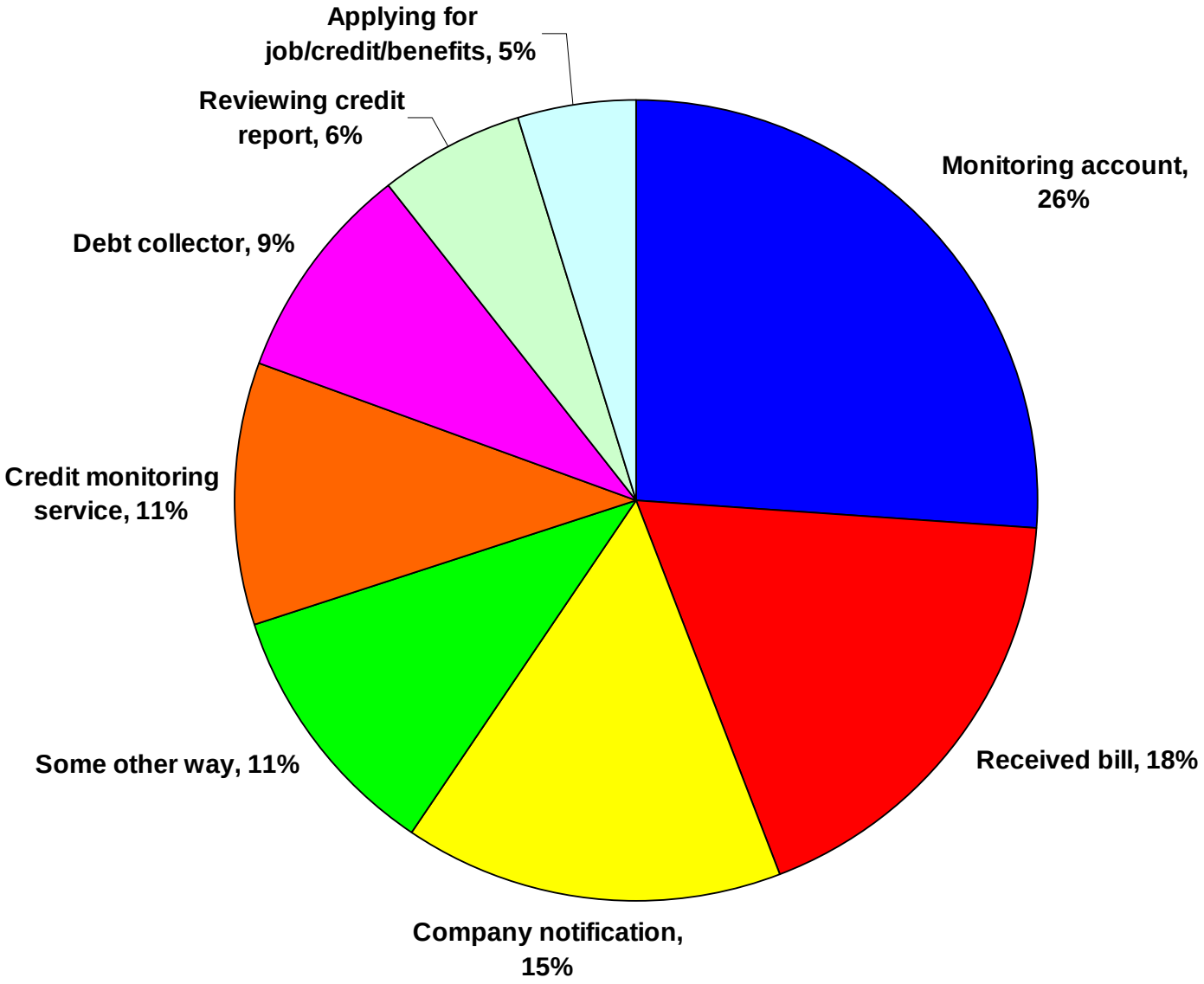
[17] The remaining 1% of respondents either refused to answer or stated that they did not know whether they knew how their information was obtained.

- Seven percent of all victims reported that their personal information was stolen during a purchase or financial transaction, including transactions conducted in a store, online, and through the mail.

- Five percent of all victims cited theft of a wallet or purse, and another 5% cited theft from a company that maintained their information.

Toll of Victimization

Figure 11 - Q21 / Q21a – How Victims Discovered ID Theft[18]



- The most common way victims discovered the misuse of their personal information was by monitoring the activity in their accounts (37% of all victims).
    - This includes victims using electronic means (12%), paper statements (6%), and those who could not recall whether they first found out electronically or by looking at a paper statement (8%). It also includes victims who used a credit monitoring service to detect unusual activity in their accounts (11%).

- How a victim was most likely to discover the misuse of their information depended on the category of ID theft suffered by the victim.

[18] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed.

- When the misuse was limited to Existing Credit Cards Only, victims most commonly discovered their information was being misused when they received a bill with fraudulent charges (25%), by monitoring their accounts (24%), or when they were notified of unusual account activity by the company affected (23%).[19]

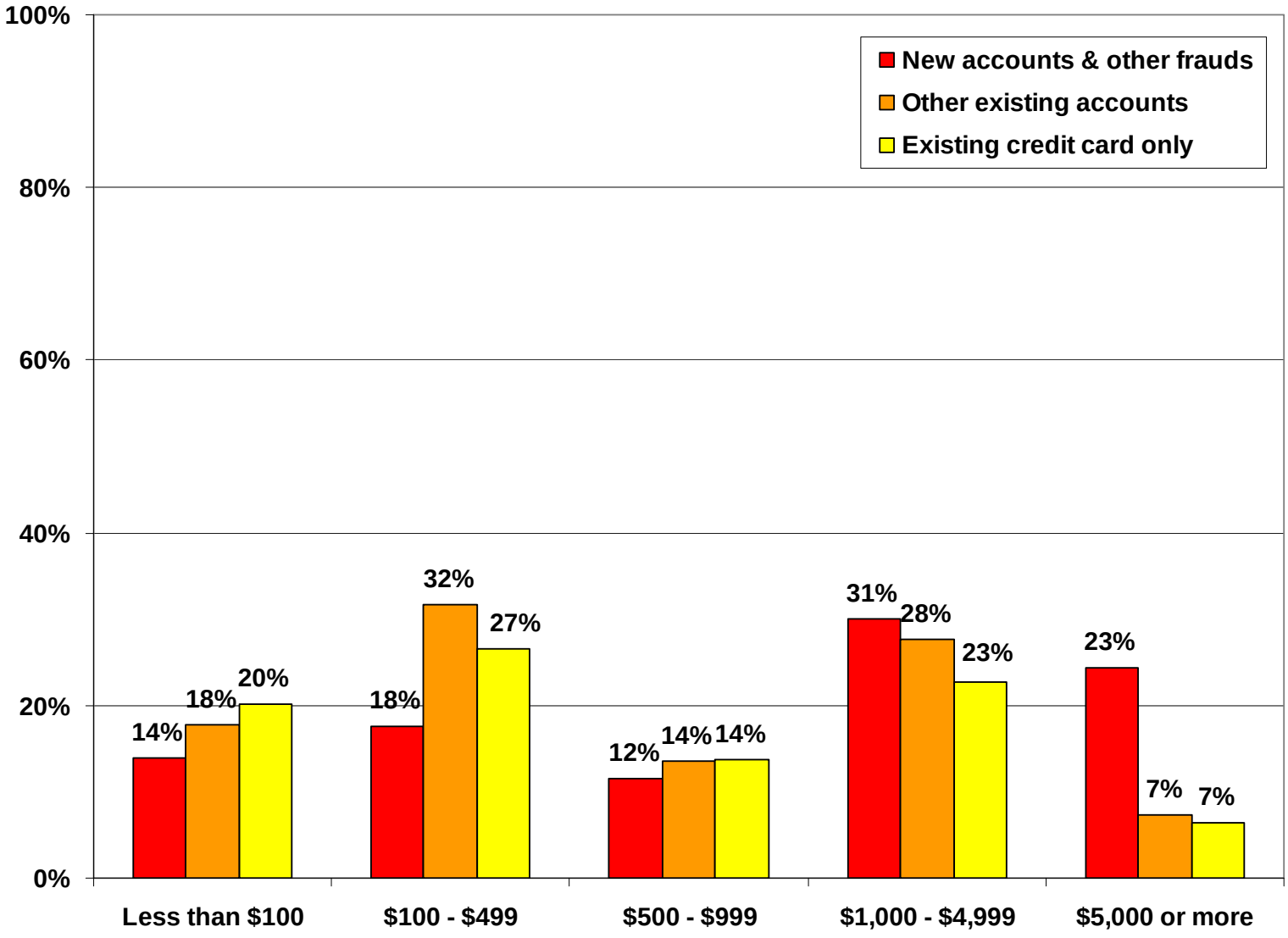
- In the Existing Non-Credit Card Accounts category, 41% of victims said that they discovered the misuse by monitoring their accounts.

- For New Accounts & Other Frauds victims, the most commonly mentioned means of discovery was being contacted by a debt collector (23%).

- Account monitoring was significantly more likely to be the way the fraud was detected for victims in the Existing Non-Credit Card Accounts (41%) and the Existing Credit Cards Only (24%) categories than for those in the New Accounts & Other Frauds category (11%).

[19] Figures for Existing Credit Cards Only, Existing Non-Credit Card Accounts, and New Accounts & Other Frauds are based on the responses of the 257, 164, and 138 individuals, respectively, who indicated that they had experienced these types of ID theft.

Figure 12 - Q36 / Q39 / Q40 – Value Thief Obtained[20]



- Victims were asked to estimate the value of the goods and services that the thief obtained from businesses, including financial institutions, using the victim's personal information. These figures include amounts where the business assumed the loss and amounts where the victim actually paid the debt created by the thief.
- The median value obtained by thieves was $500.
- The median values of goods and services obtained by the thief varied with the category of the identity theft.

[20] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed. Figures for Existing Credit Cards Only, Existing Non-Credit Card Accounts, and New Accounts & Other Frauds are based on the responses of the 257, 164, and 138 individuals, respectively, who indicated that they had experienced these types of ID theft during this period of time.

  - The median value obtained by thieves in the New Accounts & Other Frauds category was $1,350.

  - The median value in the Existing Non-Credit Card Accounts category was $457.

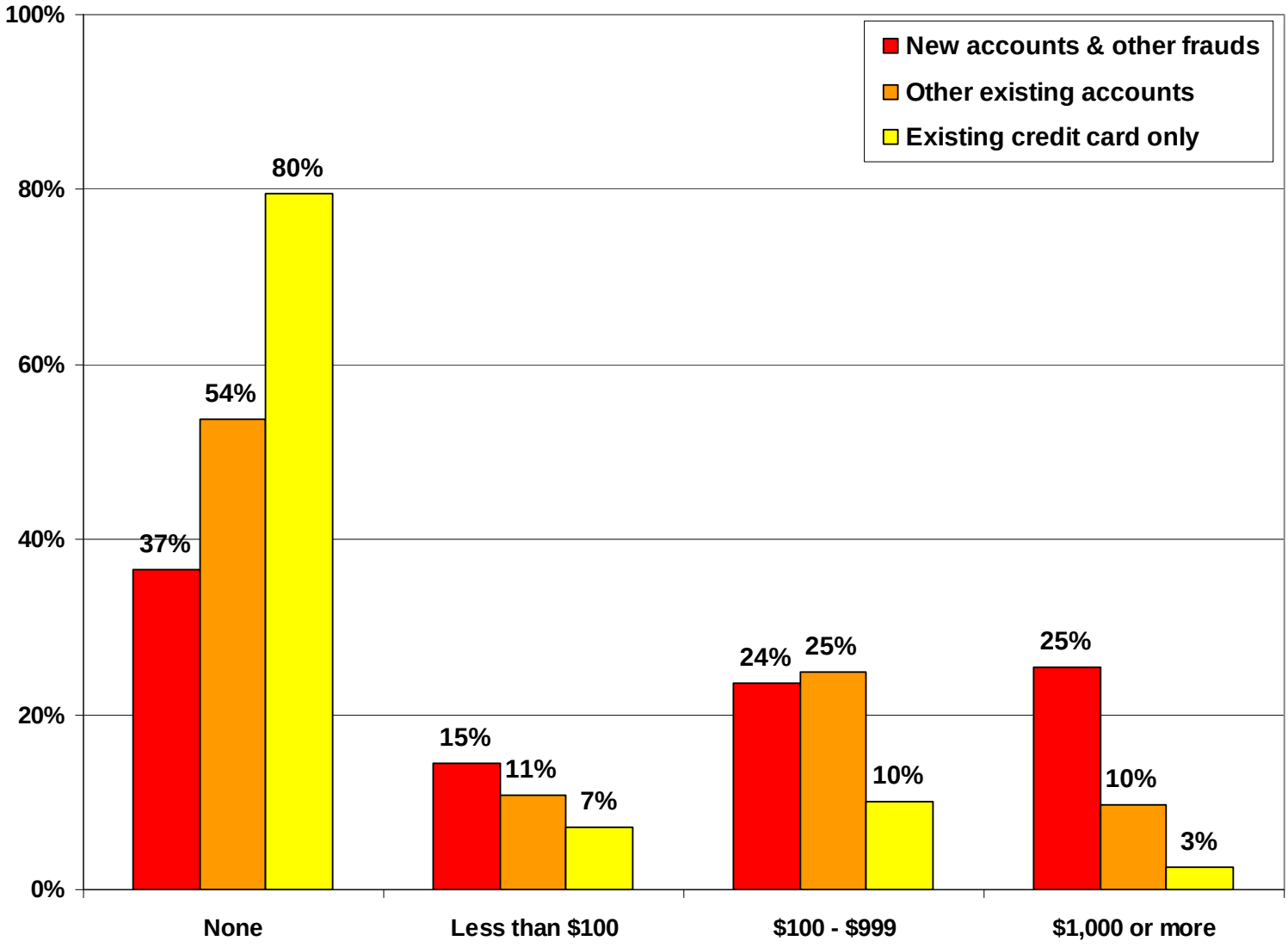
  - The median value in the Existing Credit Cards Only category was $350.

- Eighteen percent of victims reported that the thieves obtained goods or services worth less than $100.

- Twelve percent of victims reported that the thieves obtained goods or services valued at $5,000 or more.

  - Victims in the New Accounts & Other Frauds category were three times as likely to report that the thieves obtained more than $5,000 as victims in the other two categories of ID theft (23% vs. 7%).

Figure 13 - Q41 / Q44 / Q45 – Out-of-Pocket Payments by Victims[21]



- Survey participants were asked about their total out-of-pocket expenses, which include lost wages, legal fees, and payments of any fraudulent debts, as well as miscellaneous expenses such as postage and notarization fees.
- The majority of victims (59%) incurred no out-of-pocket expenses.

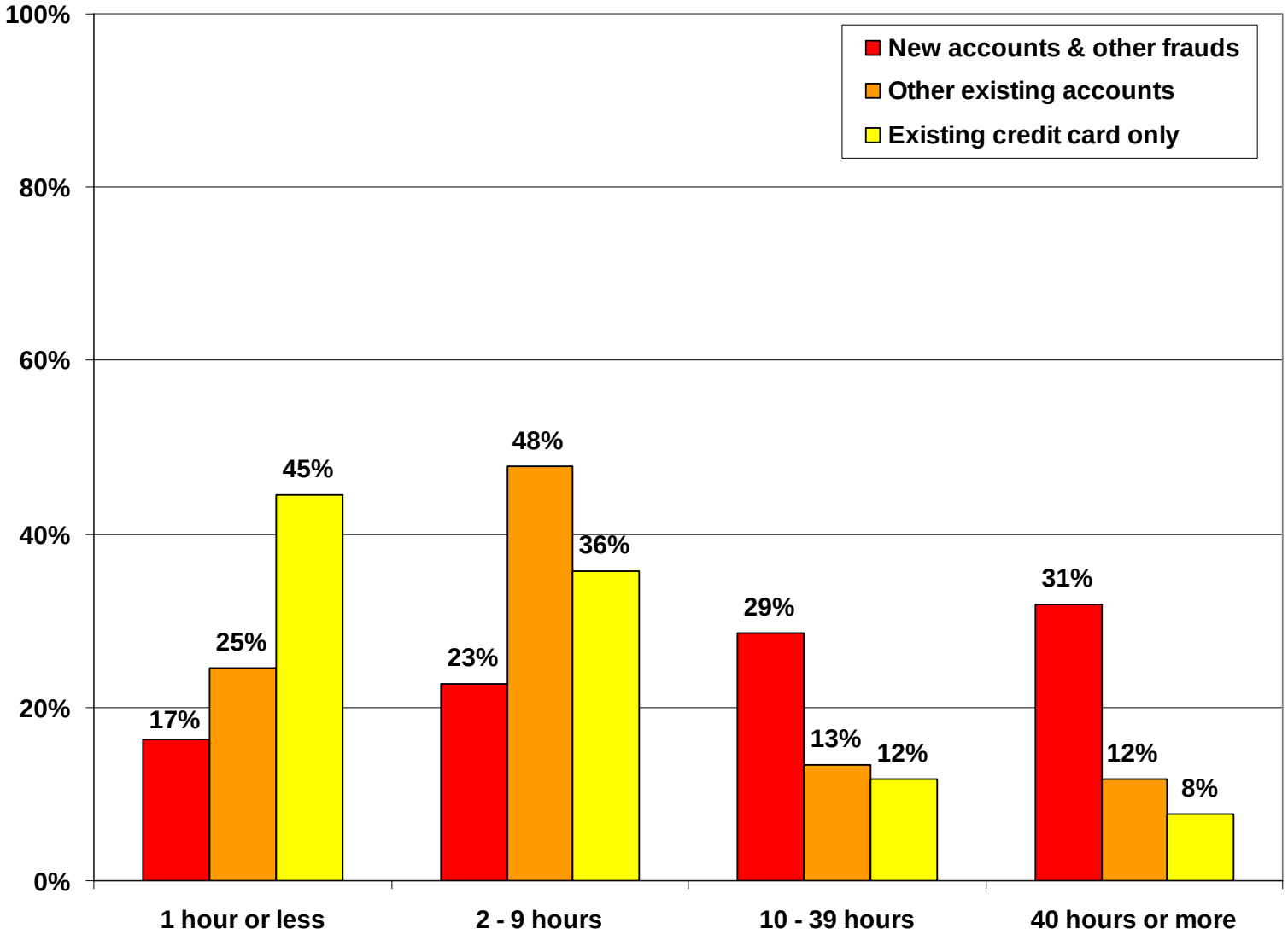
[21] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed. Figures for Existing Credit Cards Only, Existing Non-Credit Card Accounts, and New Accounts & Other Frauds are based on the responses of the 257, 164, and 138 individuals, respectively, who indicated that they had experienced these types of ID theft during this period of time.

- More than three-quarters (80%) of victims in the Existing Credit Cards Only category paid no out-of-pocket expenses, compared to 37% for victims in the New Accounts & Other Frauds category and 54% for the Existing Non-Credit Card Accounts category.
- One-quarter of victims in the New Accounts & Other Frauds category reported paying out-of-pocket expenses of at least $1,000. They are two and one-half times as likely as Existing Non-Credit Card Accounts victims (10%) and eight times as likely as Existing Credit Cards Only victims (3%), to pay this amount.

- Thirty percent of victims who had no out-of-pocket expenses nonetheless reported other types of costs in resolving their ID theft incident.[22]
    - o Nineteen percent said that they spent 10 or more hours resolving problems related to ID theft.
    - o Nineteen percent said that they experienced one or more of the other types of problems included in Figure 15.
    - o Eight percent reported both that they spent more than 10 hours resolving problems and they experienced one or more of the other problems.

[22] Figures for those who incurred no out-of-pocket expenses are based on the responses of 359 individuals.

Figure 14 - Q48 / Q51 / Q52 – Time Spent Resolving Problems[23]

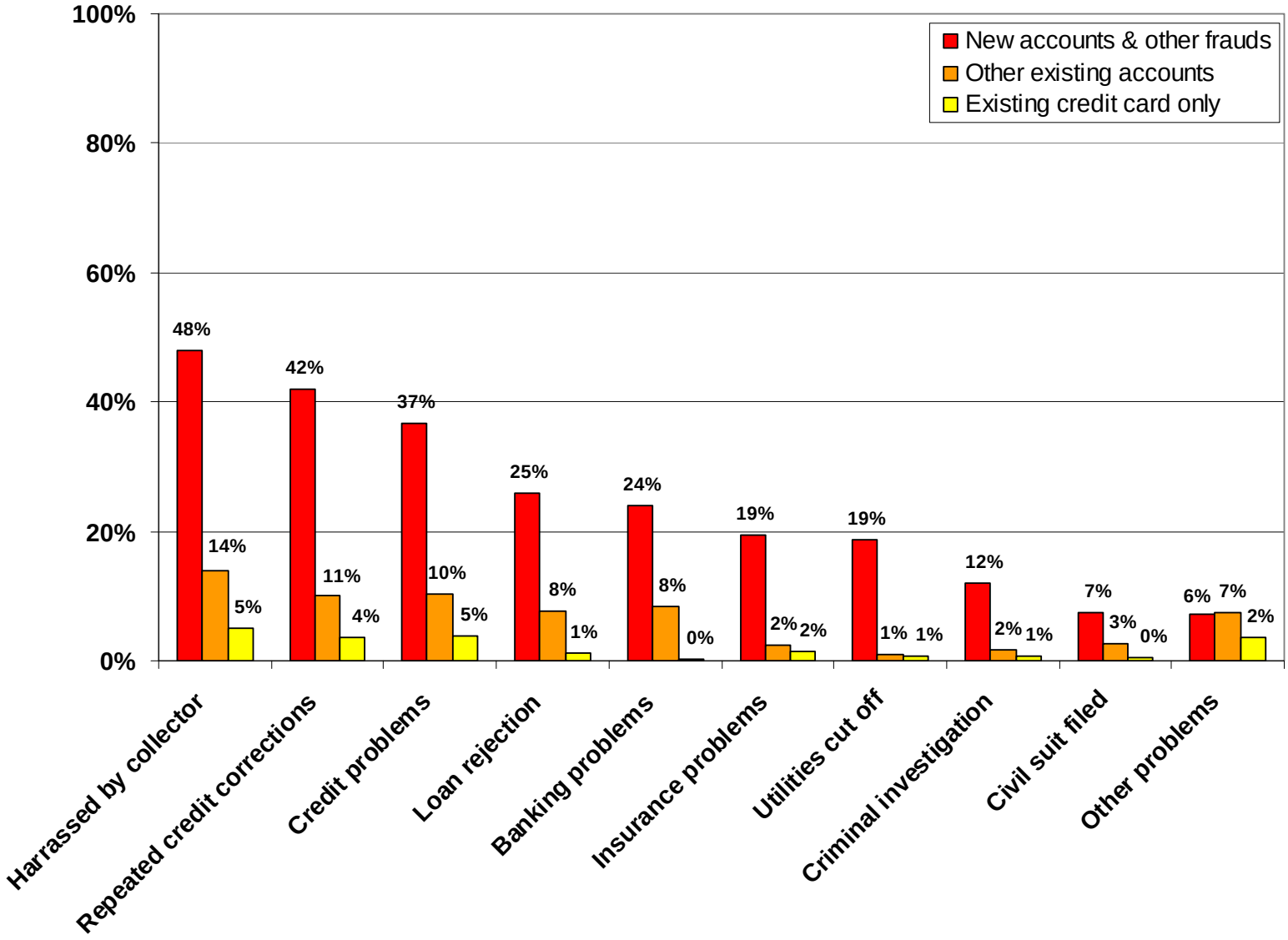


- This graph shows the estimated hours spent by victims in resolving problems stemming from ID theft. It does not refer to the amount of time that passed from when the victims discovered the crime to when their problems where resolved.
- When asked about the amount of time spent resolving problems stemming from the misuse of personal information, the median amount of time reported for all victims was 4 hours.

[23] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed. Figures for Existing Credit Cards Only, Existing Non-Credit Card Accounts, and New Accounts & Other Frauds are based on the responses of the 257, 164, and 138 individuals, respectively, who indicated that they had experienced these types of ID theft during this period of time.

- Thirty percent of victims reported that they spent one hour or less resolving problems that resulted from their ID theft.
    - Victims in the Existing Credit Cards Only category (45%) were most likely to report spending one hour or less resolving problems. Those in the Existing Non-Credit Card Accounts category (25%) and in the New Accounts & Other Frauds category (17%) were less likely to report one hour or less.
- Sixty percent of New Accounts & Other Frauds victims reported spending 10 or more hours resolving problems resulting from their ID theft. They were more than twice as likely as Existing Non-Credit Card Accounts victims (25%), and three times as likely as Existing Credit Card Only victims (20%), to spend this much time.

Figure 15 - Q67 – Problems Experienced[24]



- Victims were asked whether they had experienced various types of problems, other than dollars and time expended, as a result of having their personal information misused. These included having problems obtaining or using a credit card, being turned down for a loan, or having problems opening a bank account or cashing checks.
    - 16% of ID theft victims reported having credit problems, such as being rejected for credit or having a credit card refused by a merchant.

[24] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed. Figures for Existing Credit Cards Only, Existing Non-Credit Card Accounts, and New Accounts & Other Frauds are based on the responses of the 257, 164, and 138 individuals, respectively, who indicated that they had experienced these types of ID theft during this period of time.

  - 10% of ID theft victims reported suffering banking problems, such as being refused for a checking account or having checks rejected.

  - 7% of victims reported having insurance problems, such as having been turned down for insurance or having to pay higher rates.

- A total of 37% of all ID theft victims reported having at least one of the problems identified; 21% of victims reported having more than one of these problems.

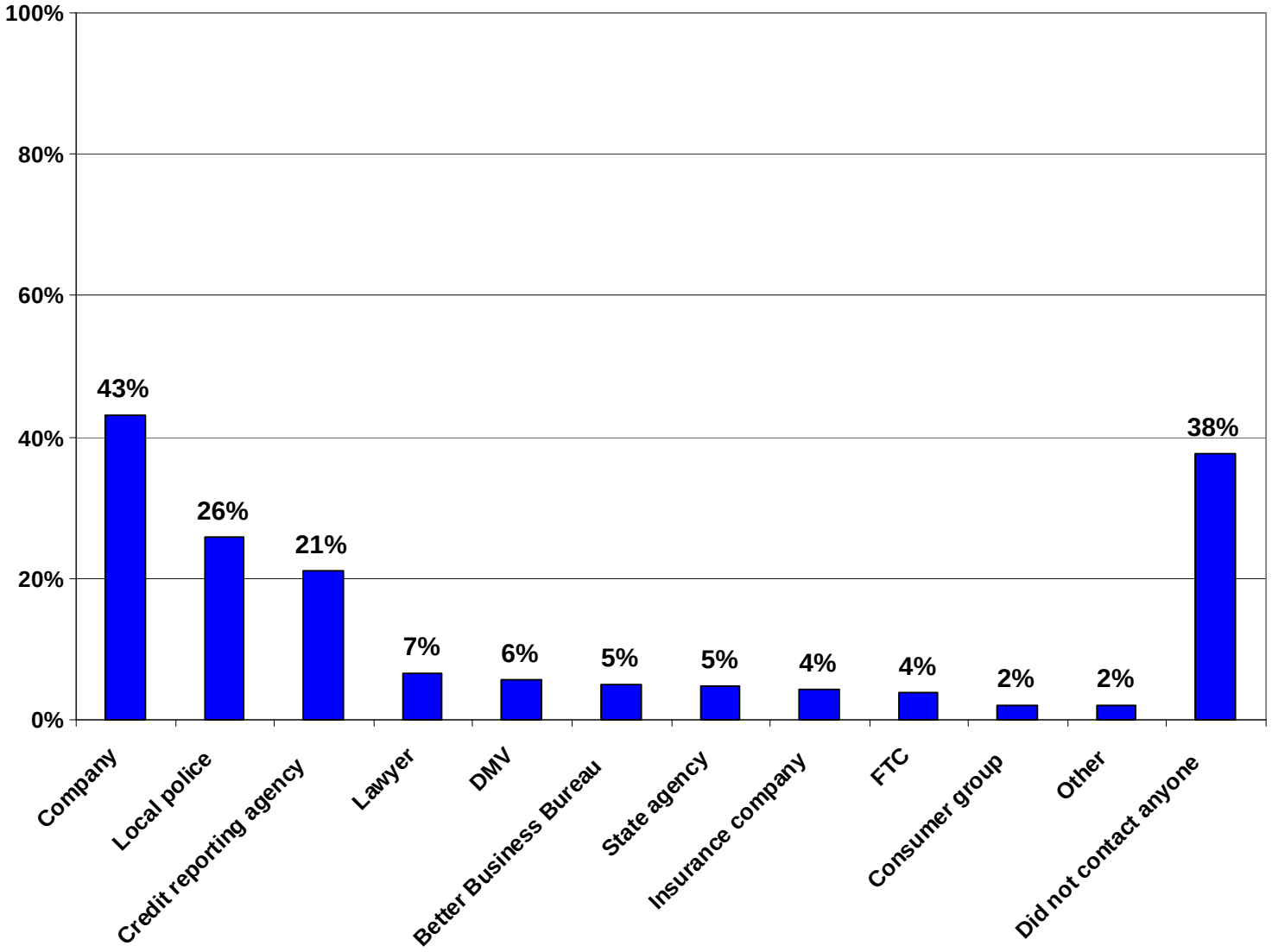
- Victims in the New Accounts & Other Frauds category were more than twice as likely to report having one or more of these problems (68%) as those in the Existing Non-Credit Card Accounts category (32%) and four times as likely as those in the Existing Credit Cards Only category (17%).

- Victims who reported that they had experienced one or more of these problems tended also to report incurring greater out-of-pocket expenses and spending more time to resolve their problems.[25]
  - Among victims who had experienced one or more of these problems, 26% said that they had out-of-pocket expenses of $1,000 or more. Only 3% of victims who did not experience these problems incurred out-of-pocket expenses of $1,000 or more.
  - Thirty-three percent of victims who had experienced one or more of these problems said that they had spent 40 hours or more resolving problems related to their ID theft. Only 6% of victims who did not experience these problems reported spending 40 hours or more resolving problems.

[25] Figures for those who experienced one or more of the problems discussed here are based on 177 observations; figures for those experienced none of the problems are based on 382 observations.

Actions Taken

Figure 16 - Q53 / Q53a/ Q54 / Q60 – Victim Contacts with Selected Parties[26]



- Forty-three percent of victims said that they contacted or were contacted by a company where an account was opened in their name or where an existing account was misused.[27]

[26] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed.

[27] This figure may not include all respondents who had contact with the company where an account was opened or misused. The 43% figure includes victims who indicated such contact in Q54, or who in answer to Q53, indicated that they had not contacted anyone, but whose verbatim responses when asked why they had not contacted anyone (Q53a) indicated that there had, in fact, been contact with a company or credit card company. However, many victims who said they had not contacted anyone were not asked Q53a and therefore remain in the "Did not contact anyone" group. Therefore, the survey is likely to underestimate the number of consumers who had contact with the company.

For the same reason, the number of consumers who did not contact anyone is likely to be overstated. In addition, the "Did not contact anyone" figure includes a significant number of people who in response to Q53 indicated that they had

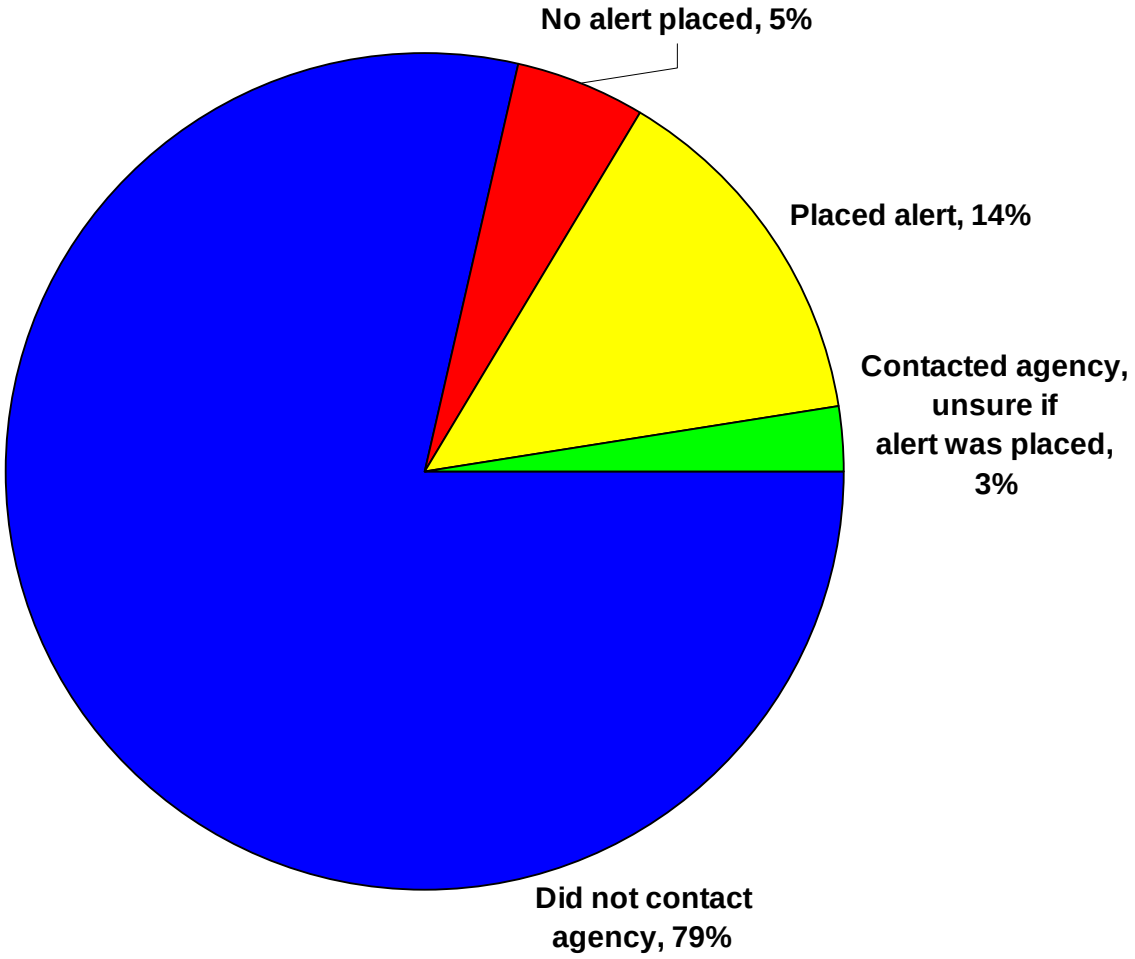
- Twenty-six percent of victims said that they had contacted the police.
    - While only 9% victims in the Existing Credit Cards Only category contacted the police, 44% of victims in the New Accounts & Other Frauds category did so.[28]
- Twenty-one percent of victims reported contacting one or more credit reporting agencies.
    - While only 15% of victims in the Existing Credit Cards Only category and 12% of the Existing Non-Credit Card Accounts category contacted a credit reporting agency, 41% of those in the New Accounts & Other Frauds category made such contact.
    - Victims were more likely to contact a credit reporting agency when the thief obtained a higher dollar amount. Twenty-nine percent of victims contacted at least one credit reporting agency when the value was over $1,000, compared to 16% when the value was less than $1,000.[29]

contacted someone, but then in response to Q54 indicated that they had not contacted any of the identified entities, including "someone else."

[28] Figures for Existing Credit Cards Only, Existing Non-Credit Card Accounts, and New Accounts & Other Frauds are based on the responses of the 257, 164, and 138 individuals, respectively, who indicated that they had experienced these types of ID theft between 2001 and the date they were interviewed.

[29] Figures for instances where the thief obtained goods and services with a value of less than $1,000 are based on 329 observations and where the value was $1,000 or more are based on 201 observations.

Figure 17 - Q54 / Q63 –Initial 90-day Fraud Alert Placed[30]



Since December 2004, the Fair Credit Reporting Act has allowed consumers who have a good faith suspicion that they have been or are about to become victims of ID theft to place an initial "fraud alert" on their credit file that will appear on credit reports issued to potential users of the report. The initial fraud alert remains in place for 90 days and notifies potential users that the consumer may be a victim of ID theft. A potential creditor that receives a credit report containing a fraud alert is required to take reasonable steps to verify the identity of the person applying for credit.[31]

- Fourteen percent of victims said they placed an initial 90-day fraud alert on their credit reports following the discovery of the misuse of their information.[32]

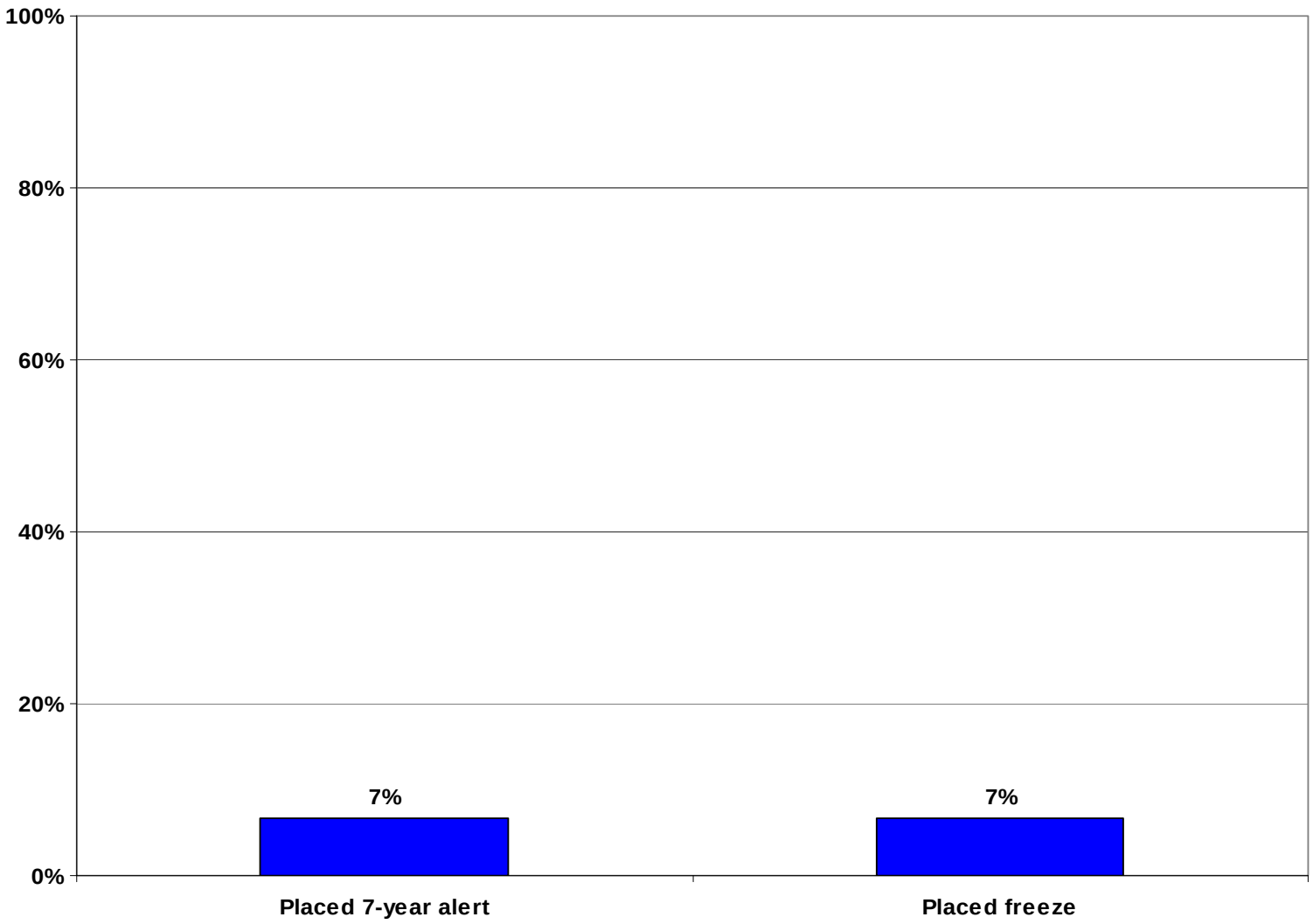
[30] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed.

[31] See Fair Credit Reporting Act, § 605A(h); 15 U.S.C. § 1681c-1(h).

[32] Figures for Existing Credit Cards Only, Existing Non-Credit Card Accounts, and New Accounts & Other Frauds are based on the responses of the 257, 164, and 138 individuals, respectively, who indicated that they had experienced these types of ID theft between 2001 and the date they were interviewed.

- Twenty-nine percent of victims in the New Accounts & Other Frauds category placed such alerts on their credit reports.
- Six percent of victims in the Existing Credit Cards Only category reported placing initial fraud alerts on their credit reports.

Figure 18 - Q66 / Q61 – Further Measures Taken By Victims[33]



If a consumer has become an ID Theft victim, the Fair Credit Reporting Act since December 2004 has allowed the victim to place an extended, seven-year fraud alert on his or her credit file. The extended alert appears on all credit reports about the victim, notifying any potential user that the consumer has been a victim of ID theft. The extended alert also contains a telephone number at which the consumer may be reached, and any potential creditor is required to contact the consumer either at this number or in person before extending any additional credit in the consumer's name.[34] To get an extended alert, the consumer must provide the credit reporting agencies with an "Identity Theft Report," which is a detailed report that has been filed with a law enforcement agency.

[33] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed.

[34] See Fair Credit Reporting Act § 605A(b), 15 U.S.C. § 1681c-1(b).

In addition, some states allow ID theft victims to request a "credit freeze," which prevents their credit reports from being accessed without their express consent.[35] Because most companies obtain a credit report from a consumer before extending credit to a consumer, a credit freeze generally prevents the creation of new credit accounts in a consumer's name without the consumer's express permission. At the time this survey was conducted, credit freezes were available to consumers in 10 states.[36] As of the date of publication, most states have enacted credit freeze laws. Also, the three nationwide credit reporting agencies have offered freezes to consumers, even in states without specific credit freeze laws.

- Relatively few ID Theft victims took advantage of either extended alerts or credit freezes:
  - Seven percent of ID Theft victims placed extended alerts on their credit reports.
  - Seven percent of ID Theft victims placed a freeze on their credit reports.
  - Each of these actions was taken by 15% of those in the New Accounts & Other Frauds category, but only by 3% to 4% of those in the Existing Accounts categories.[37]

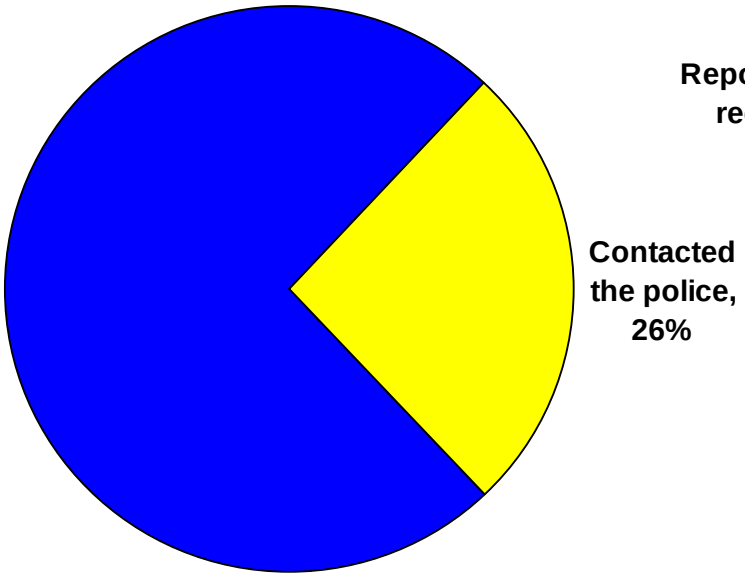
[35] Some states permit all consumers to obtain credit freezes, regardless of whether they are identity theft victims.

[36] See, e.g. California Civil Code § 1785.11.2, Connecticut General Statutes § 36a-701a; Louisiana Statutes Annotated § 9.3571(H) to (Y); North Carolina General Statutes §75-63.

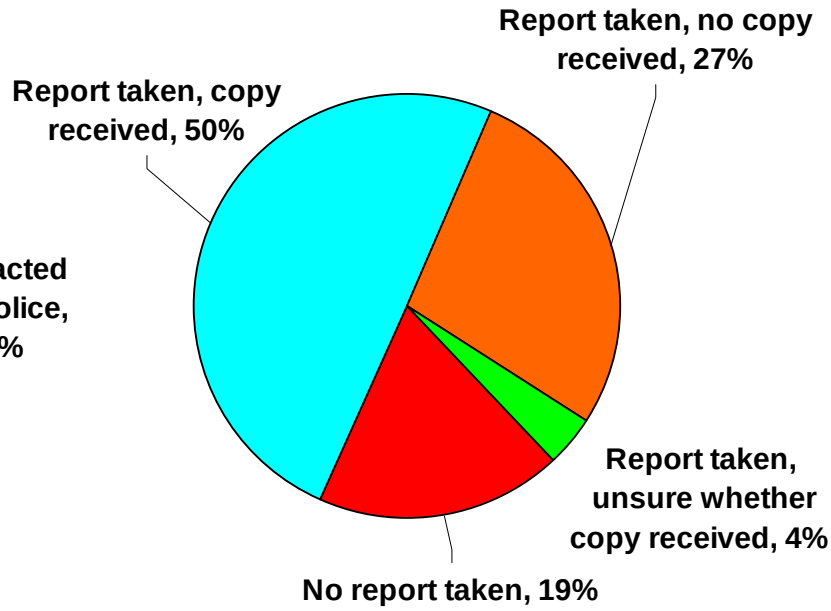
[37] Figures for Existing Credit Cards Only, Existing Non-Credit Card Accounts, and New Accounts & Other Frauds are based on the responses of the 257, 164, and 138 individuals, respectively, who indicated that they had experienced these types of ID theft between 2001 and the date they were interviewed.

Figure 19 - Q54 / Q55 / Q56 – Contact with Local Law Enforcement[38]

All ID Theft Victims



Those Who Contacted the Police



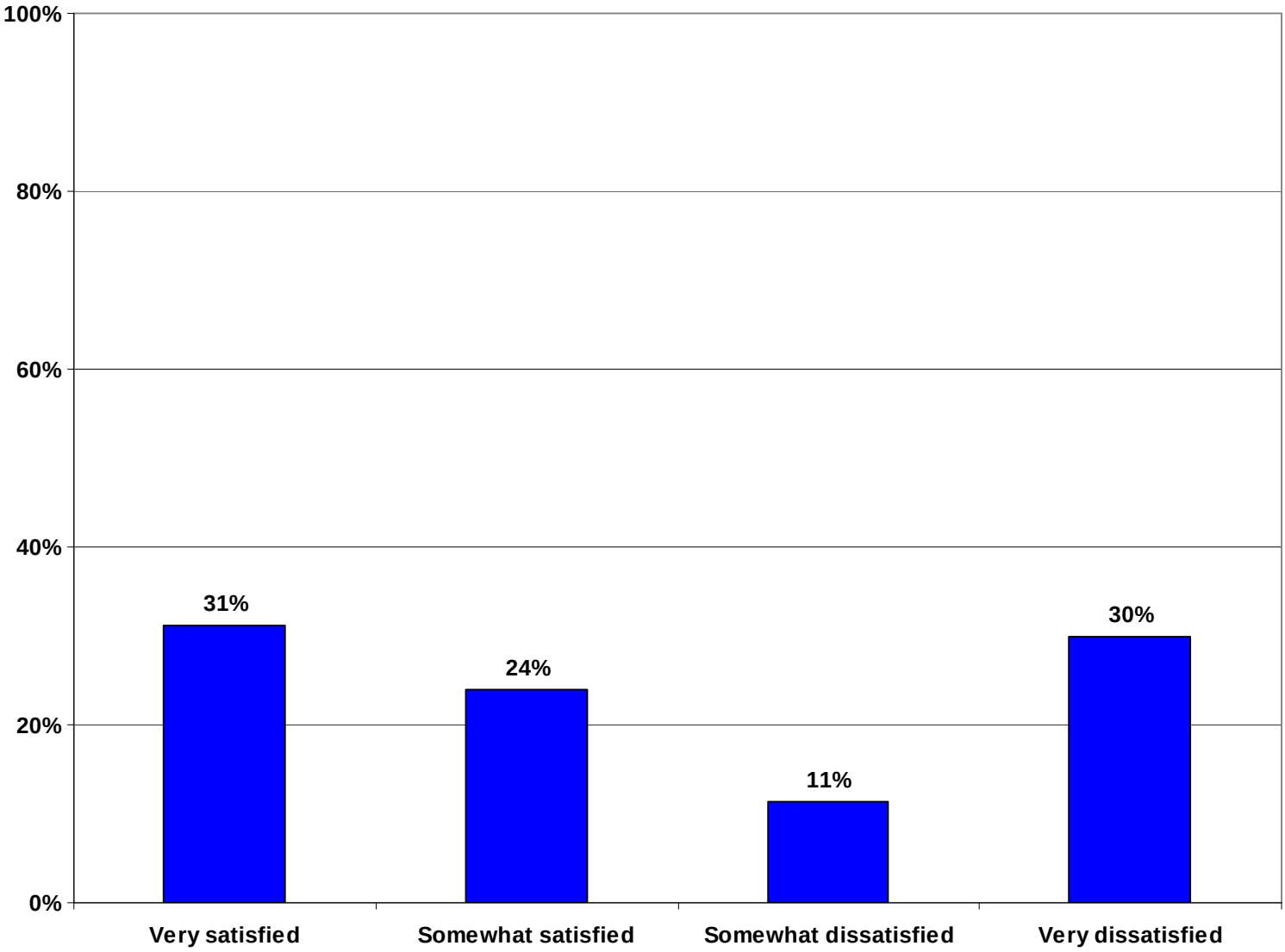
- A total of 26% of all victims contacted a local law enforcement agency.
- Although only 9% of victims in the Existing Credit Card Only category contacted the police, the police were contacted by 44% of those in the New Accounts & Other Frauds category.[39]
- Eighty-one percent of victims who contacted a local law enforcement agency reported that the police took a report (21% of all victims).[40]
- The police did not take a report from 19% of victims who contacted them (5% of all victims).
- Where the local police took a report, 60% of victims reported receiving a copy of the report (13% of all victims). However, 40% of victims did not get a copy or could not recall if they got a copy (7% of all victims, and 1% of all victims, respectively).

[38] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed.

[39] Figures for Existing Credit Cards Only, Existing Non-Credit Card Accounts, and New Accounts & Other Frauds are based on the responses of the 257, 164, and 138 individuals, respectively, who indicated that they had experienced these types of ID theft between 2001 and the date they were interviewed.

[40] Figures on the experiences of victims who contacted a local police department are based on 127 observations, while those where a police report was taken are based on 107 victims.

Figure 20 - Q57 – Satisfaction with Local Law Enforcement Response[41]

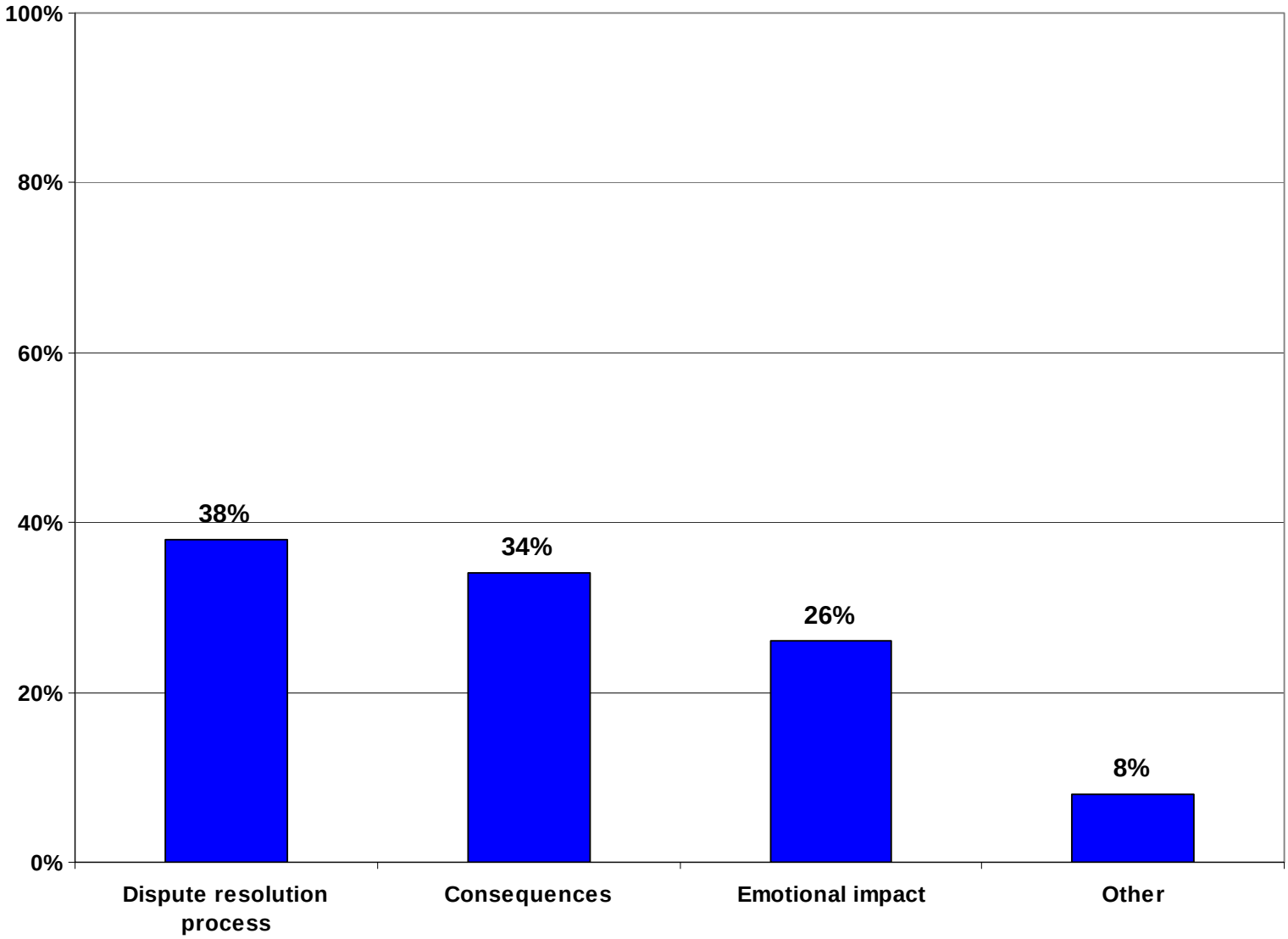


- Of the victims who contacted local law enforcement, 55% said they were “very” or “somewhat” satisfied, whereas, 41% of the victims who contacted local law enforcement were either “very” or “somewhat” dissatisfied with the response of local law enforcement.[42]

[41] These figures are based on the responses of 127 participants who said that they had contacted a local police department.

[42] These figures do not total 100% because some victims indicated either that they did not know whether they were satisfied with the response of the police or refused to answer the question.

Figure 21 - Q68 – Biggest Challenges of Experience[43]



- Respondents who had spent 10 or more hours resolving problems were asked to describe in their own words the most difficult part of their experience. These respondents represent 31% of all ID Theft victims.

- Nearly 4-in-10 of these victims (38%) said that going through the dispute resolution process, itself, was the most difficult part. The dispute resolution process involves communicating with consumer reporting agencies and the companies where the thief committed the fraud to have the debts absolved and the credit reports corrected. It also involves the procedure of replacing credit cards and other key documents. Respondents also mentioned the sheer amount of time the dispute resolution process took.

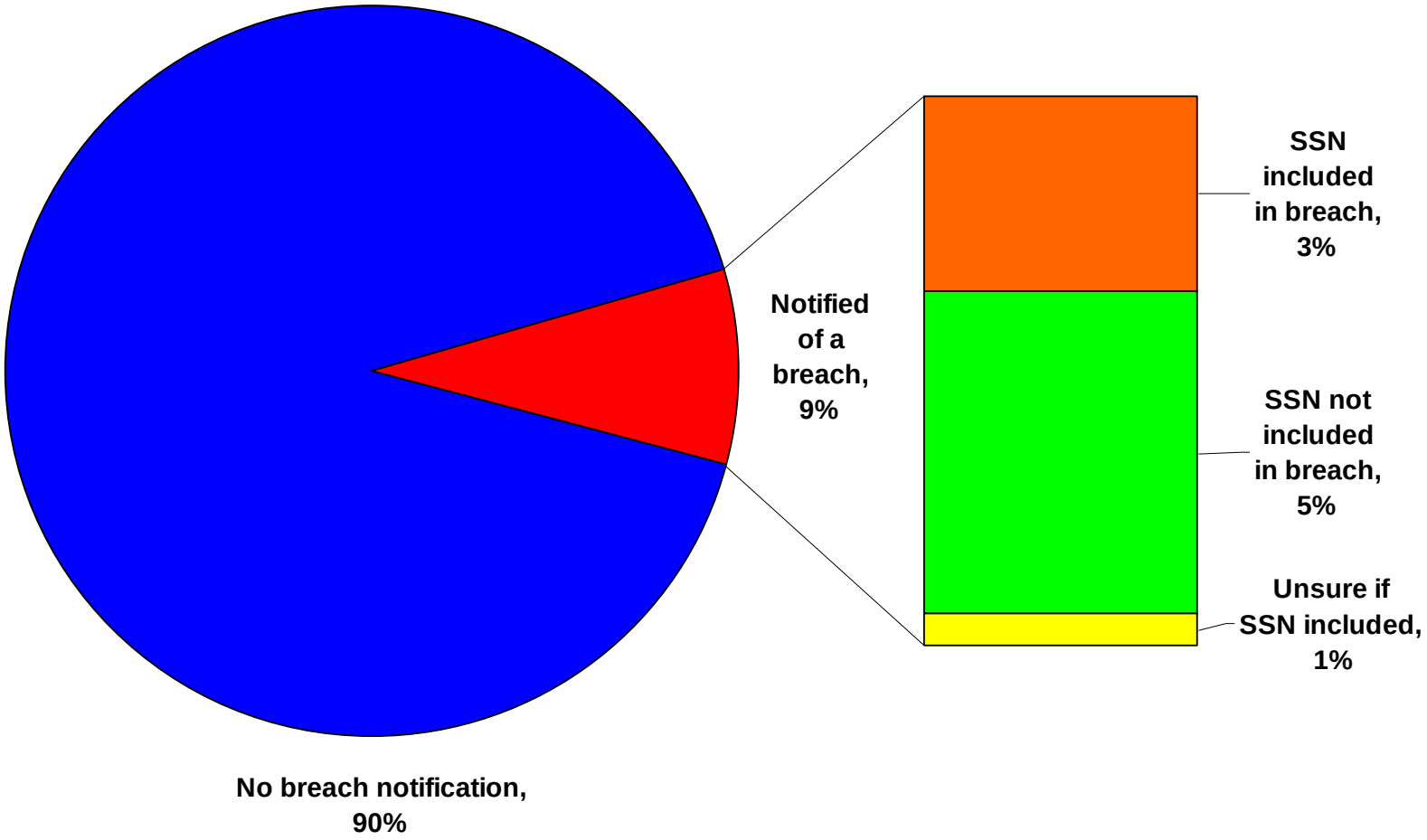
[43] These figures are based on 172 responses of victims who said that they spent 10 hours or more resolving problems associated with being a victim of ID theft.

- About one-third (34%) of these victims mentioned dealing with the practical consequences of the thief's actions, rather than the process of resolving disputes, as the most difficult part of their experience. Victims must cope with losing money, being unable to use their credit and bank accounts, or having their utilities shut off. Victims also reported being unable to open new accounts and other consequences flowing from the damage to their credit reports.

- Twenty-six percent of these victims said they were most affected by the emotional impact of the ID theft including the effects of stress on their lives and their health or the emotional toll resulting from the realization that they were vulnerable or had been betrayed.

Breach Notification

Figure 22 - Q10 / Q10aa – Breach Notification Since 2001[44]



- All survey participants, including those who were not identity theft victims, were asked if they had received notice of a breach of their personal information. A breach notification involves a company, agency, or some other organization notifying consumers that there has been a breach of the security of their data files, and that the consumer's personal information is among the information that has been compromised. It does not demonstrate any misuse of the information, just that the information has been compromised.[45]

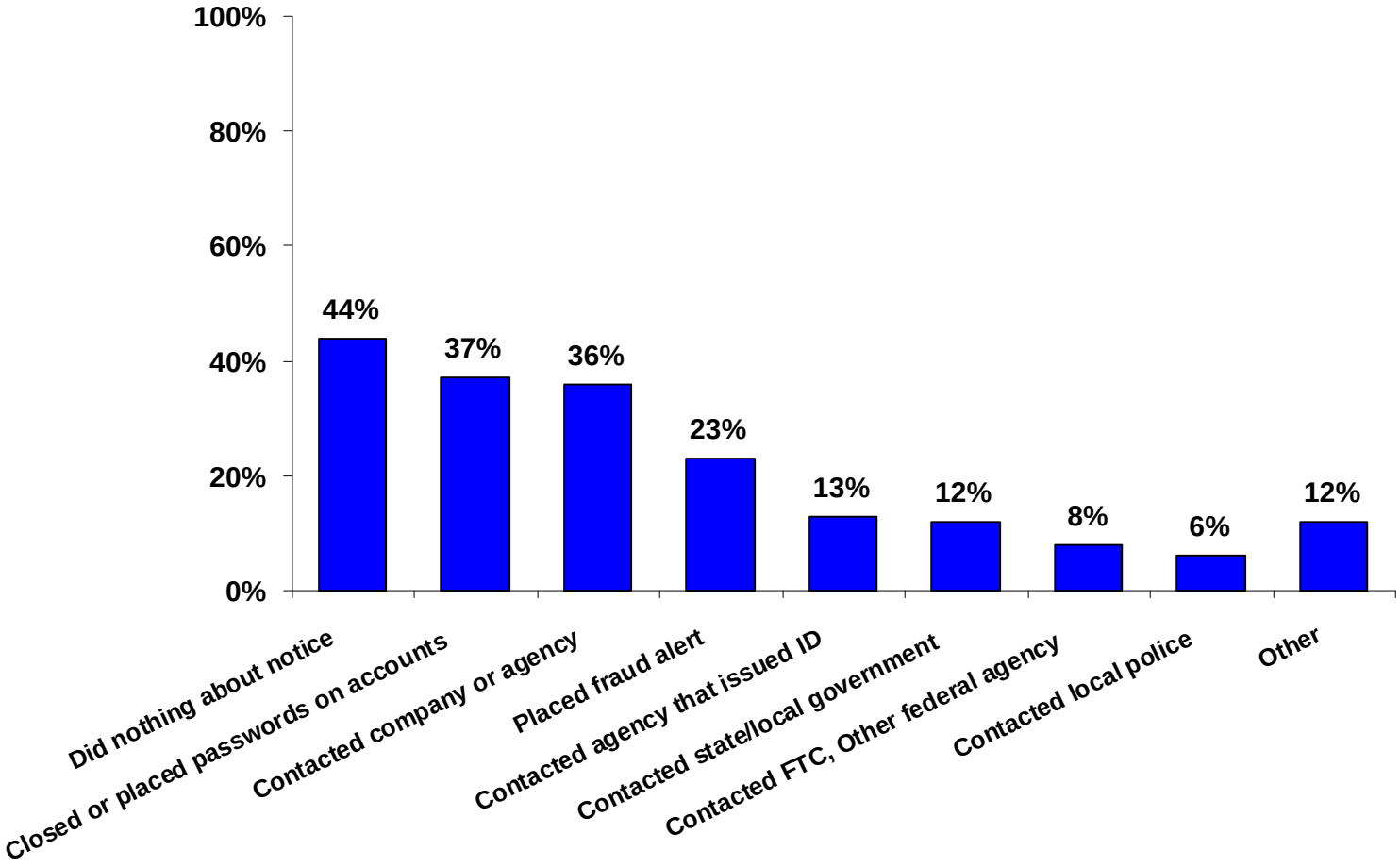
[44] Percentage of people receiving a breach notification is based on 1,496 observations. Based on the survey design, demographic characteristics were only collected for 1,496 of the 4,916 people interviewed, including all of those who reported being a victim of ID theft and a random sample of those who were not victims. Weights could only be computed for these observations with weights adjusted to reflect the fact that only a sample of non-victims would be included in weighted calculations. (See Methodological Appendix.)

[45] The practice of notifying consumers of data breaches is a relatively recent development. In 2003, California passed a law (Civil Code § 1798.92) requiring any business that stores data concerning California residents to notify those residents in the event of any actual or suspected data breach. Since the passage of the California statute, over 30 other states have passed some form of breach notice law. As a result of these laws, breach notices, and the resulting publicity regarding breaches, have become more common. Because breach notices were not a common occurrence prior to the passage of the California law, the 2003 FTC Survey did not include questions about them.

- Nine percent of all respondents indicated they had been notified about a breach of their personal information since 2001. [46]

[46] This figure may overstate slightly the share of survey participants who received breach notices. Respondents who were contacted by a credit card or other company about actual misuse of their individual accounts may have answered that they had received a "breach notice," even though breach notices are not generally considered to include this type of contact. In addition, recent testing of a similar survey question suggests that some respondents who experienced ID theft may mistakenly have answered "yes" to the question because they discovered that their "information had been lost or stolen," even though they had not "been notified by a company, government agency, or other organization" of this fact.

Figure 23 - Q12 / Q13 – Actions Taken Following Breach Notification[47]



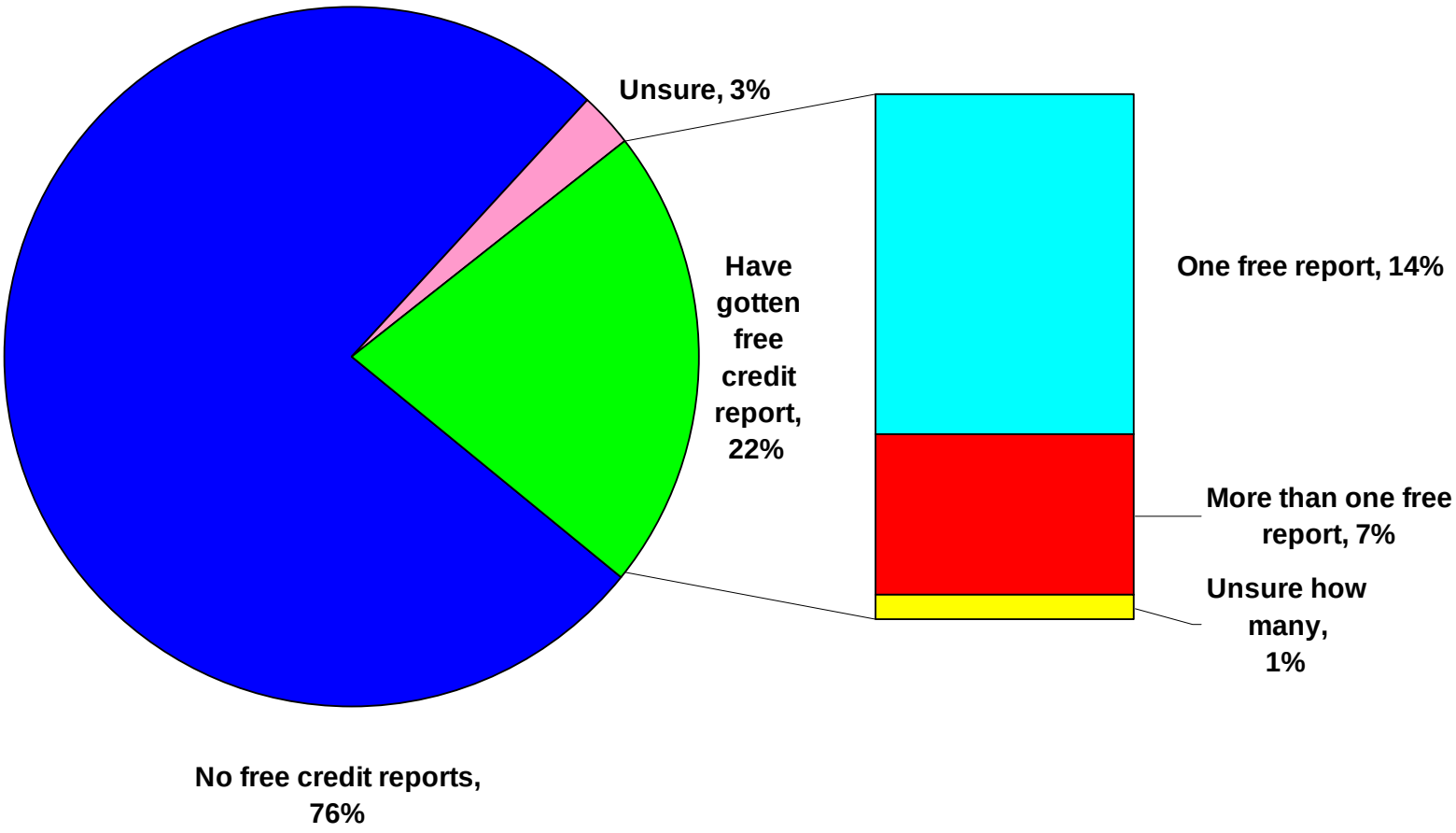
- Most people (55%) who received a notice about a breach of their information took action to understand or proactively address the situation.[48] Note that respondents could mention more than one action, so the sum of the specific steps taken displayed in the graph above will be greater than 55%.

- Most of those who were notified of a breach and did take action either called the company or agency that sent the notice (36% of those who received a breach notice) or closed an affected account or placed a password on it (37%).

[47] Based on responses of 187 individuals who said that they had received a breach notification since 2001.
[48] The figures for those that took some sort of action in response to a breach notice (55%) and those that took no action (44%) do not total 100%. This is because 1% of respondents refused to answer or stated that they did not know whether they took any action.

Free Credit Reports

Figure 24 - Q13a/Q13b – Free Credit Reports Since 2004[49]



All consumers are entitled to receive a free copy of their credit report from each of the three nationwide credit reporting agencies ("CRAs") (Experian, Equifax, and TransUnion), as well as from various nationwide specialty CRAs, every twelve months.[50] Additionally, placing a fraud alert entitles consumers to immediately request free copies of their credit reports regardless of the timing of their previous requests.[51] Consumers who have had an extended fraud alert placed on their credit reports are entitled to request two free copies of their credit report from each of the CRAs in the twelve months following the date the extended alert was placed.[52]

[49] Based on 1,496 observations. Demographic characteristics were only collected for 1,496 of the 4,916 people interviewed, including all of those who reported being a victim of ID theft and a random sample of those who were not victims. Weights could only be computed for these observations with weights adjusted to reflect the fact that only a sample of non-victims would be included in weighted calculations. (See Methodological Appendix.)

[50] FCRA § 612(a), 15 U.S.C. § 1681j(1).

[51] FCRA § 605A(a)(2), 15 U.S.C. § 1681c-1(a)(2).

[52] FCRA § 605A(b)(2)(A), 15 U.S.C. § 1681c-1(b)(2)(A).

- Just over 1-in-5 respondents in the overall sample (22%) said they had availed themselves of a free credit report since the annual free credit reports began to become available in parts of the country on December 1, 2004.[53] Annual free credit reports became available nationwide on September 1, 2005.

- Those with more than a high school education were nearly twice as likely as those with a high school education or less to request a free credit report (27% vs. 14%).[54]

- Respondents between the ages of 25 and 44 were most likely to request a free credit report (29%), while those age 65 and over were least likely to do so (13%).[55]

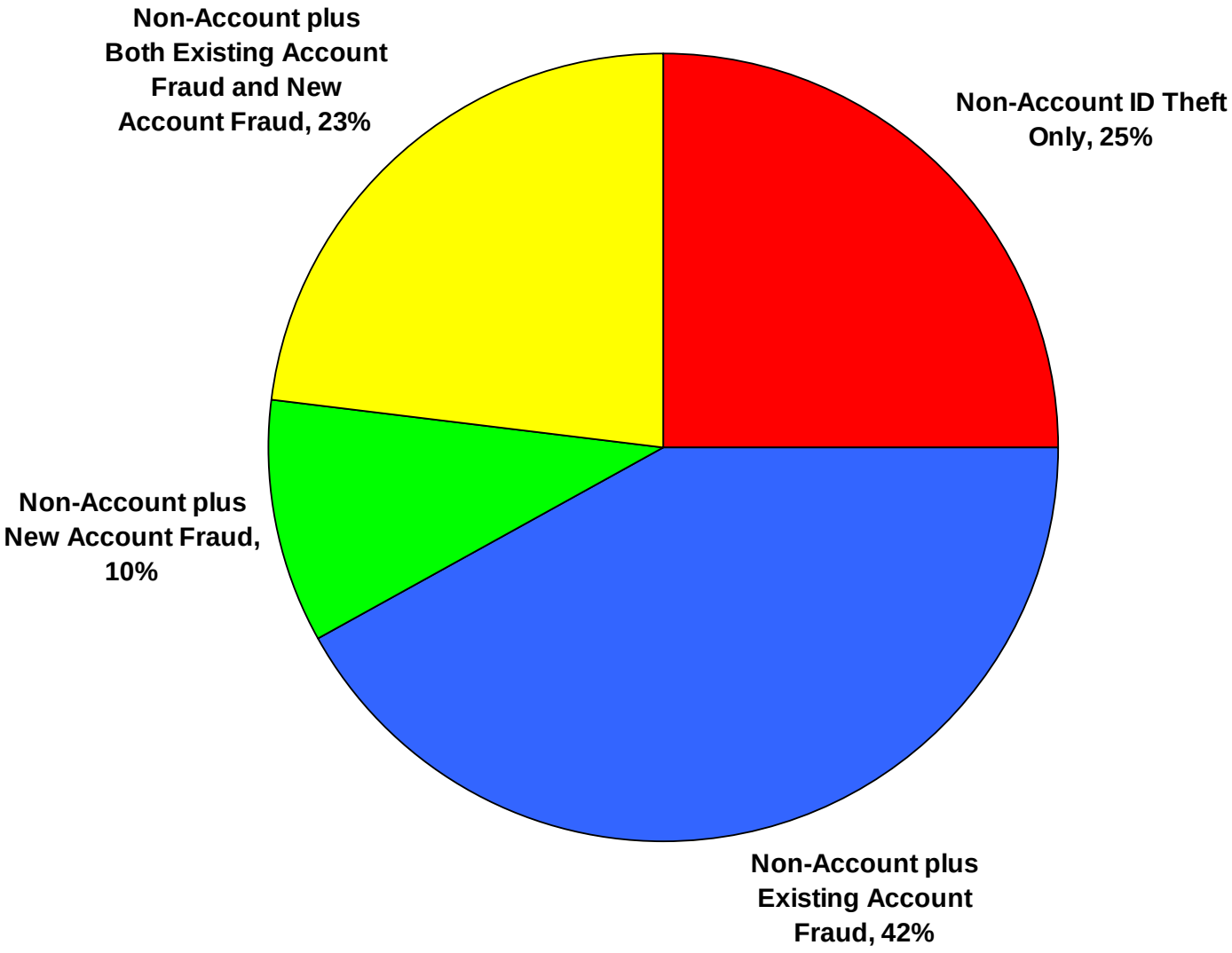
[53] Although respondents were asked whether they had received any "free annual credit reports," some respondents may have answered "yes" for credit reports received through other means, such as reports received as a result of placing a fraud alert.

[54] Based on responses of 453 individuals who were high school graduates or had not completed high school and 993 individuals who had attended at least some college.

[55] Based on responses of 428 individuals between 25 and 44 years of age and 309 individuals age 65 or over.

Victims of Non-Account ID Theft

Figure 25 - Q9 / Q34 – Non-Account ID Theft



- Overall, the experiences of 20% of ID theft victims included having their personal information used in "Non-Account ID Theft," which is fraud that does not involve accessing the victim's existing accounts or creating new financial accounts in the victim's name.[56] For example, the thief might provide the victim's name and information to employers for employment purposes, to the government to obtain disaster relief or benefits, or to police when being charged with a crime.
- Among Non-Account ID Theft victims, 61% reported a specific way that their information had been misused – Figure 6 describes their responses. The remaining 39% indicated that their information had been misused to commit this type of fraud, but did not indicate the specific

[56] This figure cannot be compared directly with those in Figure 2 on page 14. As noted in footnote 11, Figures 1 – 3 are based on responses of people who discovered that their information was being misused in 2005, while the rest of the report is based on the responses of people who discovered that their information was being misused between the beginning of 2001 and the time they were interviewed.

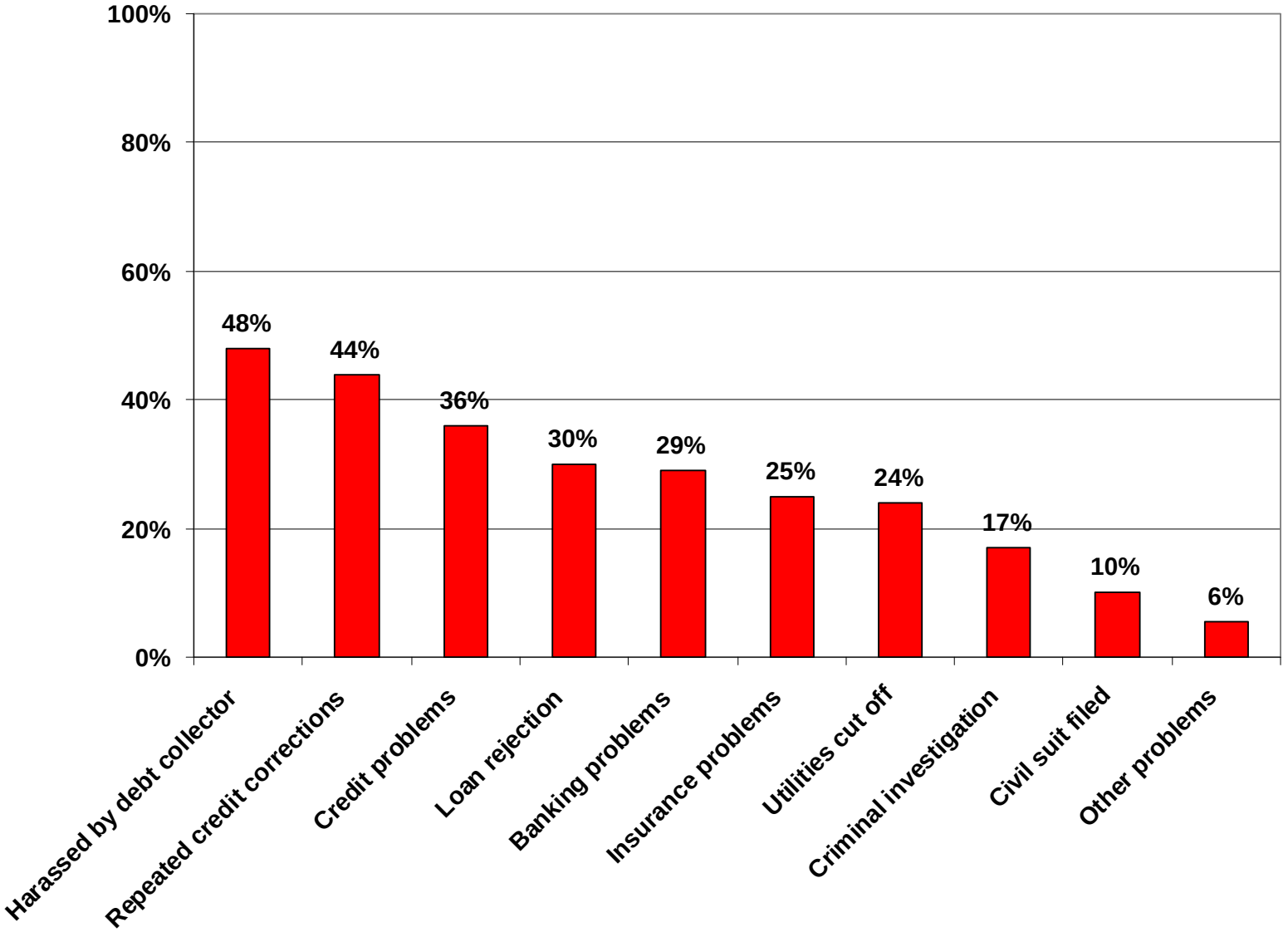
way it had been misused. Among the specific offenses committed by thieves using their information:

- Twenty-seven percent had their name given to law enforcement when the perpetrator was stopped or charged with a crime.
- Eighteen percent had their information used by the thief to obtain medical treatment, services, or supplies.
- Renting housing and obtaining government benefits were each reported by 6% of these victims, and obtaining employment was reported by 5%.

- Many Non-Account ID Theft victims also experienced types of ID theft that involve financial accounts: 65% experienced the misuse of existing accounts, and 33% had one or more new accounts opened in their name.[57]
  - Forty-three percent had an existing checking or savings account misused.
  - Thirty-four percent had an existing credit card misused.
  - Twenty-five percent had existing telephone (cellular or conventional) accounts misused and 18% had new telephone accounts opened in their name.
  - Fourteen percent had new credit card accounts opened in their name.

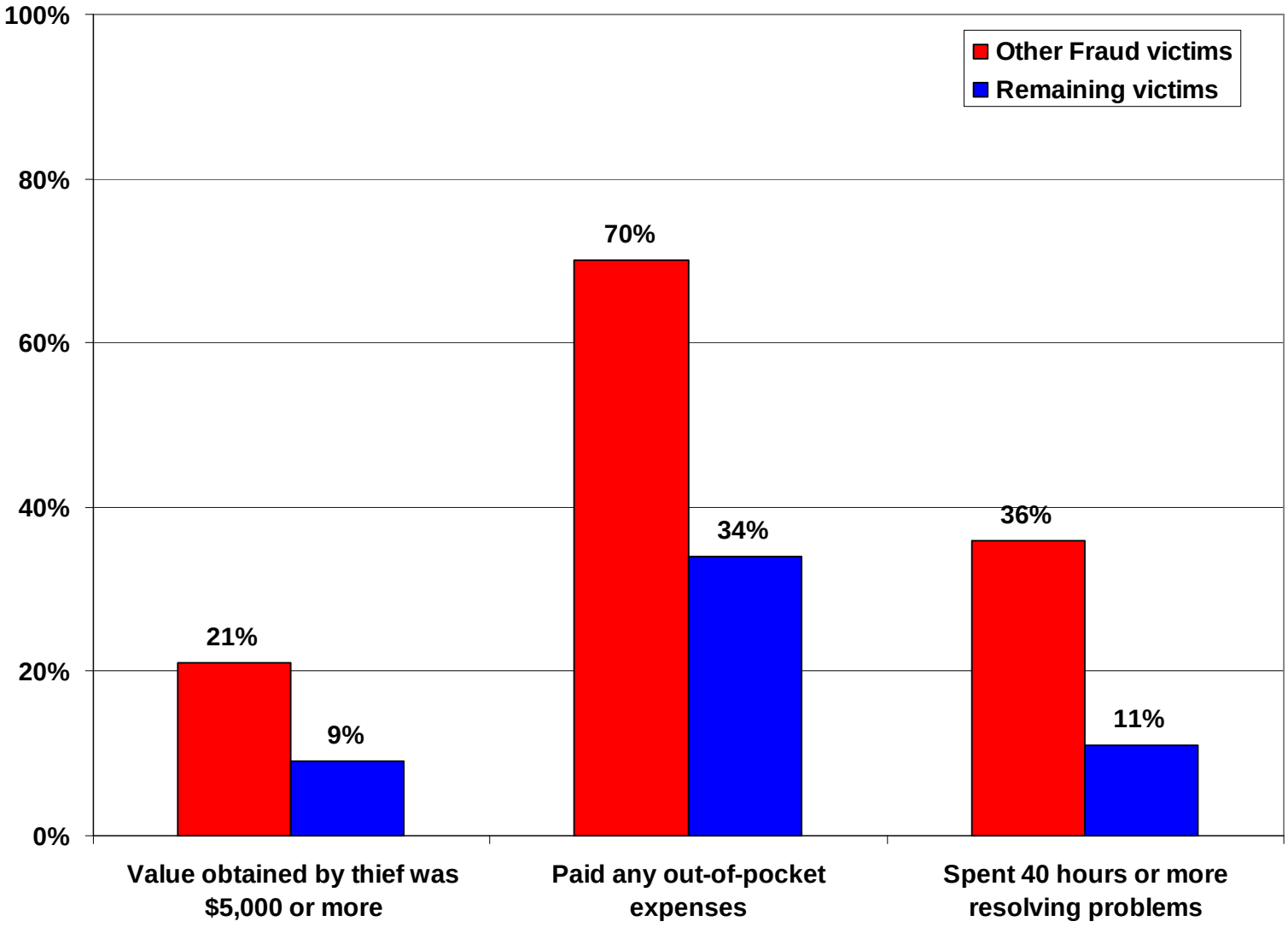
[57] Based on the responses of 84 survey participants who indicated that they had experienced non-account ID theft.

Figure 26 - Q67 – Non-Account ID Theft Victim Experience



- Approximately two-thirds (70%) of all ID Theft victims whose experiences included Non-Account ID theft encountered one or more of the problems in the above graph. This is nearly two and one-half times the rate for those whose experiences did not include Non-Account ID Theft (29%).
- The most frequently reported problems were:
  - Forty-eight percent of Non-Account ID Theft victims reported being harassed by a debt collector.
  - Forty-four percent said they needed to repeatedly correct information on their credit report.
  - Thirty-six percent said they experienced credit problems.
  - Thirty percent had been turned down for a loan.
  - Twenty-nine percent reported having banking problems.

Figure 27 - Q36 / Q41 / Q48 – Costs of Non-Account ID Theft



- Where the victim's experience included Non-Account ID Theft, the value obtained by the thief was more than twice as likely to be $5,000 or more (21%) than for cases that did not involve this kind of misuse (9%).
- Victims whose experiences included Non-Account ID Theft were more likely than the remaining ID Theft victims to suffer costs associated with their experience.
    - Non-Account ID Theft victims were more than twice as likely to have actual, out-of-pocket expenses associated with their experience (70% of Non-Account ID Theft victims had to pay out of pocket expenses vs. 34% of the remaining victims).
    - Victims of Non-Account ID Theft were over three times more likely than the remaining victims to spend 40 hours or more resolving their problems (36% vs. 11%).

APPENDIX A: METHODOLOGY REPORT

FTC Identity Theft 2006 Methodology Report

Contract: FTC-04-Z-0004

Prepared for:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20500

Prepared by:

1650 Tysons Blvd. Suite 110
McLean, VA 22102-3915

September 28, 2006

I. Background and Objectives

The Federal Trade Commission (FTC) commissioned a study to gather information on consumer experiences with Identity Theft building upon similar research conducted in 2003. Since that time, more has become known about Identity Theft, the ways people are victimized, the costs, and the toll taken on its victims. The previous survey instrument was updated based on a review of 2003 results and the updated information will help policymakers, organizations, and citizens combat Identity Theft.

The survey was conducted through telephone interviews using a Random-Digit-Dialing (RDD) sampling methodology. The sampling scheme was designed to obtain a random sample of U.S. adults age 18 and older. A total of 4,917 interviews were conducted between March 27 and June 11, 2006.

The results contained in this report are based generally on the responses of those people who discovered that their personal information was being misused—that is, that they were victims of ID theft—between the beginning of 2001 and when they were interviewed. The data on the number of people who discovered they were victims of ID theft in 2005 and the data in the sections on breach notification and free credit reports are based on the responses of all survey participants from whom demographics were collected.[1] The data in Figure 2 and 3 are based on the responses of those who discovered that their personal information was being misused in 2005.

For many of the survey questions, there were a few respondents who either did not know the answer to the question or who refused to answer the question. In computing the figures in the report, those who answered “don’t know” or refused to answer have not been eliminated. Rather, they are included and simply recorded as not giving any of the indicated responses to a particular question. As a result, the responses to a question may total to less than 100 percent even where the question called for each participant to give only one response.

II. Methodology

A. Sampling Frame

The sampling frame consisted of all blocks of telephone numbers with at least one listed residential telephone number. A block of telephone numbers consisted of 100 numbers having the same first eight digits. The survey employed the GENESYS sampling system which randomly generates representative single-stage samples of telephone numbers. It generates each telephone number by randomly selecting a block known to contain at least one listed residential telephone number and then randomly generating the two final digits to complete the number. The advantage of beginning with blocks containing a known residential number is that it avoids generating numbers in blocks that are assigned exclusively to businesses or are unassigned. The resulting sample of telephone numbers represents all households in the U.S. with telephones, both listed and unlisted, without bias and with the efficiency of a single-stage sample.

[1] See Section II.I, below for a discussion of the collection of demographic data and the weighting of the resulting responses to ensure that the resulting analysis was representative of the population of U.S. adults as a whole.

The sampling frame was stratified to meet the goals of the sampling plan. The strata were constructed such that the resulting sample would provide a nationally representative statistical sample of US households in the 50 states and the District of Columbia.

Eight strata were defined and compiled by Census Region and urban/non-urban requirements. The top three classes of Metropolitan Statistical Areas as defined by the Census Bureau were categorized as urban, while the bottom two classes were categorized as non-urban.

The strata and the number of sample records dialed in each stratum are listed in the table below:

Identity Theft Study 2006 Starting Sample Distribution	
Region	**Sample records**
Northeast / urban	6,228
Northeast / non-urban	1,854
Midwest / urban	6,498
Midwest / non-urban	2,224
South / urban	16,136
South / non-urban	2,952
West / urban	10,986
West / non-urban	2,222
TOTAL	**49,100**

B. Questionnaire Design

The initial draft questionnaire was designed by the Federal Trade Commission, and subsequent drafts were developed collaboratively by the FTC and Synovate.

To ensure that all aspects of the survey instrument and protocol were working as designed, pilot testing was performed early in the field period with a limited number of interviewers dialing households. The pilot testing involved trained interviewers and the fully developed survey instrument programmed into the Computer Assisted Telephone Interviewing (CATI) system. The survey was deemed to be working as intended from a substantive and technical perspective, and the fieldwork continued.

A copy of the final questionnaire appears in Appendix C.

C. Telephone Data Collection

Interviewing began on March 27, 2006 and continued through June 11, 2006. Interviews were conducted between 9 a.m. and 9 p.m. Monday through Friday, between 9 a.m. and 8 p.m. on Saturdays, and between 11 a.m. and 8 p.m. on Sundays (all times local to the households being called).

Interviewers were monitored for quality and provided with guidance and correction when necessary. In addition, project management reports were generated by computer on a daily basis in order to track sample disposition and production rates.

Synovate's CATI system was used for data collection. The questionnaire was programmed into the system, and telephone interviewers read questions as they were logically fed in predetermined order from the computer to a viewing screen. Answers were sent back to the computer through the keyboard. This system reduced interviewer (non-random) error, such as not adhering to skip patterns, thus enhancing the quality of the data.

D. Respondent Eligibility

To be eligible to participate in the study the respondent had to be age 18 or older. The person who answered the telephone was asked to identify the household member, age 18 or older, with the most recent birthday, who then served as the randomly selected respondent.

E. Procedures to Maximize Response Rates

Several procedures were undertaken in order to maximize the response rates and to reduce the chance of interpretive error or bias associated with low response rates. The procedures were:

- Experienced interviewers were assigned to the project.
- Telephone interviews were conducted at different times of the day and days of the week in order to increase the likelihood of locating available respondents at times convenient for them. When possible, callbacks were scheduled at specific times requested by respondents.
- Every telephone number that did not result in contact with a respondent (this excludes business numbers, disconnects, faxes and modems) was dialed up to 7 times in order to increase the chances of finding a potential respondent.
- Production rates, interview length, and sample dispositions were monitored closely every other day.
- Project management personnel received weekly reports containing the number of refusals received and hours dialed by each interviewer. These reports were closely monitored and interviewers with a high refusal to hours-dialed ratio were removed from dialing. Those interviewers who had a ratio above the average were provided corrective feedback and monitored more closely by quality control supervisors. In addition, those who demonstrated the lowest refusal to hours-dialed ratio were selected for conversion dialing.

F. Non-Response Follow-up Results

All people who declined to take the survey were re-contacted by telephone one to two weeks following the initial contact in order to secure their cooperation. The contact was made by more experienced interviewers, specially trained in refusal avoidance techniques. Those respondents who requested they not be contacted again were omitted from these dialing efforts.

In order to assess the extent of any bias due to non-response, a random subset of those who refused for a second time during the conversion attempt answered a few key questions. The results of this interviewing are discussed in Appendix B.

G. Final Sample Dispositions and Response Rates

The table below shows the final dispositions for the entire random digit dial (RDD) sample generated by GENESYS for the FTC Identity Theft Survey. The classification of each sample piece was based on the most significant attempt. For example, if a respondent was not available on the first attempt and subsequent attempts resulted in a no answer, the final disposition was Respondent Not Available. If a respondent refused to participate during the first phase of dialing and the number was found to be an answering machine on a subsequent conversion attempt, it was categorized as a Refusal. Interviews completed during the conversion phase of the study were included in the calculation of the final response rates.

The response rate was computed using the AAPOR Outcome Rate Calculator Version 2.1, formula AAPOR RR3.

Identity Theft Study 2006
Final Overall Sample Disposition

	Total	
	Frequency	Percent
Interview - Category 1		
Completed screening interviews	4,917	10.01
Partial interviews	353	0.72
Total	**5,270**	**10.73**
Eligible, non-interview, Category 2		
Refusal and break off	3,801	7.74
Total	**3,801**	**7.74**
Unknown Eligibility, non-interview, Category 3		
Always busy	533	1.09
No answer	12,417	25.29
Answering machine-don't know if household	2,998	6.11
Call blocking	595	1.21
No screener completed	8,980	18.29
Total	**25,523**	**51.98**
No Eligible, Category 4		
Fax/data line	2,296	4.68
Disconnected number	5,780	11.77
Non-working number	1,620	3.30
Temporarily out of service	150	0.31
Number changed	60	0.12
Cell phone	30	0.06
Business, govt. office, other organization	3,744	7.63
No eligible respondent	826	1.68
Total	**14,506**	**29.54**
TOTAL PHONE NUMBERS USED	**49,100**	**100.0**
AAPOR Response Rate		
Response Rate 3		**26%**

H. Data Preparation and Processing

Data cleaning and quality control checks were automatically performed during the interviewing process on the CATI system. Final cleaning runs checked all questionnaire logic and relationships among items.

I. Weighting

The basic survey design for the FTC Identity Theft Study consisted of the following: The study sampled U.S. adults, 18 years or older, by calling a random sample of U.S. telephone households. Through a series of screening questions, the respondent was identified as either a victim of identity theft or not. If the respondent was a victim, he or she completed an extensive interview. A random portion of respondents who were not victims were asked a series of demographic questions. Those that were not asked these questions were thanked and no further questions were asked.

Sample weights were constructed based on the survey design to provide unbiased estimates for total national demographics and for victims of identity theft. The sample weights include a design weight – the correction for the random selection of non-victims to be asked demographic questions and a post-stratified adjustment weight to correct for different rates of contact and cooperation among different age groups, genders, educational groups, race/ethnicity groups and regions.

The design weights were calculated using the information in the following table. The goal is to recreate an unbiased national sample representative of the U.S. population. The total sample of 4,916 respondents would be an unbiased national sample. By including the design weights, the 1,496 respondents for whom demographic information was collected are also an unbiased national sample.

Sample Subgroups	Number in Sample[2]	Number in Sample with Demographic Information	Design Weight to adjust for sub-sampling
Identity Theft Victims (including minor victims)	915	915	915/915 = 1.000000
Non-identity Theft Victims	4,001	581	4001/581=6.886403
Total	4,916	1,496	--

The next step is to produce a final weight using post-stratified adjustments to account for different contact and cooperation rates among different demographic groups. The post-stratified adjustment used iterative proportional fitting to marginal population distributions for Gender, Age, Race, Region, and Hispanic Ethnicity within Region. This methodology is also referred to as sample balancing, raking or rim weighting. For this study, the estimates from the March 2005 Supplement of the Current Population Survey were used as the population marginal distribution.

[2] In total, 4,917 individuals were contacted and completed the screening portion of the survey. In retrospect, one respondent did not answer appropriately, so they were subsequently dropped. This reduced the total sample to 4,916 completed screens with 915 respondents reporting Identity Theft for themselves or a minor child in the household.

The target population percentages for Gender, Age, Race, Region, and Hispanic Ethnicity within Region are summarized in the following table.

	Region	Population Percentage
1	Northeast	18.89
2	Midwest	22.34
3	South	36.03
4	West	22.74

	Age	Population Percentage
1	18 to 24	12.86
2	25 to 34	18.09
3	35 to 44	19.95
4	45 to 54	19.31
5	55 to 64	13.59
6	65 plus	16.20

	Gender	Population Percentage
1	Male	48.29
2	Female	51.71

	African-American	Population Percentage
1	Yes	11.88
0	No	88.12

	Asian	Population Percentage
1	Yes	4.54
0	No	95.46

	Native American	Population Percentage
1	Yes	1.69
0	No	98.31

	Region	Hispanic Origin	Population Percentage
1	Northeast	Yes	1.96
2		No	16.59
3	Midwest	Yes	1.20
4		No	21.08
5	South	Yes	5.03
6		No	31.06
7	West	Yes	6.18
8		No	16.90

White		Population Percentage
1	Yes	82.03
0	No	17.97

An additional marginal was set based on an interim review of the data. This review revealed that some respondents were considering credit card fraud as identity theft. The questionnaire was adjusted to isolate credit card fraud only and this adjusted questionnaire was fielded using nationally representative replicates. Based on these interviews, a marginal distribution of credit card only victims, other victims and non-victims was created, summarized as:

- 7.1% - Existing Credit Card only victims,
- 10.7% - All other victims, and
- 82.2% - Non-victims

These percentages were used as the targets for the final marginal in the post-stratification adjustments to the weights.

The distribution of the final weights is summarized in this table.

N	Mean	Sum	Standard deviation	Minimum	Maximum
1,496	3.2861	4,916	4.57382	0.03103	55.4446

APPENDIX B: DROP-OUT AND REFUSED REPORT

As with any survey of a sample of a population, the results of this survey may differ from what one would find if all adult Americans – the population covered by this survey – were interviewed. There are a number of reasons for this. First, uncertainty is introduced because only a sample of the population was interviewed and their experiences may differ somewhat from those of others in the relevant population. Perhaps a smaller or larger percentage of this particular group of individuals experienced ID theft than was true of the population as a whole. The degree of uncertainty resulting from the use of a sample rather than a census is a function of the number of people who were asked a particular set of questions and is captured by standard statistical methods in standard errors of the estimates which are included in the figures on the prevalence of the various types of ID theft.

However, additional problems can arise because not everyone who was asked to participate in the survey agreed to do so. In addition, some of those who began the survey failed to complete it. The results reported in the body of this study are based on the responses of those who participated in and completed the survey. Therefore, if the experiences of either those who refused to participate in the survey or those who failed to complete the survey differ from the experiences of those who completed the survey, the results will not be completely representative of the population as a whole in ways that are not captured in the number of interviews completed and the standard errors of the estimates. This appendix preliminarily considers how the inability to include these two groups in the survey may have affected the results – particularly the estimates of the prevalence of ID theft.

Incomplete Interviews

As shown in the Methodology Report in Appendix A, 5,270 interviews were begun, and of these, 353 were not completed. Of these 353 people, 79 completed enough of the interview to allow determination of whether they had ever been a victim of ID theft and, if so, the type of ID theft they experienced – that is, they participated at least through Q9; 274 did not complete enough of the survey to be able to determine whether or not they had ever been victims of ID theft. By comparing the prevalence figures based on only the 4,916 completed interviews with the figures based on both complete interviews and the 79 interviews that were incomplete but provide enough information to determine whether the person had ever experienced ID theft, one can get some idea of how the failure to complete the interview affected the results This assumes that those who quit after Q9 also are representative of those who quit prior to Q9.

As shown in Table 1, inclusion of these incomplete interviews does result in a slightly higher measure of the percentage of people who have experienced some form of ID theft at some point in their lives – 19.5 percent with the incomplete interviews included compared to 18.5 percent including only the completed interviews.[1] Similar increases – a few tenths of a percentage point – are found for each of the three types of ID theft.

Refused to Participate

[1] The figures in this appendix cannot be compared with the figures in the body of the report. There are at least two reasons for this. First, these data measure the percentage of people whose survey answers indicated that they had been a victim of ID theft at some point in their lives, not just in 2005. Second, the data here are not weighted to adjust for differences between those who were interviewed and the population at large.

A second problem that can cause the results of a survey to differ from the actual experiences of the population being surveyed is the fact that not everyone who is asked to participate agrees to do so. Indeed, as shown in the Methodological Report, the response rate for this survey was 26 percent. While steps, including the use of random digit dialing to locate survey participants, were used to ensure that the sample was as random as possible, if those who did not agree to participate differ in some relevant way from those who were actually interviewed, the survey results may not reflect the actual experiences of the population as a whole.

In order to get some idea of possible differences between those who refused to participate in the survey and those who did participate, the contractor persuaded a sample of 100 people who were unwilling to participate in the survey to answer a few questions – including the questions about whether the person had ever been a victim of ID theft. (This sample is referred to as the "Conversion Sample.") Comparing the prevalence figures for these 100 people to those of the people who did agree to participate in the survey can provide some measure of any possible bias introduced by the fact that not everyone was willing to participate in the survey.

Table 1 contains the relevant figures for the Conversion Sample as well as for the complete and incomplete interviews. In general, the responses of the Conversion Sample suggest that those who refused to participate in the survey may be somewhat more likely to have experienced ID theft than those who agreed to participate in the survey.[2] However, one must be careful in drawing conclusions from these data. The Conversion Sample consists of only 100 observations and the observed differences are not statistically significant.

Table 1: Comparison of Prevalence of ID Theft, Complete Interviews Only, Complete and Incomplete Interviews, and Conversion Partial Interviews, Ever a Victim

	Complete Interviews Only	**Complete & Incomplete Interviews**	**Conversion Sample**
Victim of Any Kind of ID Theft	18.5%	19.5%	25.0%
Only Misuse of an Existing Credit Card	8.9%	9.2%	11.0%
Misuse of Other Existing Accounts	5.1%	5.6%	6.0%
New Accounts & Other Frauds	4.5%	4.8%	8.0%
n =	4,916	4,995	100

Note. The data in this table cannot be compared with the data in the body of the report for at least two reasons. First, these data measure the percentage of people who indicate that they have been a victim of ID theft at some point in their lives, not in 2005. Second, the data here are not weighted to adjust for differences between those who were interviewed and the population at large.

[2] Again, these figures are unweighted and reflect whether the person had ever experienced ID theft. Therefore, they cannot be compared directly with the figures in the body of the report.

APPENDIX C: QUESTIONNAIRE

FEDERAL TRADE COMMISSION
INCIDENCE OF IDENTITY THEFT STUDY

2006 Identity Theft Survey Instrument

Hello, I'm ..... of Synovate. I am calling on behalf of the Federal Trade Commission, a U.S. government agency that enforces a number of consumer protection laws. We are conducting a research survey today. We are not selling anything, and no sales calls will be made. The survey is anonymous and you will not be asked for any personal information.

(READ ONLY IF NECESSARY:) For your information, under the Paperwork Reduction Act, as amended, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. For this survey, that number is 3084 - 0124.

A. In order to interview the right person, I need to speak with the member of your household who is aged 18 or over and has had the most recent birthday. Would that be you?

1. YES (**CONTINUE TO QUESTION 1**)
2. NO

IF QA:2 (NO) THEN ASK:

May I please speak to the person in your household who is 18 years of age or older and has had the most recent birthday?

IF THAT PERSON IS NOT HOME, THEN ASK:

When would be a convenient time for me to call him or her back?

(REPEAT INTRODUCTION AND QUESTION A WITH NEW RESPONDENT)

10. Have you ever been notified by a company, government agency, or other organization that it had lost your personal information, such as an account number or your social security number, or that the information had been stolen or hacked?

1. Yes
2. No – **SKIP TO Q13a**
3. Don't Know – **SKIP TO Q13a**
4. Refused – **SKIP TO Q13a**

If Q10:1, Read: **IF YOU RECEIVED MORE THAN ONE NOTIFICATION ABOUT THE LOSS OR THEFT OF YOUR INFORMATION, PLEASE THINK ABOUT THE MOST RECENT NOTIFICATION YOU RECEIVED IN ANSWERING THE NEXT FIVE QUESTIONS.**

10a. When did you receive that notification?

1. Since the beginning of 2006
2. In the last 6 months of 2005
3. In the first 6 months of 2005
4. In 2004
5. In 2003
6. In 2002
7. In 2001
8. Before 2001
9. Don't know
10. Refused

10aa. Did the notification indicate that your Social Security Number was included in the information that was lost or stolen?

1. Yes
2. No
3. Don't Know
4. Refused

12. After receiving this notification, did you do anything about the loss or theft of your information?

    1. Yes
    2. No – **SKIP TO Q11**
    3. Don't Know – **SKIP TO Q11**
    4. Refused – **SKIP TO Q11**

13. What did you do about the loss or theft of your information after receiving this notification? Did you (**INSERT AND RANDOMIZE) (CAN BE MULTIPLES.)**

    1. Consult a lawyer or other professional
    2. Contact the company or agency that sent the notification
    3. Place a fraud alert on your credit report
    4. Close or put a password on your affected accounts
    5. Contact the State Attorney General or a state or local consumer agency
    6. Contact your local police or the local police in another jurisdiction
    7. Contact the government agency that issued the identification number that was lost or stolen, such as contacting the DMV if your drivers license number was lost or stolen

    (**ALWAYS ASK IN THIS ORDER**)
    9. Contact the Federal Trade Commission
    10. Contact another federal agency (SPECIFY)_____ (CAN BE MULTIPLES).

    11. (**ASK LAST**) Or contact someone else (SPECIFY)_____.
    12. Don't Know
    13. Refused

11. Did you discover that someone had misused your information after you received the notification?
    1. Yes
    2. No
    3. Don't Know
    4. Refused

13a. Have you gotten any free annual credit reports since December 1, 2004?

1. Yes
2. No – **SKIP TO INSTRUCTION BEFORE Q1**
3. Don't Know – **SKIP TO INSTRUCTION BEFORE Q1**
4. Refused – **SKIP TO INSTRUCTION BEFORE Q1**

13b. How many free annual credit reports did you get?

1. One
2. Two
3. Three
4. More than three
5. Don't know
6. Refused

(IF "YES" ON Q10, READ: "Now I would like to learn about any actual misuse of your information whether in connection with the data breach we discussed earlier or as a separate incident.")

1. Has anyone ever placed charges on you existing credit card account without your permission?

1. Yes
2. No
3. Don't know
4. Refused

2. **(THERE IS NO Q2)**
3. **(THERE IS NO Q3)**
4. (**THERE IS NO Q4**)
6. (THERE IS NO Q6)

7. Has anyone ever placed charges on or taken money from any of your existing accounts OTHER THAN a credit card account without your permission? This could include misusing an existing wireless telephone account or an ATM or check card to take money from your banking account.

1. Yes
2. No
3. Don't know
4. Refused

(ASK IF Q1 = 1 OR IF Q7 = 1; ELSE GO TO Q8)

5. Did someone change the billing address or have themselves added as an authorized user of . . . ?
(READ. ENTER SINGLE RESPONSE FOR EACH TYPE OF ACCOUNT.)
1. **(READ IF Q1 = 1)** any of the credit card account(s) that were misused, or
2. **(READ IF Q7 = 1)** any of the existing account(s) that were misused OTHER THAN credit card accounts

8. Has anyone ever opened NEW credit card accounts, bank accounts, or other accounts using your personal information such as your Social Security number or date of birth without your permission?

1. Yes
2. No
3. Don’t Know
4. Refused

9. Has anyone ever used your personal information without your permission for some other fraudulent purpose, such as giving your information to the police when they were cited for a traffic violation or charged with a crime; obtaining government benefits, medical care, or a job; or renting an apartment or house?

1. Yes
2. No
3. Don’t Know
4. Refused

IF “YES” ON Q1, Q7, Q8, OR Q9, ASK Q14; OTHERWISE GO TO QD5 BEFORE Q69

14. I would like to learn some more about the misuse of your personal information. This might include the misuse of any of your existing accounts, the opening of new accounts, or any

other fraud committed using your personal information. First of all, has your personal information been MISUSED within the last five years?

1. Yes
2. No
3. Don't Know
4. Refused

15. Can you tell me when you DISCOVERED that your personal information had been misused? (**READ LIST IF NECESSARY. ENTER SINGLE RESPONSE.**) **(INTERVIEWER NOTE: IF "DON'T KNOW" OR "REFUSED," PROBE:** Please give me your best estimate.)

1. Since the beginning of 2006
2. In the last 6 months of 2005
3. In the first 6 months of 2005
4. In 2004
5. In 2003
6. In 2002
7. In 2001
8. Before 2001 **- SKIP TO QD5 BEFORE Q69**
9. Don't know - **SKIP TO QD5 BEFORE Q69**
10. Refused - **SKIP TO QD5 BEFORE Q69**

16. From the time the misuse of your information first began, how long did it take you to discover it was being misused? **(READ LIST IF NECESSARY. ENTER SINGLE RESPONSE.)**

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 less than 2 years
8. 2 years to less than 3 years
9. Or, 3 years or more
10. Don't know
11. Refused

17. Has the misuse of your personal information stopped, or is someone still misusing your personal information?

1. Misuse has stopped
2. Still Misusing information – **SKIP TO Q21**
3. Don't Know – **SKIP TO Q21**
4. Refused – **SKIP TO Q21**

18. **(THERE IS NO Q18)**

19. Is the misuse of your personal information still causing you problems? For example, are you still spending time clearing up your accounts or your credit report? Or, have you managed to resolve all of the problems caused by the misuse of your information?

1. Still experiencing problems – **SKIP TO Q21**
2. All problems resolved
3. Did not experience any problems – **SKIP TO Q21**
4. Don't know – **SKIP TO Q21**
5. Refused – **SKIP TO Q21**

20. Can you tell me how long it took you to resolve the problems after you discovered that your information was being misused? (**READ LIST IF NECESSARY. ENTER SINGLE RESPONSE.**)

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 less than 2 years
8. 2 years to less than 3 years
9. Or, 3 years or more
10. Don't know
11. Refused

21. How did you first find out someone had misused your personal information? Was it…(**READ AND RANDOMIZE**)? (**ENTER SINGLE RESPONSE.**)

1. By monitoring your accounts
2. When notified by your credit monitoring service
3. When notified of unusual account activity **(PROG NOTE: ALWAYS ASK 3 AFTER 2 AND 4.)**
4. When contacted by a debt collector
5. When you received a bill you did not owe
6. When you applied for credit, employment, or other services or benefits
7. When you reviewed your credit report
8. (**ASK LAST AND ONLY IF PERSON DOES NOT SELECT ONE OF RESPONSES 1 - 7.**) Or, did you find out some other way? (SPECIFY) _____
9. Don't know
10. Refused

IF Q21:1 – "By monitoring your accounts" – ask Q21a; ELSE GO TO Q23

21a. You said that you first discovered someone had misused your personal information by monitoring your accounts. Was that through: (**READ AND RANDOMIZE. ENTER SINGLE RESPONSE**.)?

1. Paper statements
2. The Internet, an ATM, or other electronic means
3. Don't know
4. Refused

22. (THERE IS NO Q22)

23. Was the person who misused your personal information… (**READ AND RANDOMIZE LIST UNTIL AN ANSWER IS GIVEN. ENTER SINGLE RESPONSE**.)?

1. Someone you don't personally know (**ALWAYS READ FIRST; PAUSE BEFORE GOING ON**)
2. A Family Member or Relative **(IF YOU ARE ASKED, THE DEFINITION INCLUDES PRESENT & FORMER FAMILY MEMBERS, INCLUDING IN-LAWS AND STEP-FAMILY MEMBERS)**
3. A co-worker who you know
4. A Friend, Neighbor or In Home Employee
5. (**ASK LAST AND ONLY IF THE PERSON DOES NOT SELECT ONE OF RESPONSES 1-4**) Or someone else (**SPECIFY**)_____
6. Don't know
7. Refused

IF Q23: 1, 5, 6, or 7, ASK Q25; OTHERWISE SKIP TO Q24

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

1. Yes
2. No – **GO TO INSTRUCTION BEFORE Q29**
3. Don't know – **GO TO INSTRUCTION BEFORE Q29**
4. Refused – **GO TO INSTRUCTION BEFORE Q29**

26. How was your personal information obtained? Was it stolen (**READ AND RANDOMIZE**)? (**ENTER SINGLE RESPONSE.**)

1. From your wallet or checkbook
2. From your postal mail
3. As a result of a fraudulent change of address
4. From *your* garbage
5. During a purchase or other transaction
6. From your employer
7. From someone hacking into *your* computer
8. As a result of a scam e-mail that you responded to
9. From an office or company that had your personal information in its files
10. (**ASK LAST AND ONLY IF PERSON DOES NOT SELECT ONE OF RESPONES 1-9**) Or, was it obtained some other way (**SPECIFY**)_____
11. I don't know how my information was obtained
12. Refused

24. Did any police or government official inform you that the person who stole your information was . . .?
(READ ITEMS A – B IN ORDER. READ ITEM B, "CONVICTED," WHETHER THE PERSON SAYS "YES" OR "NO" TO ITEM A, "CAUGHT". READ ITEM C ONLY IF THE ANSWER TO ITEM A = "YES" AND THE ANSWER TO ITEM B = "NO" RECORD YES/NO FOR EACH ITEM A – C THAT IS ASKED.)

	Yes	No	DK	Ref
A. Caught				
B. Convicted				
C. Not prosecuted				

IF Q23 = 2,3,4, ASK Q26a AND POP-IN RESPONSE FROM Q23, THEN GO TO INSTRUCTION BEFORE Q29.
IF Q23 = 1,5,6 OR 7, AND Q26 = 1 THROUGH 10, READ Q26b, AND POP-IN RESPONSE FROM Q26.
IF Q26 = 11 OR 12, SKIP TO INSTRUCTION BEFORE Q29

26a. Can you briefly explain how you know that [READ RESPONSE TO Q23] misused your personal information? (**RECORD RESPONSE VERBATIM**)

26b. Can you briefly explain how you know that your personal information was obtained [READ RESPONSE TO Q26] [IFQ26 = 10, READ "in the way you described]? (**RECORD RESPONSE VERBATIM**)

IF Q26:5 – "During a purchase or other transaction" – ASK Q27. ELSE GO TO INSTRUCTION BEFORE Q29

27. You indicated that your information was obtained during a purchase or other transaction. Was the transaction **(READ AND RANDOMIZE)**? (**ENTER SINGLE RESPONSE.**)

1. An Online purchase
2. An In store purchase
3. A Mail Order or telephone purchase
4. An Online financial transaction such as checking your account balances or paying bills
5. (**ASK LAST AND ONLY IF PERSON DOES NOT SELECT ONE OF RESPONSES 1-4**)
   Or, Some other type of transaction (**SPECIFY**) _____
6. Don't know
7. Refused

IF Q26:9 – "From an office or company that had your personal information in its files" – ASK Q27a. ELSE GO TO INSTRUCTION BEFORE Q29

27a. You indicated that your information was obtained from **an office or company that had your personal information in its files**. Was the person who stole the information someone who had been employed by that office or company?

1. Yes
2. No
3. Other (Specify) _____ (**DO NOT READ**)
4. Don't know
5. Refused

28. (THERE IS NO Q28)

ASK Q29 - Q31 IF "YES" TO Q7; OTHERWISE GO TO INSTRUCTIONS BEFORE Q32

29. You said that one or more of your **existing** accounts, **other than credit card** accounts, had been misused. Did the person run up charges on, take money from, or otherwise misuse, any of the following accounts? (READ AND RANDOMIZE) **(ENTER SINGLE RESPONSE FOR EACH ACCOUNT**.)

ACCOUNTS:
Checking or Savings Accounts, including misuse of an ATM or debit card
Medical Insurance Accounts
Internet or Email Accounts
Telephone Accounts, Whether Conventional or Cell Phone
Email Payments Accounts, such as Paypal or Bidpay
Other accounts (SPECIFY)_____

30. **(THERE IS NO Q30)**

31. **ASK IF YES TO CHECKING OR SAVINGS ACCOUNT ON Q29. ELSE, SKIP TO INSTRUCTION BEFORE Q32.** You said that one or more of your **checking or savings** accounts had been misused. How did the person take money from, make payments from, or otherwise misuse, your checking or savings accounts? Was it ...? **(READ AND RANDOMIZE) (CAN BE MULTIPLES)**

1. By paper transactions, such as checks
2. By card-based transactions, such as an ATM or payment card
3. By electronic transactions, such as an electronic transfer or ACH payment
4. Don't know
5. Refused

(Read: Now I would like to learn more about any NEW accounts that may have been opened, rather than existing accounts that you already had that were misused.)

32. Did the person use your personal information to obtain any (**INSERT AND RANDOMIZE ACCOUNTS**)

1. New Credit Card Accounts
2. New Checking or Savings Accounts
3. New Loans
4. New Medical Insurance Policies
5. New Automobile Insurance Policies
6. New Email payments Accounts, such as Paypal or Bidpay
7. New Telephone Accounts, Whether Conventional or Cell Phone
8. (**ASK LAST**) Other new accounts (SPECIFY)_____

(**FOR EACH TYPE OF ACCOUNT FOR WHICH THE PERSON ANSWERS "YES" ON Q32, ASK Q33**)

33. How many (**INSERT ACCOUNT**) were obtained using your information?

1. #_____ (**VALID RANGE 1 TO 25**)
2. Don't know
3. Refused

IF Q1 is NOT EQUAL TO YES AND Q7 IS NOT EQUAL TO YES AND Q8 IS NOT EQUAL TO YES AND THERE AREN'T ANY YES RESPONSES TO Q32, SKIP TO INSTRUCTION BEFORE Q34.

35. Were any of the existing accounts that were misused or new accounts that were opened joint accounts with your spouse or another adult?

1. Yes **(GO TO Q35a)**
2. No **(GO TO INSTRUCTION BEFORE Q33a)**
3. Don't know **(GO TO INSTRUCTION BEFORE Q33a)**
4. Refused **(GO TO INSTRUCTION BEFORE Q33a)**

35a. Do you know whose name was used when the joint account or accounts were misused? Was it: (READ CODES 1 – 4)

1. Only your name that was used
2. Only the name of the other person on the account that was used
3. The names of both persons were used
4. Someone else's name was used
8. Don't know
9. Refused

IF "Yes" on any of the accounts identified in Q32 and Q8:2, 3, or 4, ASK; ELSE GO TO INSTRUCTION BEFORE Q34:

33a. I notice that you just said that [**INSERT RESPONSE(S) TO Q32 TO WHICH THE PERSON ANSWERED "YES"**] had been opened using your personal information. However, when we asked earlier if someone had used your personal information to obtain NEW credit cards, bank accounts, loans or other accounts, you answered [**INSERT RESPONSE TO Q8**]. Can you briefly explain why you answered these two questions in this way? (**RECORD RESPONSE VERBATIM**)

IF "YES" to Q7, Q8, OR Q9, ASK Q34; ELSE GO TO Q36.

34. As far as you know, did the person use your information in any of the following ways? Did the person **(INSERT AND RANDOMIZE) (CAN BE MULTIPLES)**?

1. File a fraudulent tax return
2. Obtain medical treatment, services, or supplies
3. Obtain employment
4. Provide your identifying information to law enforcement when they were stopped or charged with a crime
5. RENT an apartment or house
6. Obtain government benefits, such as Social Security, Medicare, Disaster Relief, Food Stamps, etc.
7. (**ASK LAST**) Use your information in any other way (**SPECIFY**)_____.
8. Don't Know
9. Refused

(IF "Yes" on any of the fraudulent uses identified in Q34 and Q9:2, 3, or 4, ASK Q34a; ELSE GO TO Q36:

34a. I notice that you just said that your personal information had been used to [**INSERT RESPONSE(S) TO Q34 TO WHICH THE PERSON ANSWERED "YES"**]. However, when we asked earlier if someone had used your personal information for some other fraudulent purpose, such as to obtain government documents, medical care, or a job, you answered [**INSERT RESPONSE TO Q9**]. Can you briefly explain why you answered these two questions in this way? (**RECORD RESPONSE VERBATIM**)

36. What is the approximate total dollar value of what the person obtained while misusing your information? In answering this question, include the value of credit, loans, cash, services, and anything else the person may hav e obtained.

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

IF PERSON SAYS DON'T KNOW OR DECLINES TO PROVIDE AN AMOUNT ON Q36, ASK Q37; ELSE GO TO INSTRUCTION BEFORE Q67:

37. Can you tell me whether (READ RESPONSES 1-3 IN ORDER. ENTER SINGLE RESPONSE)

1. The thief got $1,000 or more – **GO TO Q40**
2. The thief got less than $1,000, or – **GO TO Q39**
3. You don't know if the thief got more or less than $1,000 – **GO TO INSTRUCTION BEFORE Q67**
4. Refused – **GO TO INSTRUCTION BEFORE Q67**

38. DELETE Q38

39. Was the value

1. Less than $100
2. $100 - $499
3. $500 - $999
4. Don't know
5. Refused

GO TO INSTRUCTION BEFORE Q67

40. Was the value

1. $1,000 - $4,999
2. $5,000 - $9,999
3. $10,000 - $24,999
4. $25,000 - $49,999
5. $50,000 - $99,999
6. $100,000 or more
7. Don't know
8. Refused

IF "YES" ON Q35, THEN READ: You indicated that one or more of the accounts that were misused or opened were joint accounts with another adult. In answering the rest of the questions, please consider both actions taken or amounts paid by yourself and by the person with whom you held the joint accounts.

67. What other types of problems, IF ANY, have you experienced as a result of the misuse of your personal information? Have you (**INSERT AND RANDOMIZE**)?

1. Been turned down for a loan
2. Had banking problems, such as being turned down for a checking account, or having checks rejected
3. Had credit problems, such as being turned down for a credit card, or having a card rejected
4. Had phone or utilities cut off, or been denied new service
5. Been turned down for insurance or had to pay higher rates
6. Been harassed by a debt collector or collections department
7. Had a lawsuit filed or a judgment entered against you
8. Been the subject of a criminal proceeding
9. Had to repeatedly correct the same information on your credit reports
10. (**ASK LAST**) Had any other types of problems (**SPECIFY**) _____
11. Don't know
12. Refused

41. How much money did you pay out of your pocket as a result of the misuse of your personal information? In thinking about this answer, include costs for things such as lost wages, legal fees, or payment of any fraudulent debts. Also include miscellaneous expenses such as postage, and notarizing documents.

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

IF RESPONSE IS $0, GO TO Q48
IF PERSON GIVES AN AMOUNT GREATER THAN $0, GO TO INSTRUCTION BEFORE Q46
IF PERSON SAYS DON'T KNOW OR DECLINES TO PROVIDE AN AMOUNT ON Q41, ASK Q42:

42. Would you say out of your own pocket you had to pay… (**READ RESPONSES 1 TO 3 IN ORDER, ENTER SINGLE RESPONSE.**)

    1. $500 or more – **GO TO Q45**
    2. Less than $500, or – **GO TO Q44**
    3. You don't know if you had to pay more or less than $500 – **GO TO INSTRUCTION BEFORE Q46**
    4. Refused – **GO TO INSTRUCTION BEFORE Q46**

43. DELETE Q43

44. Was the amount

1. $0 – **(GO TO Q48)**
2. Less than $50 **(GO TO INSTRUCTION BEFORE Q46)**
3. $50 - $99 **(GO TO INSTRUCTION BEFORE Q46)**
4. $100 - $499 **(GO TO INSTRUCTION BEFORE Q46)**
5. Don't know **(GO TO INSTRUCTION BEFORE Q46)**
6. Refused **(GO TO INSTRUCTION BEFORE Q46)**

45. Was the amount

1. $500 - $999
2. $1,000 - $4,999
3. $5,000 - $9,999
4. $10,000 or more
5. Don't know
6. Refused

IF Q1 = 1, ASK Q46; ELSE GO TO Q47

46. How much, if any, did your credit card company require you to pay in connection with the unauthorized purchases on your card? **(READ LIST IF NECESSARY. ENTER SINGLE RESPONSE**) (**IF OVER $1,000, PROBE**: I just want to verify that the total amount is (**INSERT AMOUNT RESPONDENT INDICATED**)?

1. Nothing
2. $1 to $49
3. $51 - $99
4. $100 - $249
5. $250 - $499
6. $500 - $999
7. $1,000 or more
8. Don't know
9. Refused

47. Did you pay any money to a debt collection agency to resolve any unauthorized purchases or expenditures?

1. Yes
2. No
3. Don't know
4. Refused

48. How many hours of your own time have you spent resolving credit, financial, and other problems caused by the theft of your information? In estimating the amount of time you spent, please include any time that you spent at work and any time spent while on leave from work. **(INTERVIEWER: CODE ANYTHING LESS THAN ONE HOUR AS "1")**

    1. RECORD EXACT NUMBER OF HOURS. _____. (**IF OVER 80 HOURS, PROBE**: I just want to verify that the total amount is (**INSERT NUMBER OF HOURS RESPONDENT INDICATED**)

IF PERSON SAYS DON'T KNOW OR DECLINES TO PROVIDE A NUMBER OF HOURS ON Q48, ASK Q49; ELSE GO TO Q53:

49. To resolve any problems you had, would you say that you had to spend. **(READ CODES 1 – 3 IN ORDER; RECORD SINGLE RESPONSE)**

    1. 40 hours or more – **GO TO Q52**
    2. Less than 40 hours, or – **GO TO Q51**
    3. You don't know if it took more or less than 40 hours to resolve these problems – **GO TO Q53**
    4. Refused – **GO TO Q53**

50. DELETE Q50

51. Was the number of hours **(READ CODES 1 – 3; RECORD SINGLE RESPONSE)**

    1. 1 hour or less
    2. 2 to 9 hours
    3. 10 to 39 hours
    4. Don't know
    5. Refused

GO TO Q53

52. Was the number of hours **(READ CODES 1 – 4; RECORD SINGLE RESPONSE)**

    1. 40 to 79 hours
    2. 80 to 159 hours
    3. 160 to 239 hours
    4. 240 hours or more
    5. Don't know
    6. Refused

53. Did you contact anyone – such as a credit card company, a local police department, a credit bureau, or a lawyer– in attempting to report the theft or misuse of your personal information or resolve the problems caused by the misuse of your information?

1. Yes - **GO TO Q54**
2. No – **GO TO INSTRUCTIONS BEFORE Q53a**
3. Don't know – **GO TO INSTRUCTION BEFORE Q68**
4. Refused – **GO TO INSTRUCTION BEFORE Q68**

IF Q7 = 1 OR Q8 = 1, OR Q9 = 1, ASK Q53a;
IF Q41 IS $1 OR MORE AND Q46 = CODES 2 – 7, ASK Q53a;
IF Q48 = 2 OR MORE, ASK Q53a.

ELSE GO TO INSTRUCTION BEFORE Q68

53a. Can you briefly explain why you did not contact anyone to report the misuse of your personal information or resolve any problems that it caused? I am particularly interested in why you did not contact your local police department or the credit reporting agencies. (**RECORD RESPONSE VERBATIM**)

GO TO INSTRUCTION BEFORE Q68

54. Did you contact **(INSERT AND RANDOMIZE)**? **(CAN BE MULTIPLES)**

1. A lawyer or other professional
2. One or more Credit Reporting Agencies
3. The Department of Motor Vehicles
4. The Better Business Bureau
5. A consumer group, such as National Consumers League or Call for Action
6. One or more companies where an account was opened or misused, including a credit card issuer
7. The State Attorney General or a state or local consumer agency
8. Your local police or the local police in another jurisdiction
9. The insurance company where you have identity theft insurance

(**ALWAYS ASK IN THIS ORDER**):

10. The Federal Trade Commission
11. Another federal agency (**SPECIFY**)_____.
12. (**ASK LAST**) Someone else (**SPECIFY**)_____.
13. Don't Know
14. Refused

IF Q54:8 – "Notify your local police or the local police in another jurisdiction – IS "YES," GO TO Q55. ELSE GO TO NEXT INSTRUCTION.

IF Q7 = 1 OR Q8 = 1, OR Q9 = 1, ASK Q54a;
IF Q41 IS $1 OR MORE AND Q46 = CODES 2 – 7, ASK Q54a;
IF Q48 = 2 OR MORE, ASK Q54a.
ELSE GO TO INSTRUCTION BEFORE Q58

Q54a: I'd like to learn more about why identity theft victims do not report to the police. Can you briefly explain why you did not contact your local police or the local police in another jurisdiction? (**RECORD RESPONSE VERBATIM**)

GO TO INSTRUCTION BEFORE Q58.

55. Did the police take a police report from you about the misuse of your information?

1. Yes
2. No – **GO TO 57**
3. Don't know – **GO TO 57**
4. Refused – **GO TO 57**

56. Did you get a copy of the report?

1. Yes
2. No
3. Don't know
4. Refused

57. How satisfied were you with the response of your local police when you reported that your personal information had been misused? (**READ LIST. ENTER SINGLE RESPONSE**.)

4. Very Satisfied
3. Somewhat Satisfied
2. Somewhat Dissatisfied, or
1. Very Dissatisfied
5. Don’t Know
6. Refused

IF Q57:1 OR 2; ASK Q57a; OTHERWISE GO TO INSTRUCTION BEFORE Q58

57a. Can you briefly explain why you were [INSERT RESPONSE TO Q57] with the response of your local police? (RECORD RESPONSE VERBATIM)

IF Q54:3 – "Notify the Department of Motor Vehicles, Q54:7 – "Notify the State Attorney General or a state or local consumer agency," OR Q54:10 – "Notify another federal agency," ASK Q58; OTHERWISE GO TO INSTRUCTION BEFORE Q60

58. Did the **[POP-IN "Department of Motor Vehicles if Q54:3, "State Attorney General or state or local consumer agency" if Q54:7 or "Federal agency" if Q54:10]** you contacted take a report about the misuse of your personal information?

1. Yes
2. No – **GO TO INSTRUCTION BEFORE Q60**
3. Don't know – **GO TO INSTRUCTION BEFORE Q60**
4. Refused – **GO TO INSTRUCTION BEFORE Q60**

59. Did you get a copy of the report?

1. Yes
2. No
3. Don't know
4. Refused

(ASK Q60 IF Q54:2 – "Notify one or more credit reporting agencies;" IF Q54 DOES NOT :2, ASK 66a)

60. You indicated that you notified one or more credit reporting agencies. How many credit reporting agencies did you contact? (**ENTER SINGLE RESPONSE**.)

1. One
2. Two
3. Three, or
4. More than three
5. Don't know
6. Refused

IF Q60 = 1, ASK Q62; ELSE GO TO Q63.

62. How many, if any, additional credit reporting agencies contacted you after you notified the one agency? (**ENTER SINGLE RESPONSE**.)

1. None
2. One
3. Two
4. Three, or
5. More than three
6. Don’t know
7. Refused

63. Were “temporary” or initial 90-day fraud alerts placed on your credit reports at the credit reporting agencies you contacted or that contacted you? **(DO NOT READ LIST. ENTER SINGLE RESPONSE.) (IF CLARIFICATION NEEDED, “INITIAL 90-DAY” FRAUD ALERTS MIGHT HAVE BEEN CALLED “TEMPORARY” FRAUD ALERTS AND MIGHT HAVE LASTED MORE THAN 90 DAYS PRIOR TO 2005.)**

1. Yes
2. No – **GO TO Q66**
3. Don't Know – **GO TO Q66**
4. Refused – **GO TO Q66**

64. (THERE IS NO Q64)

65. Were any new accounts opened after the initial 90-day fraud alerts were placed on your credit reports? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE**.)

1. Yes
2. No
3. Don't know
4. Refused

66. Have you placed 7-year or permanent fraud alerts on your credit reports? **(IF CLARIFICATION NEEDED, "7-YEAR" FRAUD ALERTS MAY ALSO BE CALLED "PERMANENT" FRAUD ALERTS)**

1. Yes
2. No
3. Don't Know
4. Refused

61. Did you place a freeze on your credit reports at the credit reporting agencies you contacted? That is, did you tell any of the credit reporting agencies to not share your credit report with anyone, such as a potential creditor, unless you "unfreeze" it for that specific purpose?

1. Yes
2. No
3. Don't Know
4. Refused

IF Q53 does not :2 "No, did not contact anyone," and Q54 DOES NOT :2 – "Notify one or more credit reporting agencies;" ask Q66a

Q66a: I would like to know more about why identity theft victims do not notify credit reporting agencies. Can you briefly explain why you did not contact any credit reporting agencies? (**RECORD RESPONSE VERBATIM**)

ASK Q68 IF Q48 is 10 HOURS OR GREATER OR IF Q50:1 OR Q51:3

68. What was the hardest part of your experience with the misuse of your personal information? (**RECORD VERBATIM. PROBE FOR CLARIFICATION. IF RESPONDENT IS UNSURE, ENCOURAGE BEST GUESS**)

ASK IF Q1 = 1 AND Q7 IS NOT EQUAL TO YES AND Q8 IS NOT EQUAL TO YES AND Q9 IS NOT EQUAL TO YES.

Q68b. Which of the following best describes the misuse of your existing credit card? **(READ, RANDOMIZE CODES 1 – 4; ACCEPT ONE MENTION ONLY)**

1. A company I had given my card or card number to charged me for a product that I had not agreed to purchase
2. A company I had given my card or card number to charged me more or for something different than what I had agreed to purchase
3. I gave my card number to someone who claimed to be with a company where I had an account and they used it to obtain cash, goods, or services for themselves
4. Someone took my card or card number and used it to obtain cash, goods, or services for themselves
5. Other (SPECIFY)
6. Don't know
7. Refused

QD5. How many people in your household are:

1. Under 18 years old. Record exact number _____ **(IF 0, GO TO INSTRUCTIONS BEFORE QD1.)**
2. Between 13 and 17. Record exact number _____
3. Refused

IF ANSWER TO QD5 IS "ONE" OR MORE, ASK Q69. ELSE, GO TO INSTRUCTIONS BEFORE QD1.

69. Has any member of your household who is currently under the age of 18 experienced any form of misuse of their personal information?

1. Yes
2. No -**GO TO INSTRUCTION BEFORE QD1**
3. Don't Know - **GO TO INSTRUCTION BEFORE QD1**
4 .Refused - **GO TO INSTRUCTION BEFORE QD1**

69a. How many members of your household currently under the age of 18 have experienced any form of misuse of their personal information?

1. #_____ (VALID RANGE 1 - 6)

IF 69a: ONE, READ Q70; IF 69a: TWO OR MORE, READ Q70a
IF Q69A IS DON'T KNOW OR REFUSED, READ Q70A

70. How long ago was it first discovered that the minor's personal information had been misused?

70a. For the minor who most recently discovered that their personal information was being misused, how long ago was the misuse first discovered? **(USE ANSWERS BELOW FOR WHICHEVER QUESTION IS ASKED)**

1. Since the beginning of 2006
2. In the last 6 months of 2005
3. In the first 6 months of 2005
4. In 2004
5. In 2003
6. In 2002
7. In 2001
8. Before 2001
9. Don't Know
10. Refused

71. (THERE IS NO Q71)

ASK QD1 – QD9 if Q1=1, Q7=1, Q8=1, Q9=1, OR Q69=1.

ASK QD1 – QD9 OF A RANDOM SAMPLE OF 600 OTHER SURVEY PARTICIPANTS.

IF Q1 NOT EQUAL TO YES, AND Q7 NOT EQUAL TO YES AND Q8 NOT EQUAL TO YES AND Q9 NOT EQUAL TO YES AND Q69 NOT EQUAL TO YES, AND NOT SELECTED FOR DEMOGRAPHICS, THANK AND TERMINATE.

Now, for statistical purposes only

QD1. May I please have your age as of your last birthday? (**DO NOT READ LIST UNLESS RESPONDENT HESITATES**)

1. Under 25
2. 25 to 34
3. 35 to 44
4. 45 to 49
5. 50 to 54
6. 55 to 59
7. 60 to 64
8. 65 to 69
9. 70 to 74
10. 75 to 84
11. 85 or older
12. Refused

QD2. What was the last grade of school you completed? (**DO NOT READ**)

1. Completed grade school or less
2. Some high school, not completed
3. Completed high school
4. Some college, not completed
5. Completed college
6. Post graduate work (such as a masters degree, PhD, MD or law degree, whether started or completed)
7. Refused

QD3. Are you married?

1. Yes
2. No
3. Refused

QD4. How many people live in your household at the present time? Please include yourself and any children.

1. Record exact number _____
2. Refused

QD6. Are you of Hispanic or Latino origin?

1. Yes
2. No
3. Don't know
4. Refused

QD7. I am going to read a list of racial categories. Please choose one or more categories that best indicates your race. Are you? **(READ AND RANDOMIZE 1 – 5. ENTER YES/NO FOR EACH. IF PERSON REFUSES TO ANSWER ON FIRST TWO RACES READ, CODE "REFUSED" ON REMAINING RACES AND SKIP TO QD8)**

1. White
2. Black or African American
3. American Indian or Alaska Native
4. Asian
5. Native Hawaiian or Other Pacific Islander
6. Some other race **(ASK ONLY IF NO OR DK OR REF TO ALL PARTS 1 - 5)**
7. Don't Know
8. Refused

QD8. Now I would like to read a series of income groups. Please stop me when I read the group which describes your total household income, from all sources, over the past year.

1. Under $15,000
2. $15,000 to less than $20,000
3. $20,000 to less than $25,000
4. $25,000 to less than $30,000
5. $30,000 to less than $40,000
6. $40,000 to less than $50,000
7. $50,000 to less than $75,000
8. $75,000 to less than $100,000
9. $100,000 or more
10. Don't know
11. Refused

QD9. What is your gender? (By Observation)
1. Male
2. Female

THANK THE PERSON FOR THEIR PARTICIPATION AND TERMINATE