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 - Identity Theft Survey Report

Prepared for Federal Trade Commission

Prepared by Synovate

September, 2003

Table of Contents

Methodology

The Federal Trade Commission (FTC) sponsored a survey of US adults on the topic of Identity Theft and the resulting experiences of victims. The specific objectives of the study were:

- Estimate the incidence of Identity Theft Victimization
- Measure the impacts of Identity Theft on the victims
- Identify actions taken by victims
- Explore measures that may help victims of future cases of Identity Theft

The study was conducted using interviews conducted by telephone. Synovate's omnibus survey - TeleNation - was the data collection vehicle. TeleNation uses a Random-Digit-Dialing (RDD) sampling methodology to obtain a random sample of US adults age 18 and older. Each administration of TeleNation yields at least 1,000 completed interviews with a nationally representative sample.

Four waves of interviewing were conducted on the following dates:

- March 17-19, 2003
- April 7-9, 2003
- April 14-16, 2003
- April 21-23, 2003

In total, 4,057 interviews with US adults were conducted. A more complete description of TeleNation's procedures is included as an Appendix to this report.

In addition to standard data processing procedures, additional weighting of the data was performed to represent properly respondents who were victims of only the credit card form of Identity Theft. For budgetary reasons, this group was only asked a limited number of questions in the April 21-23 TeleNation survey. To bring this group's responses back into proper proportion, an additional weighting step was conducted.

With the exception of the data on the number of people who discovered that they were victims of ID Theft within the last year, the results contained in this report are for victims who have discovered that their personal information was being misused - that is that they were victims of Identity Theft - within the last 5 years. That is, the results reported are based on people who gave answers 1 through 7 in response to Question 6 of the survey.

Executive Summary

The Incidence of ID Theft

1.5 percent of survey participants reported that in the last year they had discovered that their personal information had been misused to open new credit accounts, take out new loans, or engage in other types of fraud, such as misuse of the victim's name and identifying information when someone is charged with a crime, when renting an apartment, or when obtaining medical care ("'New Accounts & Other Frauds' ID Theft"). This result suggests that almost 3.25 million Americans discovered that their personal information had been misused in this kind of fraud in the past year. (See Table 1.)

2.4 percent of survey participants reported misuse of their information in the last year that was limited to the misuse of one or more of their existing credit cards or credit card account numbers ("Misuse of Existing Credit Cards or Card Numbers"). 0.7 percent of participants reported misuse of one or more of their existing accounts other than credit cards - for example checking or savings accounts or telephone accounts ("Misuse of Existing Non-Credit Card Accounts or Account Numbers").[1]

Including all types of ID Theft, a total of 4.6 percent of survey participants indicated that they had discovered they were victims of ID Theft in the past year. This result suggests that almost 10 million Americans have discovered that they were the victim of some form of ID Theft within the last year.

4.7 percent of survey participants reported that they had discovered that they were victims of "New Accounts & Other Frauds" ID Theft during the previous 5 years. 6.0 percent said that they had discovered that they were victims of the "Misuse of Existing Credit Cards or Card Numbers," while 2.0 percent indicated that they were victims of the "Misuse of Existing Non-Credit Card Accounts or Account Numbers." In total, 12.7 percent of survey participants reported that they had discovered the misuse of their personal information within the last 5 years.

[1] Victims of identity theft are classified as belonging to one of three categories based on the most serious problem the victim reported. For example, victims who reported that a new account had been opened using their information and also that their existing credit cards had been misused were placed in the "New Accounts & Other Frauds" category, not in the "Misuse of Existing Credit Card or Credit Card Number" category. The "New Accounts & Other Frauds" category was considered to be the most serious, followed by "Misuse of Existing Non-Credit Card Account or Account Number." "Misuse of Existing Credit Card or Card Number" was considered the least serious type of victimization.

Table 1: Incidence of ID Theft in the Last Year, By Type of Misuse2

Discovered That You Were a Victim in the Last Year	
New Accounts & Other Fraud [3]	1.5%
Misuse of Existing Non-Credit Card Account or Account Number	0.7 %
Misuse of Existing Credit Card or Credit Card Number	2.4 %
Total Victims	4.6 %
Discovered That You Were a Victim in the Last Five Years	
New Accounts and Other Fraud	4.7 %
Misuse of Existing Non-Credit Card Account or Account Number	2.0 %
Misuse of Existing Credit Card or Credit Card Number	6.0 %
Total Victims	12.7%

2 As explained in footnote 1, each victim is classified as belonging to only one of the categories of ID Theft based on the most serious problem the victim reported. Approximately 65 percent of those who experienced "New Accounts & Other Frauds" ID Theft within the last five years also experienced the misuse of an existing credit card or other account - 22 percent experienced the misuse of an existing credit card, 26 percent experienced the misuse of an existing non-credit card account, and 16 percent experienced both the misuse of existing credit cards and the misuse of existing non-credit card accounts. (The numbers do not add to 65 due to rounding.) Similarly, 40 percent of victims in the "Misuse of Existing Non-Credit Card Account or Account Number" category also experienced the misuse of an existing credit card account.

3 "Other Frauds" include misuse of the victim's information to misrepresent a person's identity when someone is charged with a crime by law enforcement authorities, when renting an apartment or home, when obtaining medical care or employment with the victim's information, and similar misuses.

The Costs of ID Theft

On average, victims of "New Accounts & Other Frauds" ID Theft indicated that the person or persons who misused the victim's personal information had obtained money or goods and services valued at $10,200 using the victim's information. This result suggests that the total loss to businesses, including financial institutions, from this type of ID Theft was $33 billion in the last year.[4] (See Table 2.)

Adding the costs that resulted from "Misuse of Existing Credit Cards and Credit Card Accounts Only" ID Theft and from "Misuse of Other Existing Accounts" ID Theft to those from "New Accounts & Other Frauds," the total cost of this crime approaches $50 billion per year, with the average loss from the misuse of a victim's personal information being $4,800.

Individuals whose information is misused bear only a small percentage of the cost of ID Theft. Nonetheless, looking at all forms of ID Theft, victims estimated that they had spent $500 on average to deal with their ID Theft experience. Victims of the "New Accounts and Other Frauds" type of ID Theft estimated that they had spent almost $1,200 on average. Thus, the total annual cost of ID Theft to its victims appears to be about $5.0 billion, with victims of "New Accounts & Other Frauds" ID Theft bearing $3.8 billion of that total.

Victims of ID Theft also spend a considerable amount of their own time resolving the various problems that occurred because of the misuse of their personal information. On average, victims reported that they spent 30 hours resolving their problems. On average, victims of the "New Accounts and Other Frauds" form of ID Theft spent 60 hours resolving their problems. This suggests that Americans spent almost 300 million hours resolving problems related to ID Theft in the past year, with almost two-thirds of this time - 194 million hours - spent by victims of "New Accounts and Other Frauds" ID Theft.

15 percent of ID Theft victims reported that their personal information was misused in non-financial ways. The most common such use reported was to present the victim's name and identifying information when someone was stopped by law enforcement authorities or was charged with a crime. 4 percent of victims reported that their information was misused in this way.

[4] Victims are generally not liable for losses based on fraudulent actions taken 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 check fraud and loan fraud are typically limited by state statute or common law.

Table 2: Costs of ID Theft in the Last Year[1]

	New Accounts & Other Frauds	Misuse of Existing Accounts (Both Credit Card & Non-Credit Card)	All ID Theft
Victims in the Last Year			
Percent of Population	1.5%	Credit Card - 2.4 % Non Credit Card-0.7%	4.6 %
Number of Persons[2]	3.23 million	6.68 million	9.91 million
Loss to Businesses, inc. Financial Institutions			
Average Per Victim[1]	$10,200	$2,100	$4,800
Total	$32.9 billion	$14.0 billion	$47.6 billion
Loss to Victims			
Average Per Victim	$1,180	$160	$500
Total	$3.8 billion	$1.1 billion	$5.0 billion
Hours Victims Spent Resolving Their Problems			
Average Per Victim	60 hours	15 hours	30 hours
Total	194 million hours	100 million hours	297 million hours

1 Totals by type of ID Theft may not sum to the amount shown in the totals column due to rounding. "Average Per victim" figures in the "All ID Theft" column are a weighted average of the values for the different types of ID Theft with the incidence in the past year used as weights.

2 Based on U.S. population age 18 and over of 215.47 million as of July 1, 2002. (http://eire.census.gov/popest/data/national/tables/asro/NA-EST2002-ASRO-01.php (visited July 14, 2003).

The ID Theft victim's personal information is often misused for a substantial period of time. 13 percent of victims reported that their information was misused for 6 months or more. (For "New Accounts & Other Frauds" ID Theft, 27 percent of cases involved the misuse of the victim's information for at least 6 months.) On the other hand, in 26 percent of all cases of ID Theft the misuse was limited to a single day. (Misuse was limited to a single day in 36 percent of cases that only involved the misuse of existing credit cards or card numbers.)

The Benefits of Quick Discovery

The cost of an incident of ID Theft is significantly smaller if the misuse of the victim's personal information is discovered quickly. When the misuse was discovered within 5 months of its onset, the value obtained by the thief was less than $5,000 in 82 percent of cases (including all forms of ID Theft). When victims took 6 months or more to discover that their information was being misused, the thief obtained $5,000 or more in 44 percent of cases.

The costs to the victim - both in terms of out-of-pocket expense and in time spent resolving problems - are also substantially smaller if the misuse is discovered quickly. No out-of-pocket expenses were incurred by 67 percent of those who discovered the misuse of their personal information within 5 months of the time the misuse began. Where it took 6 months or more to discover the misuse, only 40 percent of victims incurred no out-of-pocket expenses.

New accounts were opened in less than 10 percent of cases when it took victims less than a month to discover that their information was being misused. New accounts were opened in 45 percent of cases when 6 months or more elapsed before the misuse was discovered. At least in part, this result may reflect the fact that quickly discovering that a new account has been created in a person's name may be more difficult than discovering that an existing account is being misused. It may also suggest the likelihood that quick discovery reduces the risk that new accounts will be opened.

In terms of the amount of time spent resolving problems, 76 percent of victims who discovered the misuse of their information within one month spent fewer than 10 hours resolving their problems, while in only 20 percent of cases where it took more than 6 months to discover the misuse were victims able to resolve all of their problems in less than 10 hours.

Reporting ID Theft

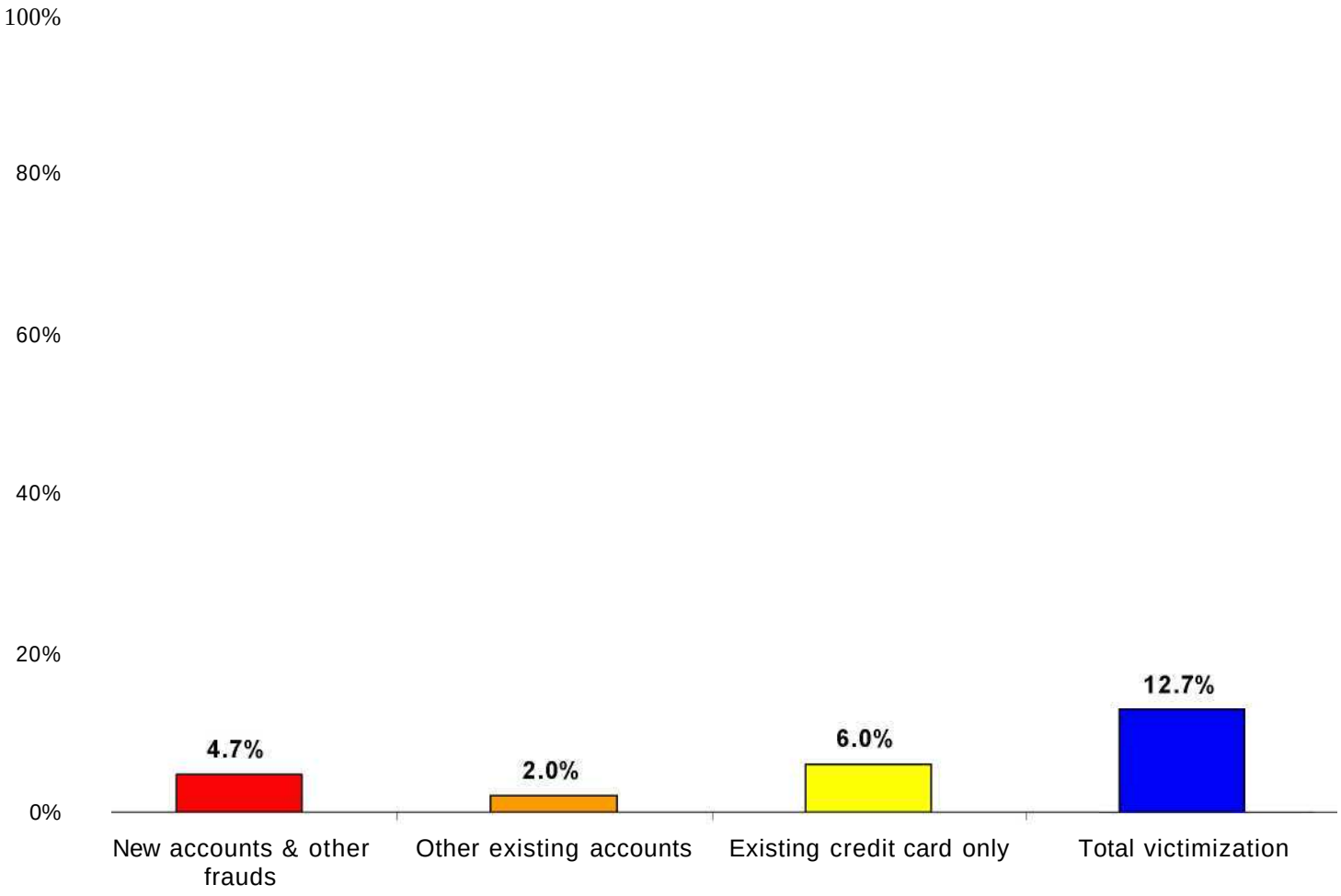
Most victims of ID Theft do not report the crime to criminal authorities. Only about 25 percent of victims who participated in the survey said that they had reported the crime to local police. Even with the more serious "New Accounts and Other Frauds" form of ID Theft, only 43 percent of victims said that they had reported their experiences to local police.

Only 22 percent of ID Theft victims said that they had notified one or more credit bureaus about their experiences. Even among those who suffered from the "New Accounts & Other Frauds" type of ID Theft, only 37 percent contacted a credit bureau. Of those victims who contacted credit bureaus, 62 percent asked to have a "fraud alert" placed on their credit reports.

Theft, including a lost or stolen wallet or pocket book or the theft of a victim's mail, was the most commonly mentioned way of obtaining the victim's personal information. Approximately 25 percent of ID Theft victims reported that their information was obtained through such theft. Approximately one-half of ID Theft victims said that they did not know how the person who misused their personal information obtained it.

Incidence of Identity Theft

Q1 / Q3a / Q4 - Incidence of Identity Theft, Past 5 Years

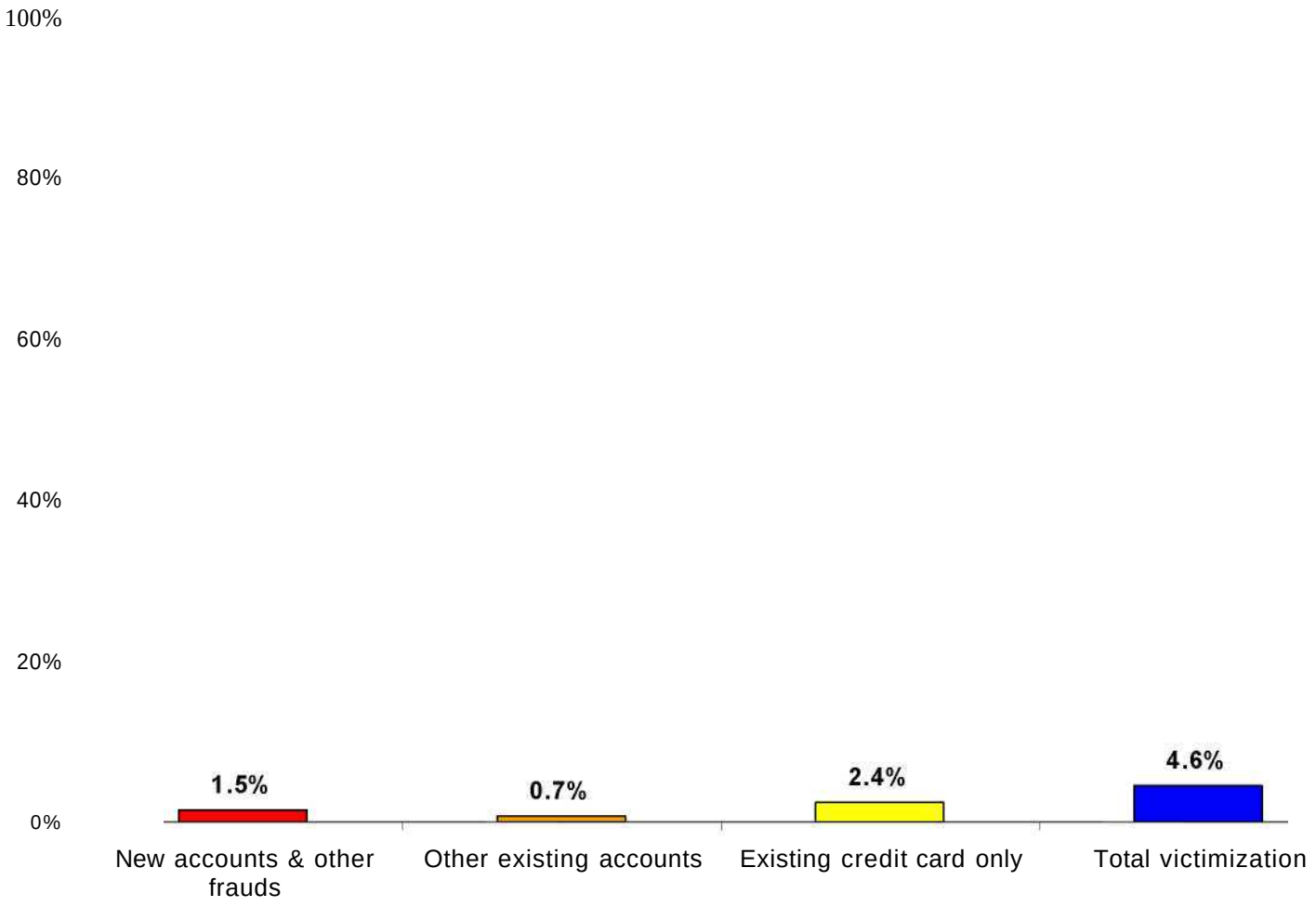


- 4.7% of American adults surveyed said that within the last 5 years they had discovered that they were the victim of an Identity Theft that involved the opening of new accounts or loans or committing theft, fraud, or other crimes using the victim's personal information ("New Accounts & Other Frauds" ID Theft). (Approximately 65% of those who experienced "New Accounts & Other Frauds" ID Theft within the last five years also experienced the misuse of an existing credit card or other account - 22% experienced the misuse of an existing credit card, 26% experienced the misuse of an existing non-credit card account, and 16% experienced both the misuse of existing credit cards and the misuse of existing non-credit card accounts.)
- Within the past 5 years, 2.0% of adults reported having an existing account other than a credit card, such as a checking or savings account or a utility account misused ("Misuse of Existing Non-Credit Card Accounts" ID Theft). (40% of these victims also experienced the misuse of an existing credit card).
- The most commonly reported form of Identity Theft involves the misuse of an existing credit card or credit card number. 6.0% of survey participants indicated they had been the victim of ID Theft, but that the misuse of their information had been limited to the misuse of an

existing credit card or credit card number ("Misuse of Existing Credit Card or Card Number" ID Theft).

- In total, 12.7% of survey respondents reported that within the last five years they had discovered that they were victims of one of the three types of Identity Theft. This implies that approximately 27 million American adults have been victims in this period.
- Non-whites also report slightly higher rates of victimization (16%) than whites (12%).
- Residents of the West Census region were most likely to be victims of Identity Theft within the past 5 years (14%). The crime was found least in the Midwest region (10%) over the same time period. Among respondents from the South, 13% reported experience with Identity Theft; 12% of those in the Northeast region also have been victimized.
- Americans age 55 and over were slightly less likely to report victimization within the past 5 years (9%) than the population as a whole (13%).

Q1 / Q3a / Q4 - Incidence of Identity Theft, Past Year

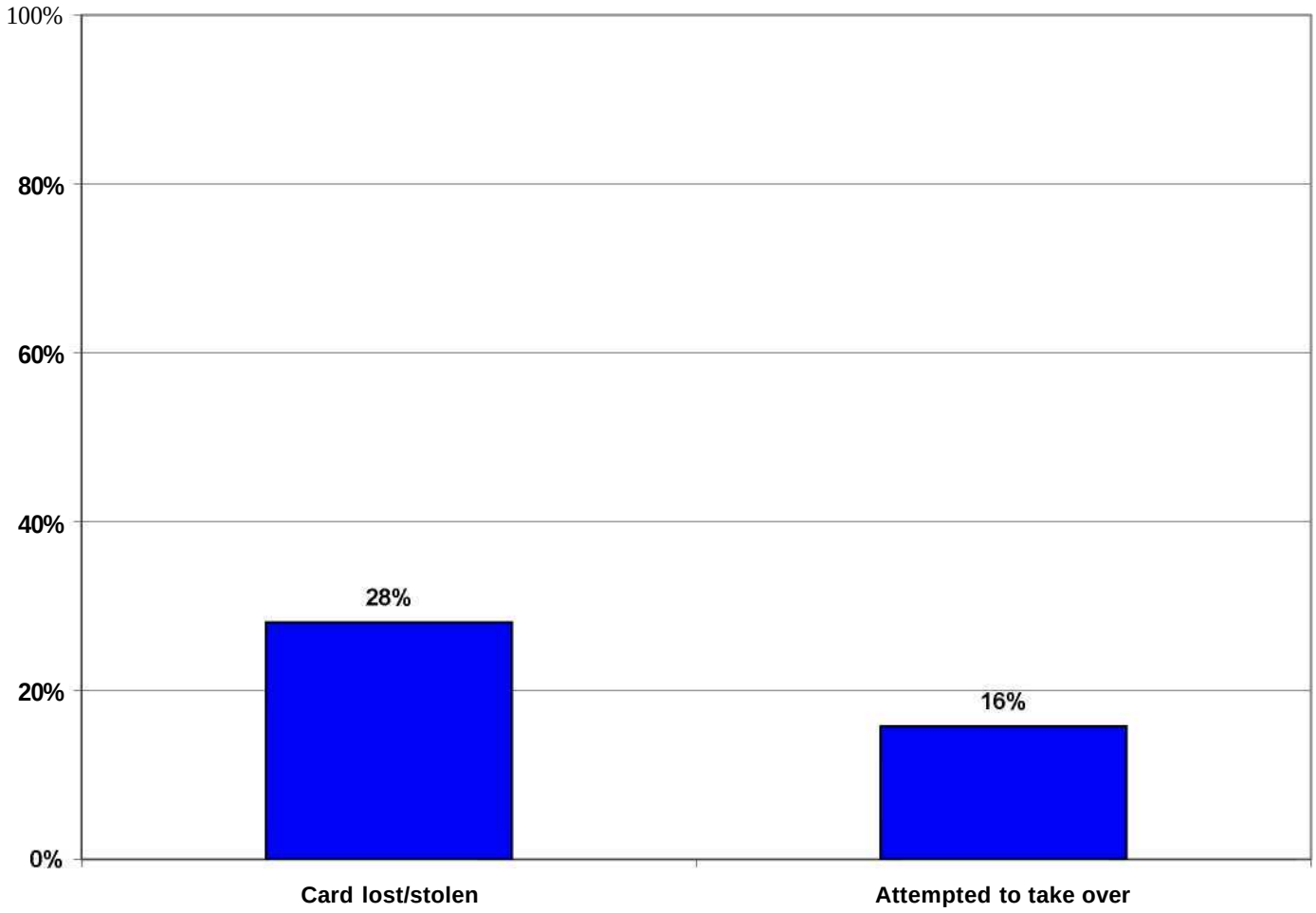


- Within the past year, 1.5% of those surveyed said that they had discovered that their personal information had been misused to open new accounts, to obtain new loans, or to commit theft, fraud, or other crimes. ("New Accounts & Other Frauds" ID Theft) This indicates that almost 3.25 million American adults were victimized in this way within the last year.

- 2.4% of participants indicated that they had discovered that they were victims of the "Misuse of Existing Credit Cards or Credit Card Numbers" within the last year. 0.7% of participants indicated that they had discovered that they were victims of the "Misuse of Existing Non-Credit Card Accounts or Account Numbers" during that period of time.

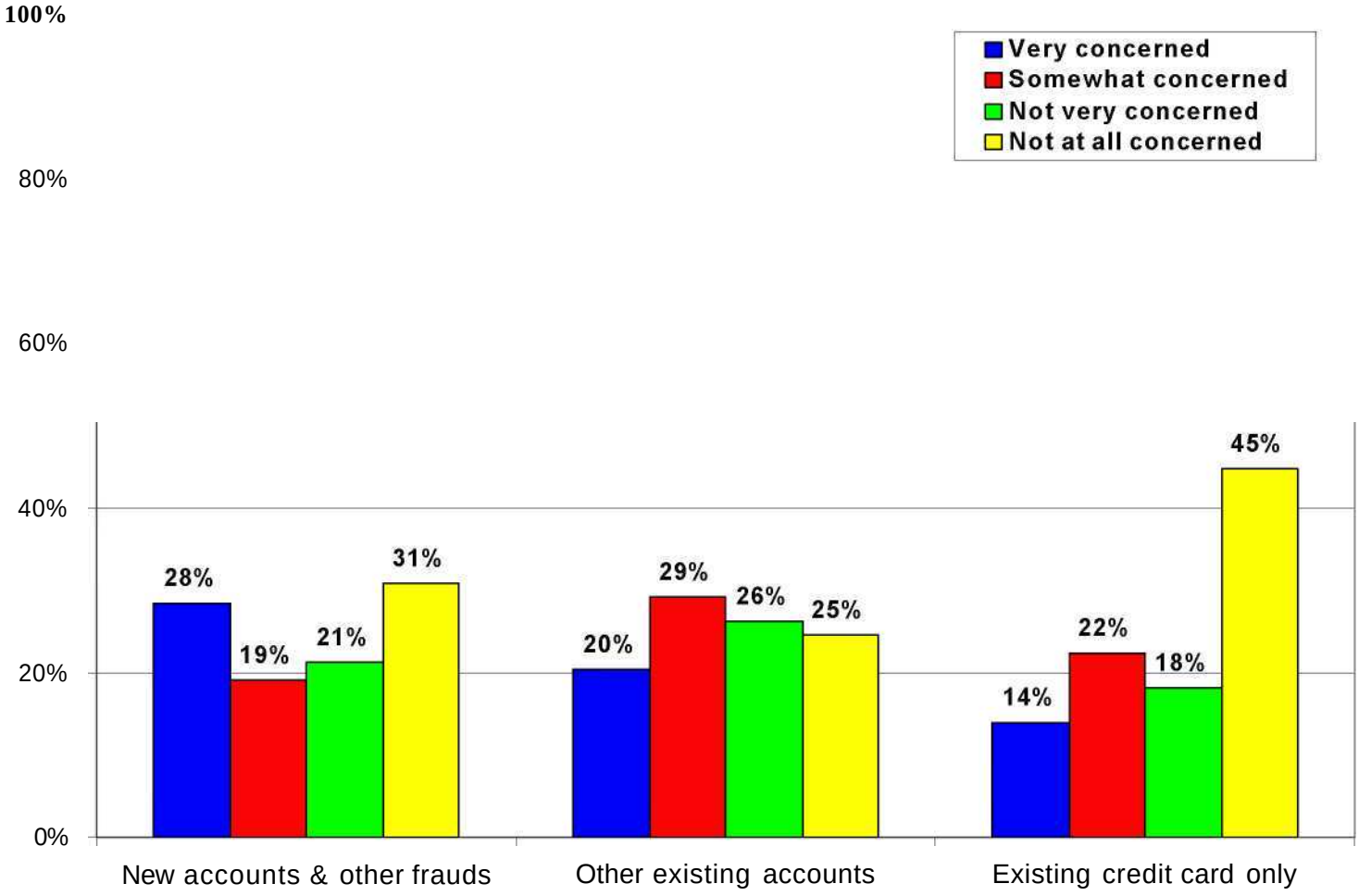
- A total of 4.6% of those who participated in this survey indicated that they had discovered that they were the victim of some form of ID Theft within the last year. This suggests that almost 10 million adults in the United States were victims in the past year.

Q2 / Q3 - Credit card misuse



- 28% of Identity Theft victims whose ID Theft experience included the misuse of existing credit cards said that the misused card had been either lost or stolen.
- 16% of victims who had their existing credit cards misused said that the person who misused their credit card also tried to "take over" the account by doing such things as changing the billing address or adding themselves to the card as an authorized user.

Q43 - Victims' concern about future victimization



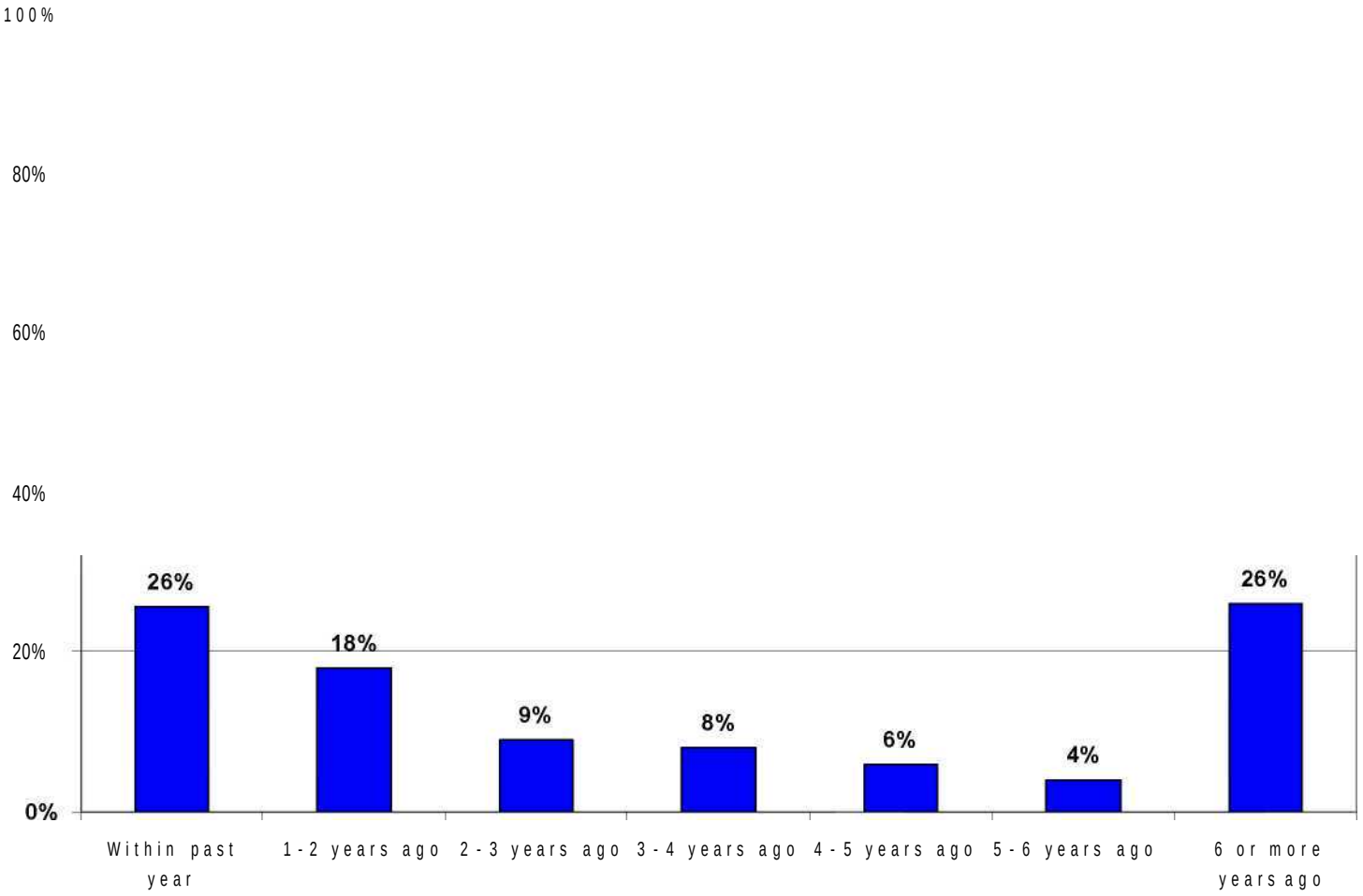
- Victims of Identity Theft are divided in their concern that they will be victims again. Looking at all victims of ID Theft - regardless of the type of misuse they experienced - slightly fewer than half (44%) say they are "very" or "somewhat" concerned that they will be victimized again, while 55% say they are "not very" or "not at all" concerned.
- Those whose personal information was misused to open new accounts or commit other types of fraud ("New Accounts & Other Frauds") are slightly more concerned about future misuse of their information (47% "very" or "somewhat" concerned) than those who only experienced the misuse of an existing credit card (36% "very" or "somewhat" concerned.)
- Non-white victims (53%) are more likely than white victims (40%) to be concerned about future acts of misuse by an identity thief.
- Lower income victims were the most likely to express concern about future victimization (60% of victims whose household incomes were less than $25,000 said that they were "very" or "somewhat" concerned).

- Victims who suffered four or more distinct misuses of their information were more likely to be concerned about future misuse than were victims whose information was not so extensively misused. 68% of those with four or more distinct misuses said that they were "very" or "somewhat" concerned about future misuse, whereas 38% of those with one to three distinct misuses were similarly concerned. (A distinct misuse is the misuse of a particular existing account, the opening of a single new account, or use of a victim's personal information for any of the purposes identified in Q28.)

Time Considerations

Federal Trade Commission

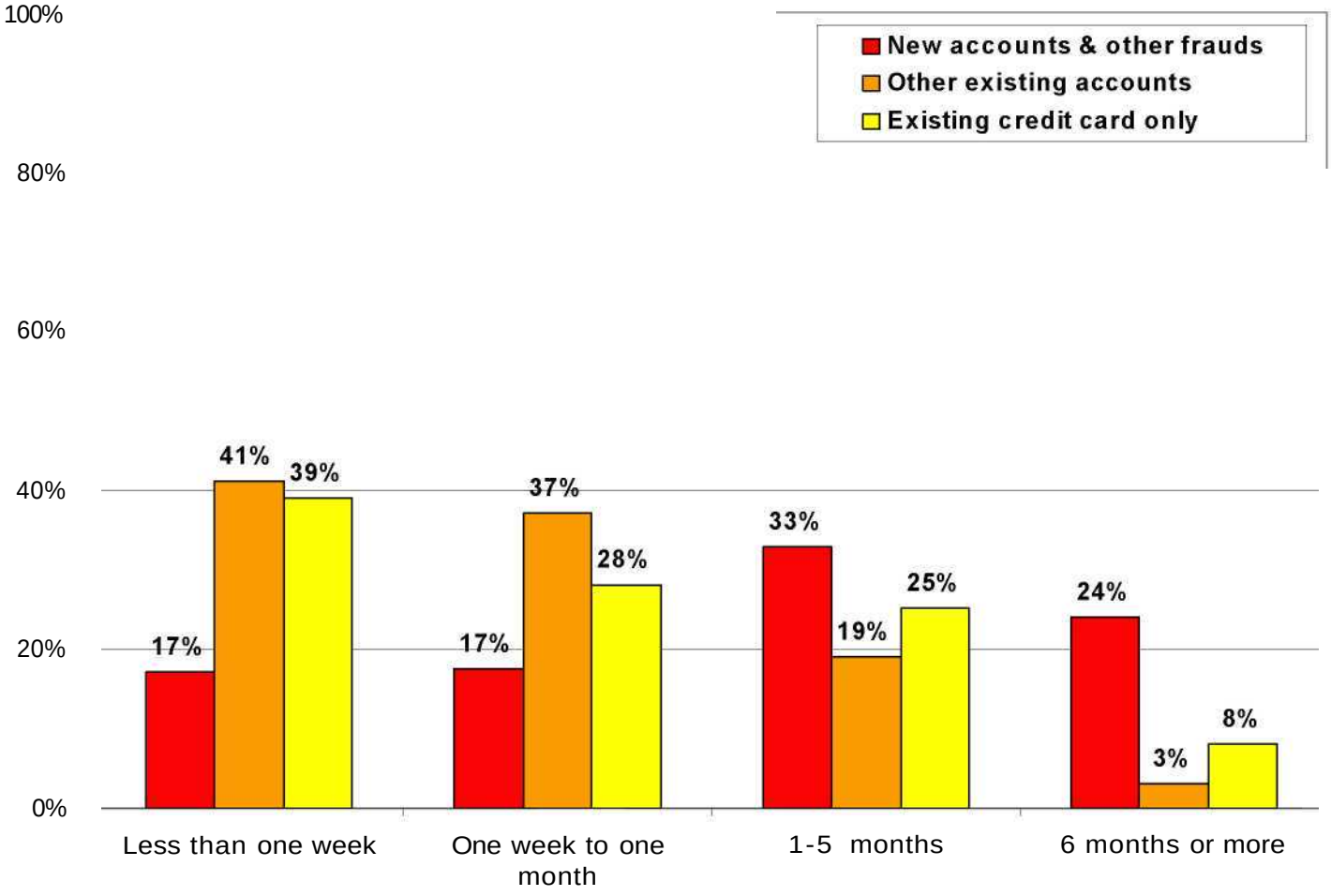
Q6 - Discovery of misuse



- Based on the survey results, it appears that incidents of Identity Theft are on the rise in the US. The trend appears to accelerate with reports of Identity Theft within the past two years.
- Approximately one-quarter of Identity Theft victims found out about the misuse of their information within the past year. This represents approximately 10 million Americans, 4.7% of American adults, who have discovered that they have been a victim of Identity Theft within the past year.
- Another quarter of respondents discovered the misuse of their personal information 6 or more years ago.
- Overall the number of ID Theft victims who reported discovering the misuse of their personal information within the last year was 41 % greater than the number discovering misuse between 1 and 2 years ago. This growth was concentrated in the "Misuse of Existing Credit Card Accounts Only" category, where the rate of growth was 71 %. For "New Accounts & Other Frauds" ID Theft, the number of victims discovering misuse within the last year was essentially unchanged from the year before.

- The number of ID Theft victims who reported discovering the misuse of their personal information between 1 and 2 years ago was almost double that for the period 2 - 3 years ago. Between these two periods, there was substantial growth in all forms of ID Theft.

Q7 - Length of time to discover misuse



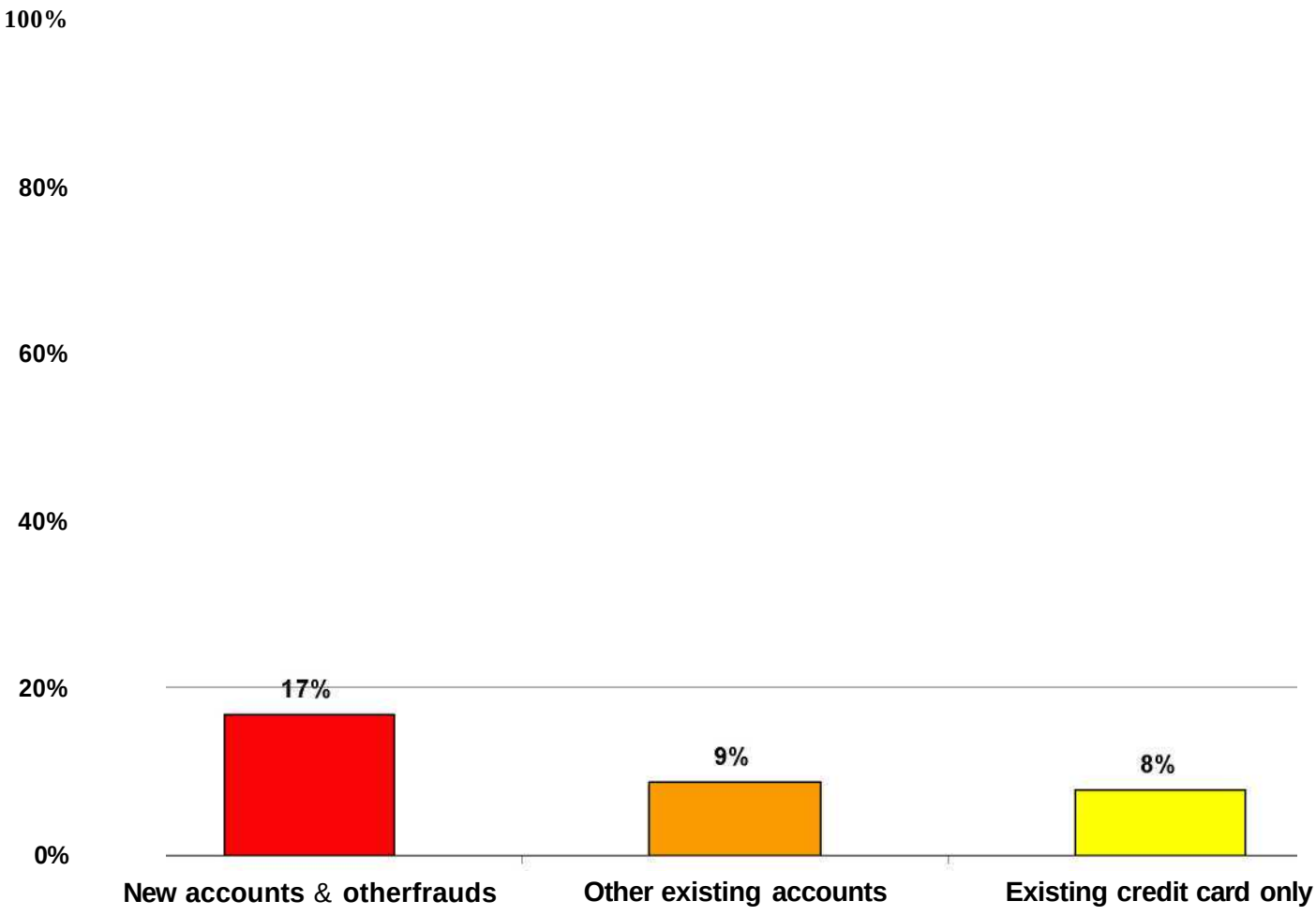
- For approximately one-third of all victims, it took less than one week to discover that their personal information was being misused.
- Discovering the misuse was quickest for people who experienced misuse of existing non-credit card accounts (41% discovered the misuse within one week) or who only experienced the misuse of existing credit cards (39%).
- Victims of "New Accounts & Other Frauds" ID Theft were far less likely to discover the misuse within one week. Only 17% of victims of ID Theft that involved the opening of new accounts and other types of fraud discovered that their information was being misused within a week of the onset of the misuse.
- 26% of all victims discovered the misuse of their information between one week and one month after the time the misuse began.
- 12% of all victims took more than 6 months to discover the misuse. The victims most likely to have discovered the misuse of their information after this lapse of time were those with lower household incomes (19% of households with incomes of under $25,000 took 6

months or more to discover the misuse, compared to just 7% of households with incomes of $75,000 or more). Non-whites (19% of whom took 6 months or more to discover the misuse) and those with lower levels of education (15% of those with a high school education or less took at least 6 months) are also likely to take longer to discover the theft of their information.

- Nearly one-quarter of the victims of "New Accounts & Other Frauds" took 6 months or more to discover the misuse.
- It is likely that the time it takes many victims to uncover the occurrence of Identity Theft is related to the billing cycle for credit cards and other existing accounts. Seeing unauthorized account activity on a billing statement was the most cited way of discovering Identity Theft.

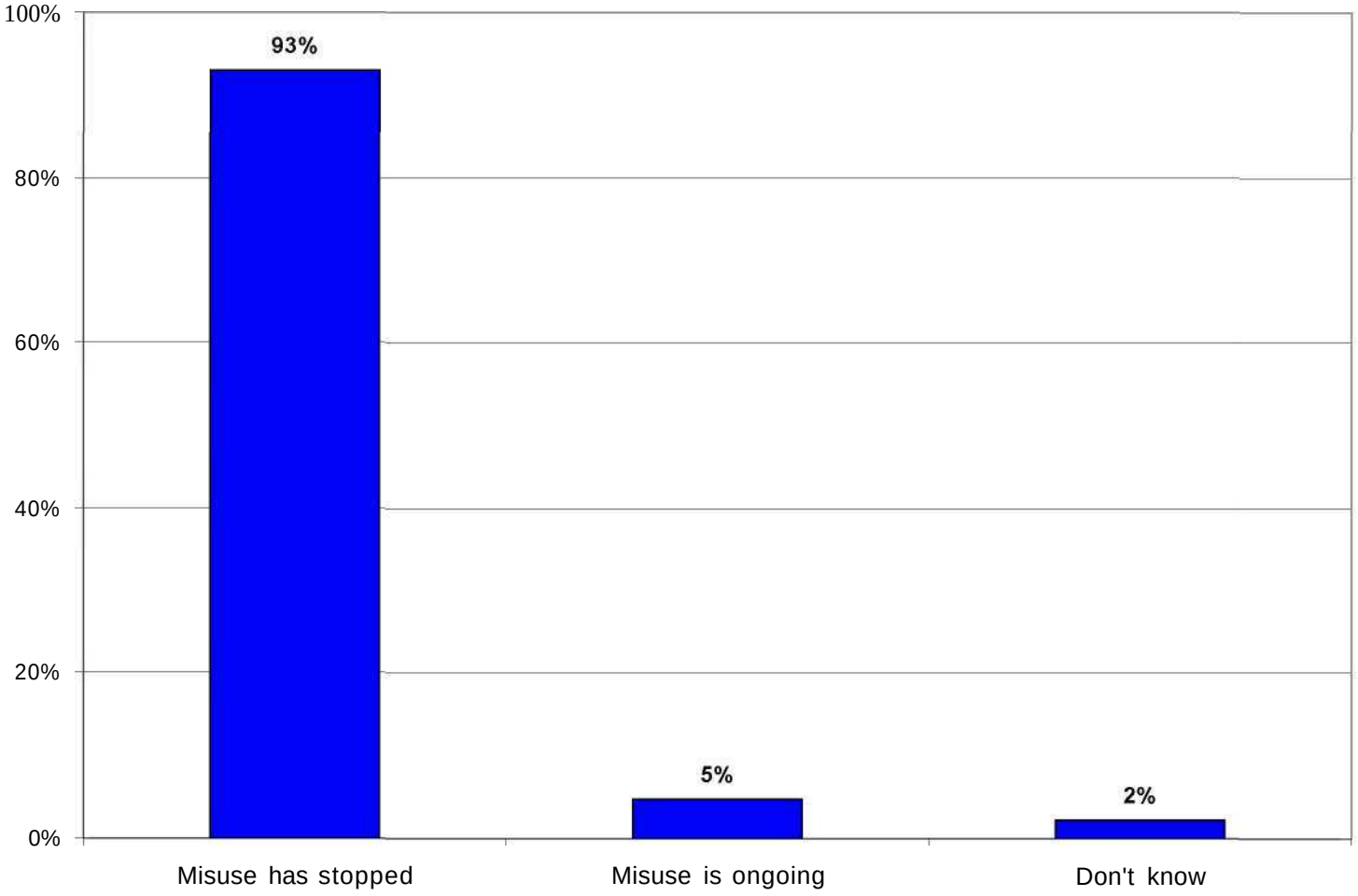
Federal Trade Commission

Q8 - Aware information taken before misuse



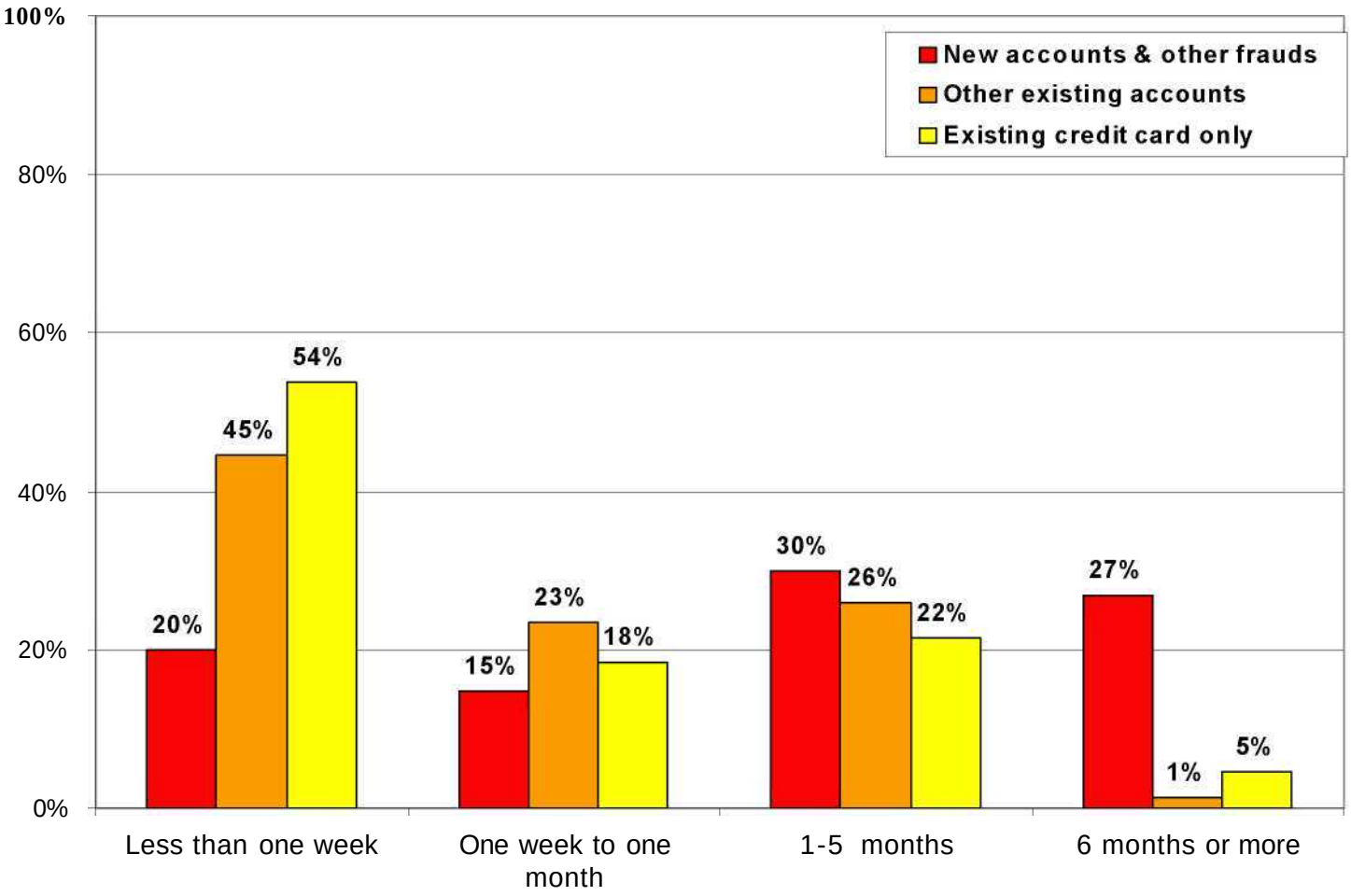
- Just 11 % of respondents said they were aware that their personal information had been taken before discovering they were victims of Identity Theft.
- 8% of those who experienced only the misuse of existing credit cards and 9% of those who experienced the misuse of existing non-credit card accounts were aware their information had been taken before the misuse began. This compares to 17% of victims of "New Accounts & Other Frauds" ID Theft.
- Victims who live in the Northeast (5%) and West (9%) were least likely to say they knew their information had been taken, while victims in the South (15%) and Midwest (14%) were most likely to know.

Q9 - Current status of misuse



- At the time of the survey, 5% of victims were still experiencing misuse of their personal information. Another 2% were not sure if the misuse had stopped.
- Victims who had experienced four or more distinct misuses of their personal information, whether the misuse of an existing account, the opening of a new account, or other types of misuse, were more likely to say that their information was still being misused (13% of these victims were still experiencing misuse of their information and another 4% were unsure whether the misuse had stopped).
- Lower-income victims (those with household incomes of less than $25,000) were also more likely to say that the misuse was ongoing - 8% were being victimized at the time of the survey and another 8% were unsure if the misuse had stopped.

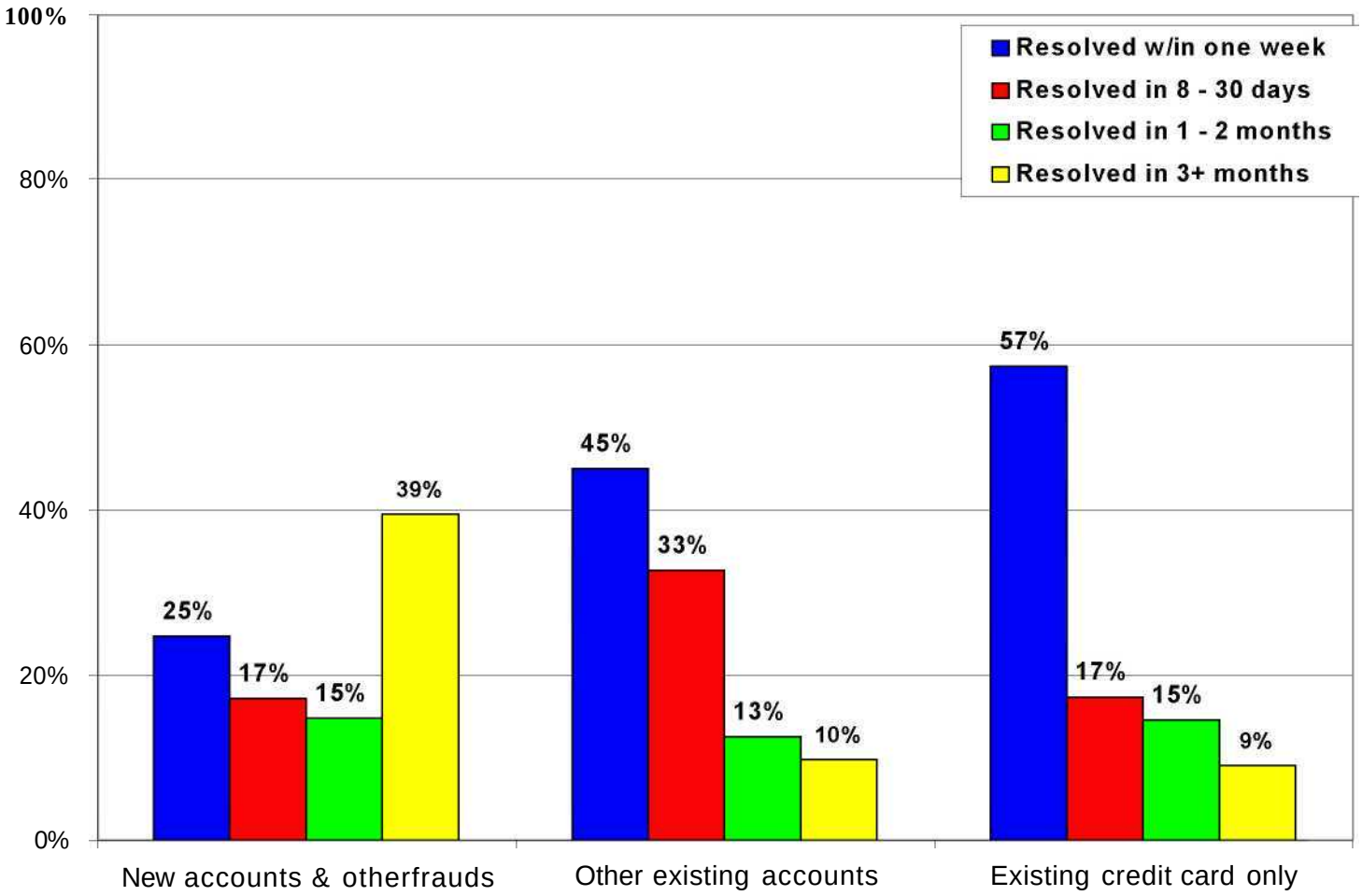
Q10 - Period of misuse



- Considering victims of all types of ID Theft, the median time period that victims say their information was misused is between one week and one month. (That is, 50% of victims said that their information was misused over this amount of time or less and the other 50% said their information was misused at least this long.) The average period of misuse was 3.2 months.
- 25% of all victims said that the misuse of their information occurred only during a single day.
- 12% of all victims reported that their information was misused for more than 6 months.
- 54% of victims who had only existing credit cards misused said that their accounts were misused over a period of less than one week.
- People who have experienced the more serious forms of ID Theft - those who had new accounts opened or other types of fraud committed using their personal information - reported that the misuse took place over a much longer period of time; more than one-quarter of these victimizations lasted 6 months or more.

- Those with lower levels of education are the most likely to report that the misuse of their information lasted 6 months or more (16% of those with only a high school education or less).
- A significant percentage of both lower and middle income households also reported victimization spanning 6 months or more (17% of victims with household incomes below $25,000; 18% of those with incomes between $25,000 and $75,000).

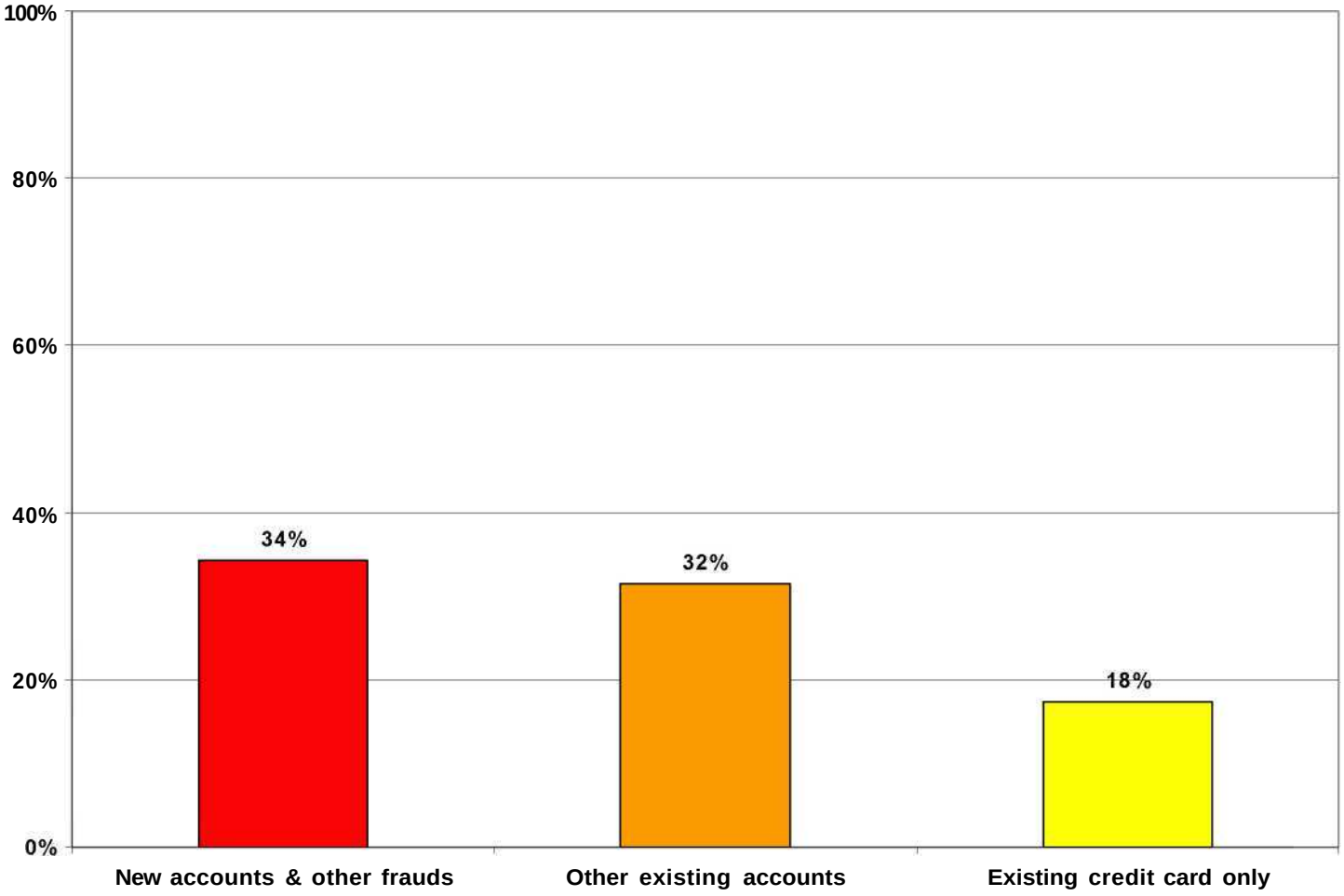
Q11 / Q12 - Problem resolution



- Although just 5% of victims said the misuse of their information was ongoing at the time of the survey, four times that number - 21 % of all Identity Theft victims - said they were still experiencing problems as a result of that misuse. (When asked whether they were still experiencing problems resulting from the misuse of their personal information, 16% of victims said that they had not experienced any problems.)
- Victims who experienced the "New Accounts & Other Frauds" form of ID Theft (34% still experiencing problems), non-whites (30%) and middle income victims (27% of those reporting household incomes of $50,000 - $75,000) were among the most likely to say they were still experiencing problems. Conversely, victims age 55 and over were less likely to still be experiencing problems (12% still experiencing problems).
- Overall, one quarter of all victims who had resolved all problems were able to do so within a single day. Among victims who only experienced the misuse of existing accounts - whether credit card accounts or other accounts - 32% were able to resolve their problems in a single day.
- The median time required to resolve problems was between one week and one month.

Offenders' Means of Access

Q14 / Q15 - Awareness of identity of thief



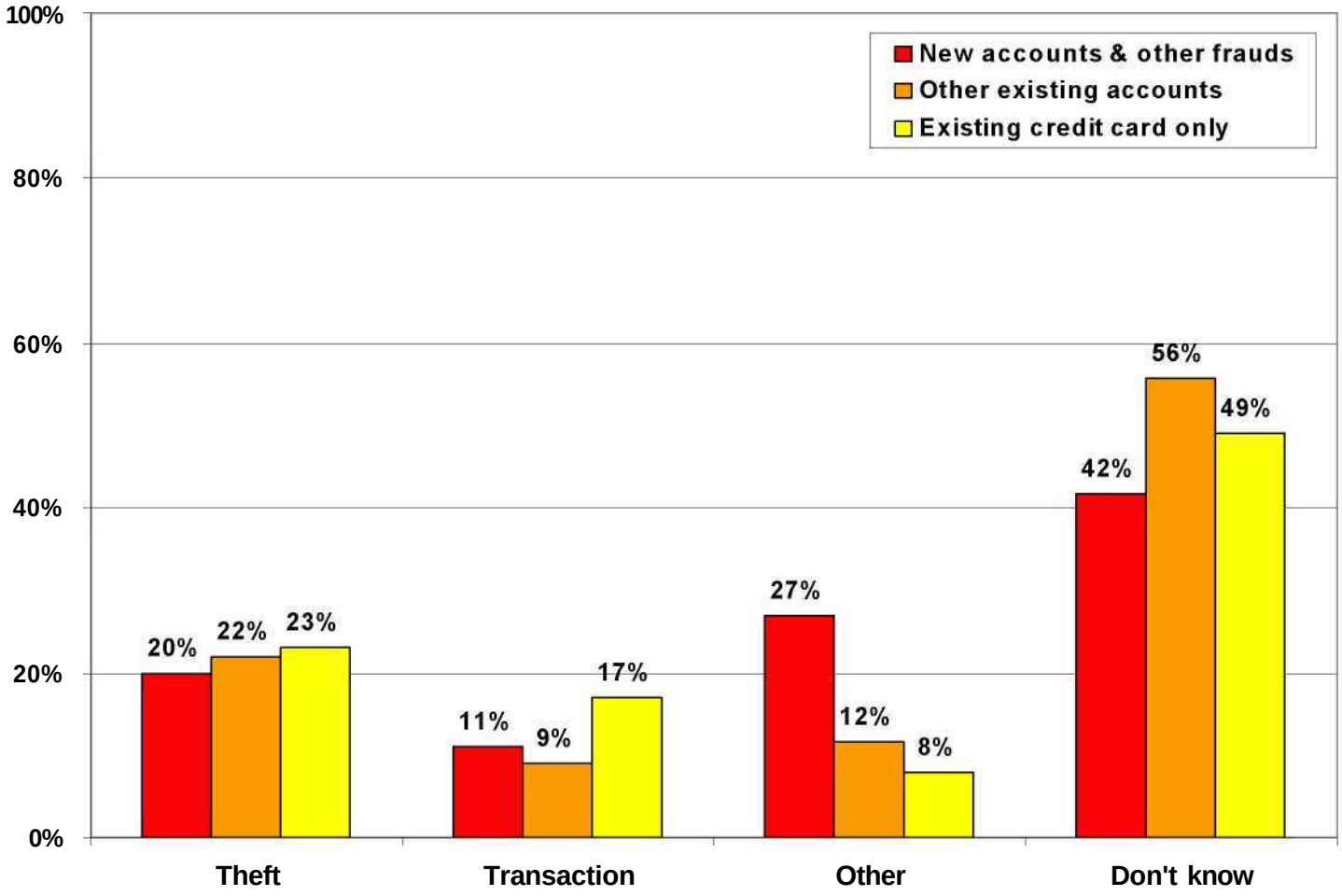
- Knowledge of the thief's identity is more likely when the crime involves more serious cases of Identity Theft. 34% of victims who experienced "New Accounts & Other Frauds" ID Theft were aware of the thief's identity. Among those who experienced only the misuse of existing credit card accounts, just 18% knew the identity of the person who misused their account(s).
- More broadly, in 26% of all cases, the victim knew who had misused their personal information.
- 35% of the 26% of victims who knew the identity (or, in other words, 9% of all victims) said a family member or relative was the person responsible for misusing their personal information.
    - In those cases where the ID Theft involved the opening of new accounts or the committing of other types of fraud, 52% of those who knew the thief's identity - 18%

of victims of this type of ID Theft - identified a family member or relative as the perpetrator.

- Where the misuse involved only existing credit cards, a family member or relative was cited as the person who misused the information by only 26% of victims who said they knew who the person was.

- 23% of the 26% of all victims who knew the identity of the thief (or 6% of all victims) said the person responsible was someone who worked at a company or financial institution that had access to the victim's personal information.
  - Where the misuse involved only existing credit card accounts, someone at a company or financial institution was cited as the source of the misused information by 33% of those who knew the person's identity.
  - In those cases that involved new accounts or other types of fraud, 13% of those who knew the identity identified the perpetrator as an employee of such companies.
- Of the 26% who knew the identity of the person who took their information, 18% said the thief was a friend, neighbor, or in-home employee, while 16% said the thief was a complete stranger, but the victim later became aware of the thief's identity. (These figures represent 5% and 4% of all victims respectively.)

Q16 / Q17 - How information was obtained

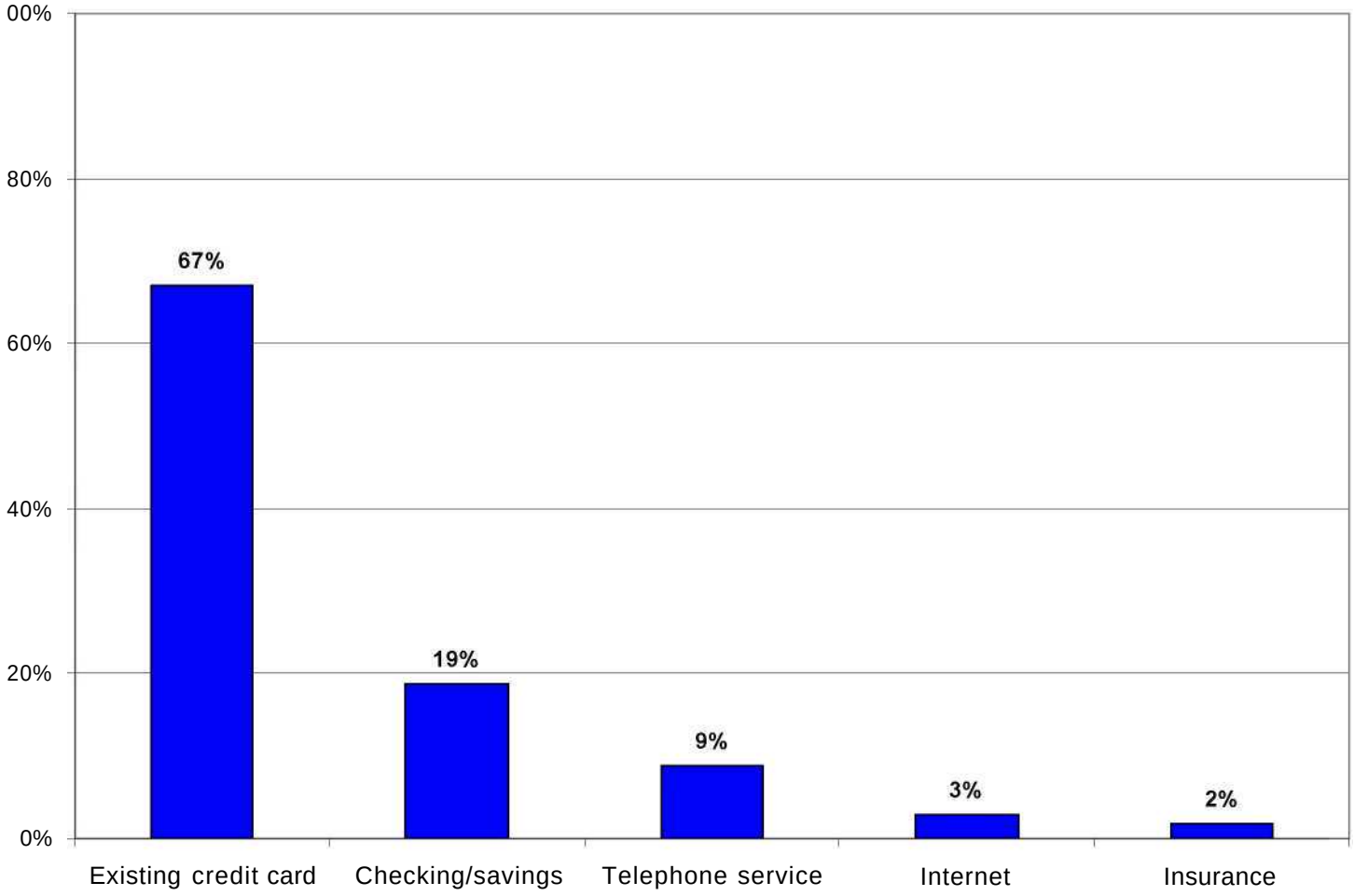


- About half of all victims (51 %) say they know how their personal information was obtained by the identity thief.
- Nearly one-quarter of all victims said that their information was lost or stolen - including lost or stolen credit cards, checkbooks, social security cards, or information obtained through stolen mail.
    - 14% of all victims said that their information had been obtained from a lost or stolen wallet, checkbook, or credit card. Loss of these items was the source of the information for 17% of victims who only suffered the "Misuse of Existing Credit Cards or Card Numbers." For victims of "New Accounts & Other Frauds" ID Theft, a lost or stolen wallet, checkbook, or credit card was the source of the information in only 8% of cases.
    - 4% of all victims cited stolen mail as the source of the information - 3% of those who suffered the "Misuse of Existing Credit Cards or Card Numbers," 7% of those who suffered "New Accounts & Other Frauds."

- 13% of all victims say their information was obtained during a transaction - by taking information from a credit card receipt or during a purchase, or through purchases made over the Internet, mail, or phone. Those who experienced theft of existing credit card accounts only were most likely to mention transactions as the source of information for the thief (17%).
- 14% of all victims said the thief used "other" means to obtain their information. This includes people who said that their personal information was misused by someone who had access to it such as a family member or a workplace associate. Others indicated that the thief had obtained their personal information from printed checks or bills or that they had given the information to someone who then used it for another purpose.
- The victim was more likely to know how their information was obtained where there had been four or more distinct misuses of the victim's information (69%) and where amounts of $1,000 or more were involved (60%).

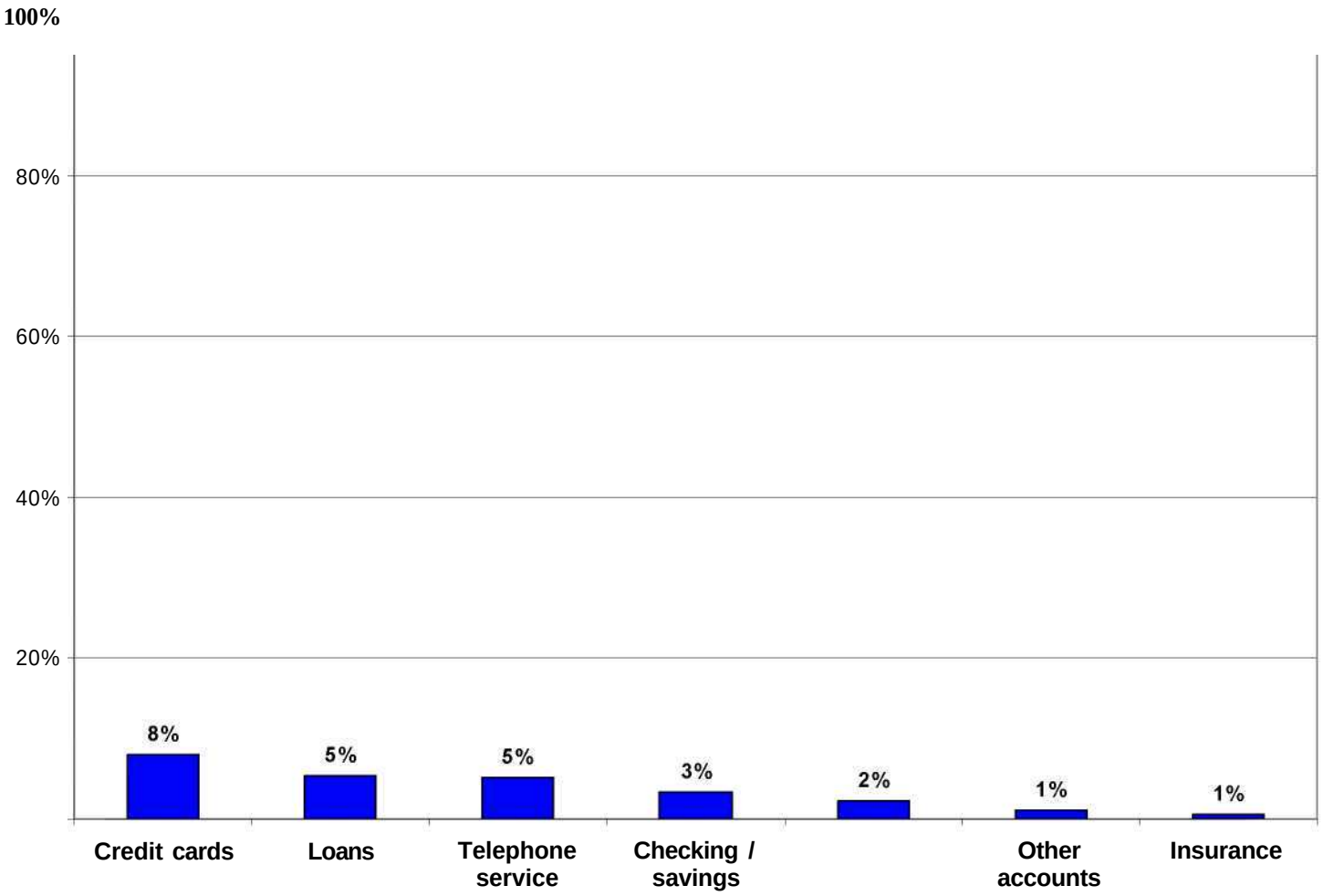
Forms of Identity Theft

Q1 / Q19 / Q20 - Existing accounts misused



- In total, 85% of ID Theft victims reported that one or more of their existing accounts had been misused.
- 67% of all victims said that they have had an existing credit card account misused.
- 19% of all Identity Theft victims said their existing checking or savings accounts were misused.
- 9% of all victims said existing telephone service accounts - conventional or wireless - were misused.
- Fewer victims mentioned misuse of existing Internet (3%) or insurance (2%) accounts.

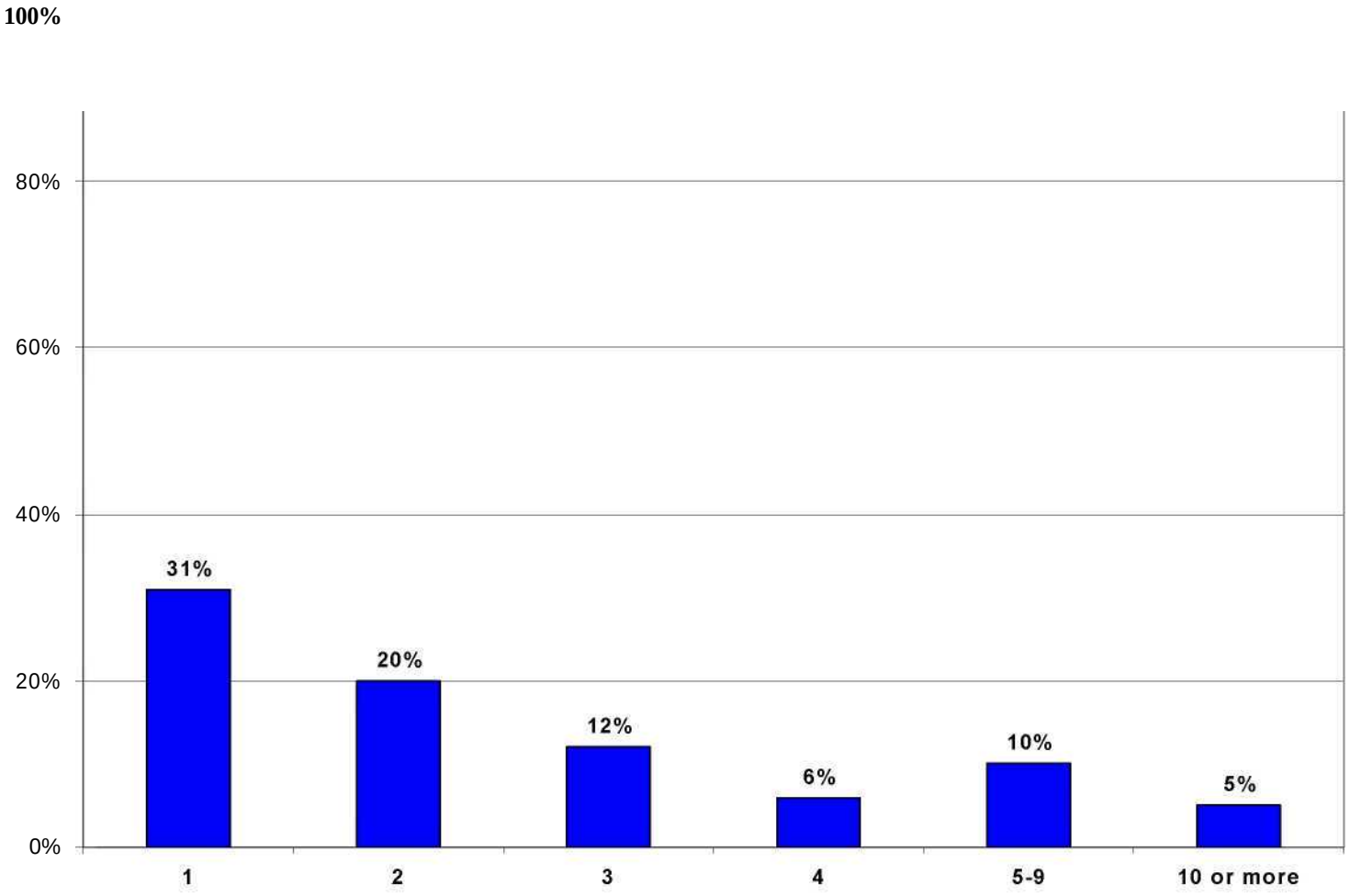
Q24 / Q25 / Q27 - New accounts opened by identity thieves



- Among Identity Theft victims, 17% said the thief used the victim's personal information to open at least one new account, such as new credit card accounts, new loans, new telephone service accounts, or some other new account.
- The most common new account obtained by the identity thief was a new credit card account. 8% of all victims - almost half of those whose personal information was used to open one or more new accounts - said that their information was used to open new credit card accounts.
- 5% of all victims - approximately one-third of those who said that their personal information was used to open new accounts - reported that the thief had obtained new loans using their information.
- 5% of all victims also said that their information had been used to obtain new telephone service - either wireless service or traditional landline.

- New checking or savings accounts were obtained using the personal information of 3% of all victims - approximately one-fifth of those who had new accounts opened.
- New accounts were opened in less than 10% of cases when it took victims less than a month to discover that their information was being misused. New accounts were opened in 45% of cases when 6 months or more elapsed before the misuse was discovered. At least in part, this result may reflect the fact that quickly discovering that a new account has been created in a person's name may be more difficult than discovering that an existing account is being misused. It may also suggest the likelihood that quick discovery reduces the risk that new accounts will be opened.

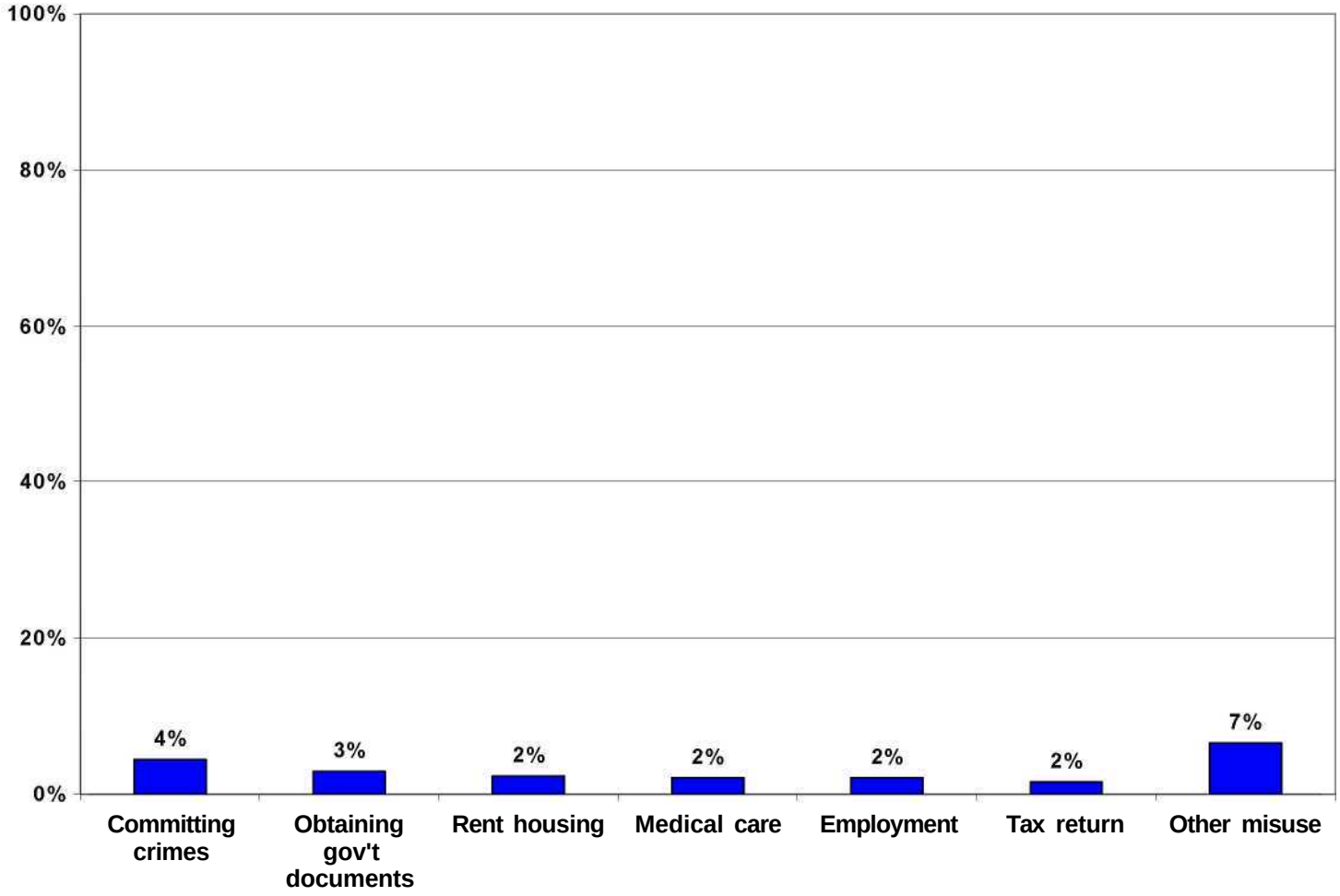
Q24b / Q25a / Q25b / Q27b - Number of new accounts opened



- Of the 17% of all ID Theft victims who reported that new accounts were opened using their information, 31% reported that only one account was opened.
- Only 15% of the 17% of all victims who reported that new accounts were opened said that 5 or more accounts were opened in their names.

Federal Trade Commission

Q28 - Misuses of personal information

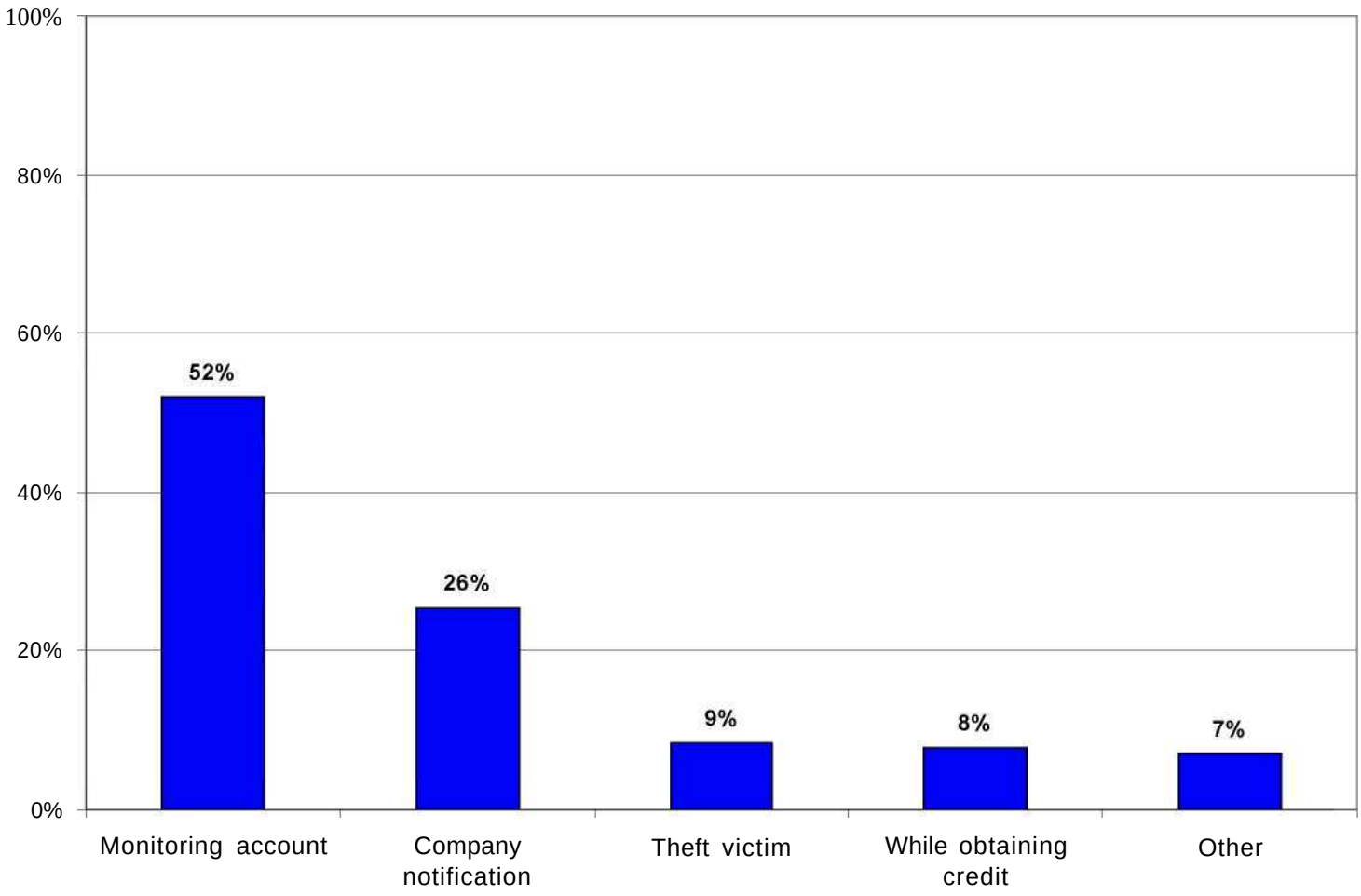


- 15% of all ID Theft victims reported that the identity thief used their information in non-financial ways.
- 4% of all victims said that they were aware that the thief provided the victim's name and identifying information when the thief was caught committing a crime.
- 3% of all victims said they were aware that the thief had used their personal information to obtain government documents, such as a driver's license or social security card. (Of course, these figures may understate the extent to which ID Theft victims' information is misused to obtain government documents because victims may be unaware that such documents have been obtained unless they are informed by police or others that a false document was presented in the process of doing something else.)
- Using the victim's personal information to rent housing, to obtain medical care, to obtain employment, or to file a fraudulent tax return were each mentioned by 2% of all victims.

Toll of Victimization

Federal Trade Commission

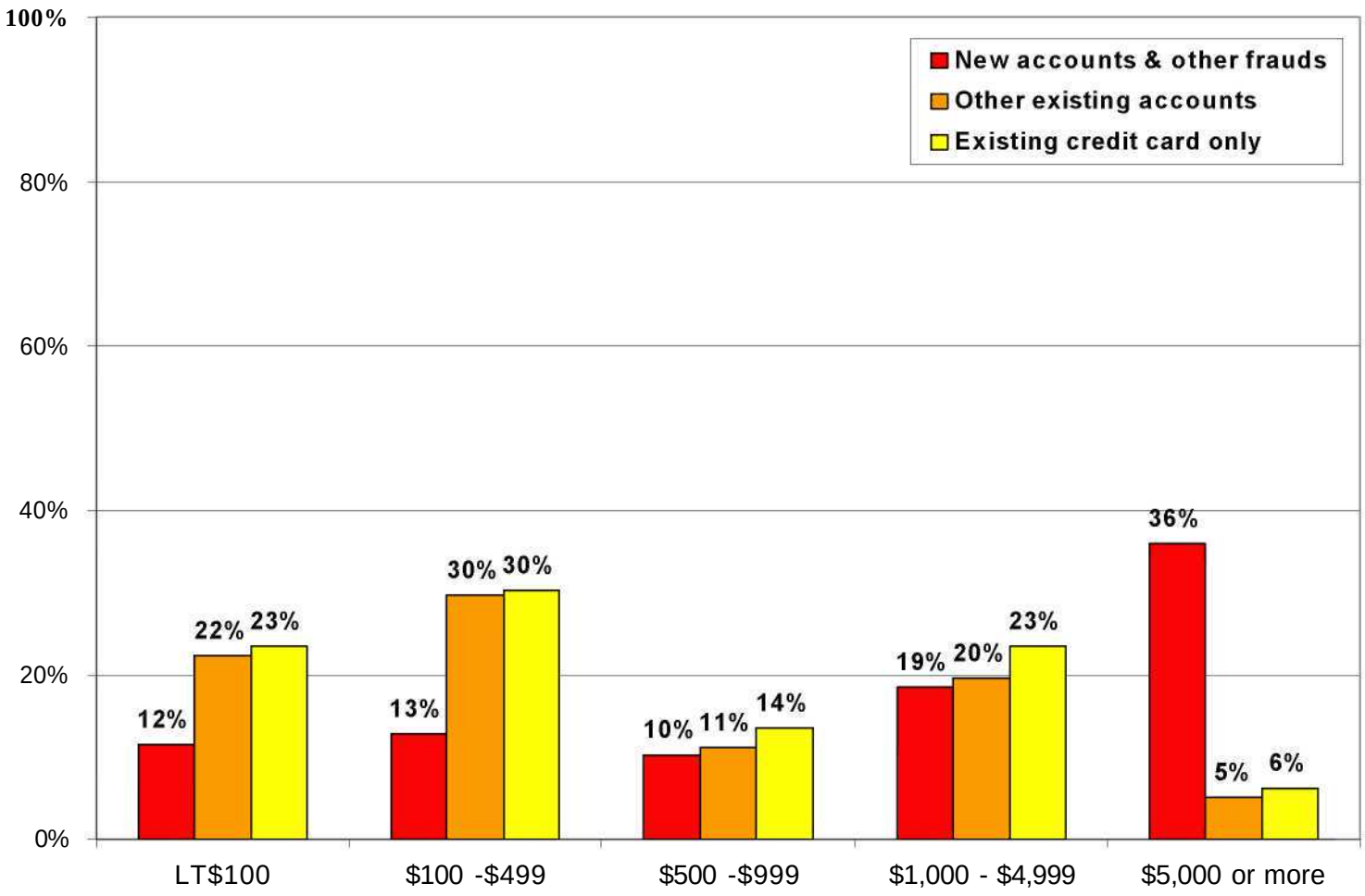
Q13 - How victims discovered ID Theft



- The most common way victims discovered the misuse of their personal information was by monitoring the activity in their accounts. This includes examining monthly statements from banks and credit card issuers. 52% of all victims cited this as the way they first found out they were victims of Identity Theft.
    - Monitoring account activity was cited as the way 62% of victims who only experienced the "Misuse of Existing Credit Cards or Account Numbers" discovered that they had been victimized.
    - Victims of the "Misuse of Existing Non-Credit Card Account" ID Theft cited this as how they discovered the misuse in 57% of cases.
    - Victims of "New Accounts & Other Frauds" ID Theft discovered the misuse of their information by monitoring accounts in only 39% of cases.
- Companies such as banks, credit card issuers, or other vendors first notified one-quarter of all Identity Theft victims of the misuse of their information after noticing suspicious account activity.

  - Being notified by a bank or credit card company was cited by 20% of victims whose ID Theft experience was limited to the misuse of existing accounts - whether credit cards or other accounts.
  - Notification by a bank or credit card company was cited by only 8% of victims of "New Accounts & Other Frauds" ID Theft. On the other hand, 18% of these victims said that they were notified by other parties - including companies where debts had been run up or government agencies.
- 8% of all victims first discovered a problem when they were turned down attempting to secure credit.
  - 18% of victims who had new accounts opened using their information or whose information was used to commit other frauds discovered the misuse when attempting to obtain credit.
  - Only 2% of victims who only had existing accounts misused - whether credit cards or other accounts - cited this as how they discovered that their information was being misused.
- 9% of all victims knew that they had lost their personal information because they had lost a wallet or purse or were victims of theft.

Q29 - Value thief obtained

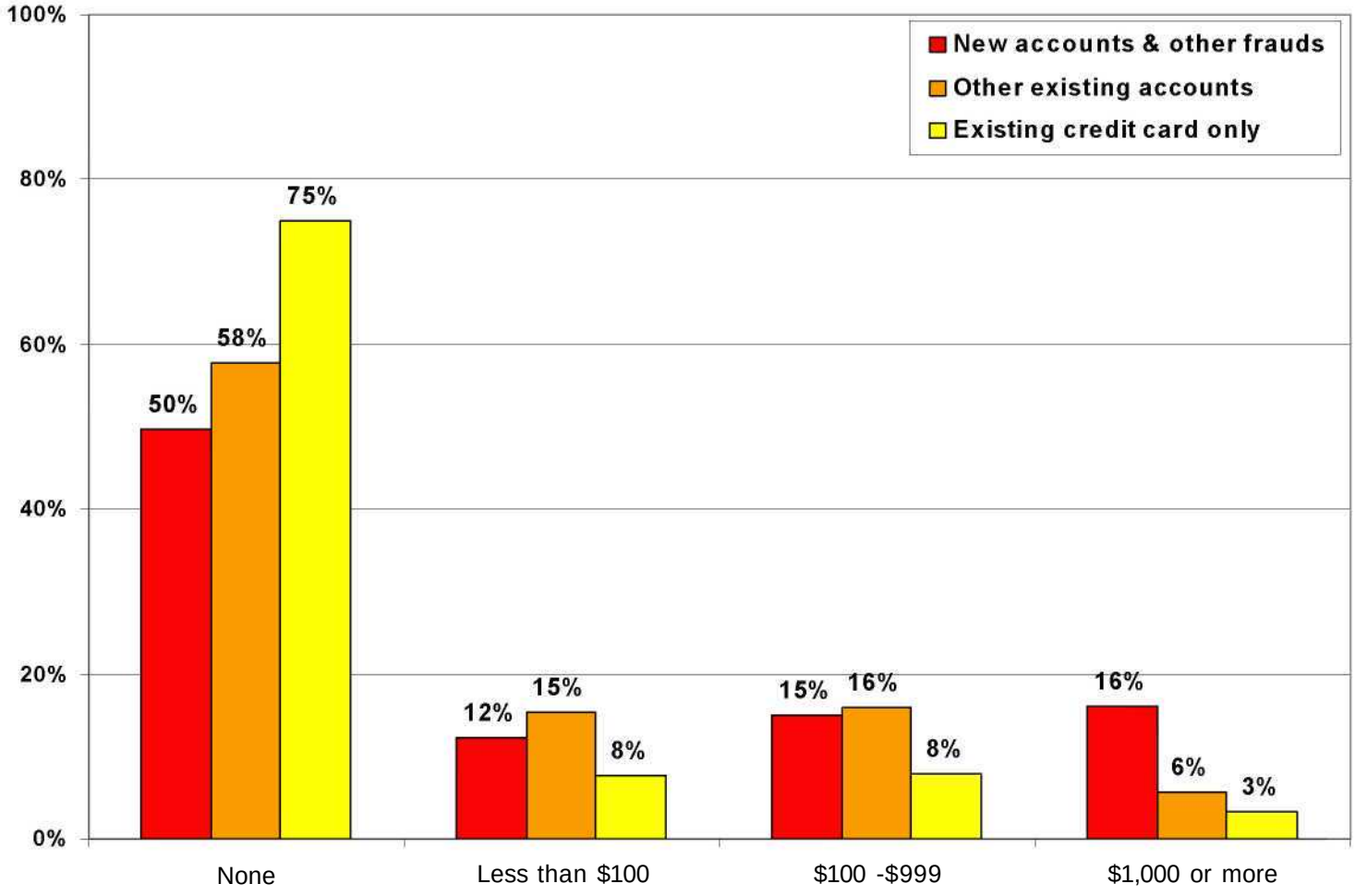


- Victims were asked to estimate the value of what the thief obtained from businesses, including financial institutions, using the victim's personal information. These figures include amounts that became losses to the businesses involved and, in situations where the victim actually paid the debt created by the thief, those amounts as well. The median value was between $500 and $999.
- Overall, 16% of victims said that more than $5,000 was lost due to the misuse of their personal information. About 1-in-5 reported that less than $100 was involved.
- Victims of more serious forms of Identity Theft, those who had new accounts opened in their names or had their information used to commit other types of fraud, reported higher amounts lost; over one-third said over $5,000 was involved, and just 12% of the victims of this type of ID Theft reported a value of less than $100. The average loss resulting from this type of ID Theft was $10,200.
- The amount obtained by the thief was lower where the misuse of the victim's information was discovered more quickly. When the misuse was discovered within 5 months of the initial misuse, the value obtained by the thief was $5,000 or more in only 11 % of the cases.

Where discovery took 6 months or more, the value obtained by the thief was at least $5,000 in 44% of cases.

- For people whose ID Theft experience only involved the misuse of an existing credit card or other account, the median amount reported as being lost was between $100 and $499. Almost 25% of these victims reported that the thief got less than $100.
- Those who suffered four or more distinct misuses of their information were also likely to report higher losses. More than one-half of this group (52%) said more than $5,000 was lost.

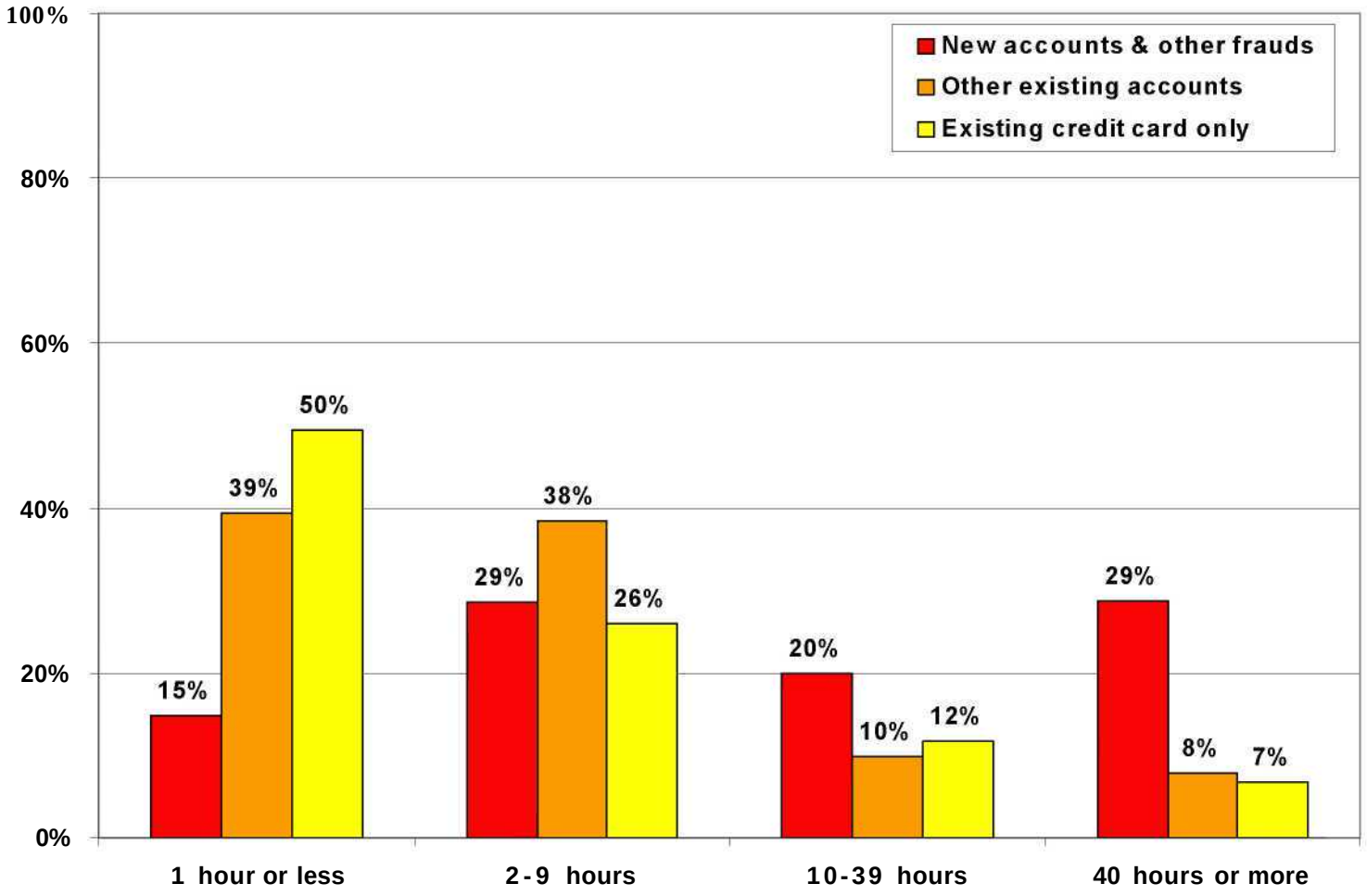
Q30 - Money paid out of pocket



- For most victims of Identity Theft (63%), there was no loss of money out-of-pocket.
- Almost three-quarters of victims who only suffered the misuse of existing credit card accounts had no out-of-pocket losses. However, even for victims of the more serious kinds of ID Theft - "New Accounts & Other Frauds" - about half of victims reported incurring no out-of-pocket expenses.
- The average amount of out-of-pocket expenses incurred by victims of ID Theft was $500. For those who suffered from "New Accounts & Other Frauds" ID Theft, the average out-of-pocket expense was $1,200.
- Victims who quickly discovered that their information was being misused were less likely to incur out-of-pocket expenses. No out-of-pocket expenses were incurred by 67% of those who discovered the misuse less than 6 months after the misuse began. Only 40% of victims who took 6 months or longer to discover the misuse were able to avoid incurring some such expenses.

- Victims with household incomes of less than $75,000 were more likely to have paid money out-of-pocket than were victims with higher household incomes (38% v 25%).
- Residents of the South and West regions were most likely to have out-of-pocket expenses as a result of being a victim of Identity Theft (36% and 35% respectively). Residents of the Northeast region were the least likely to have out-of-pocket expenses (16%).

Q31 - Time spent resolving problems

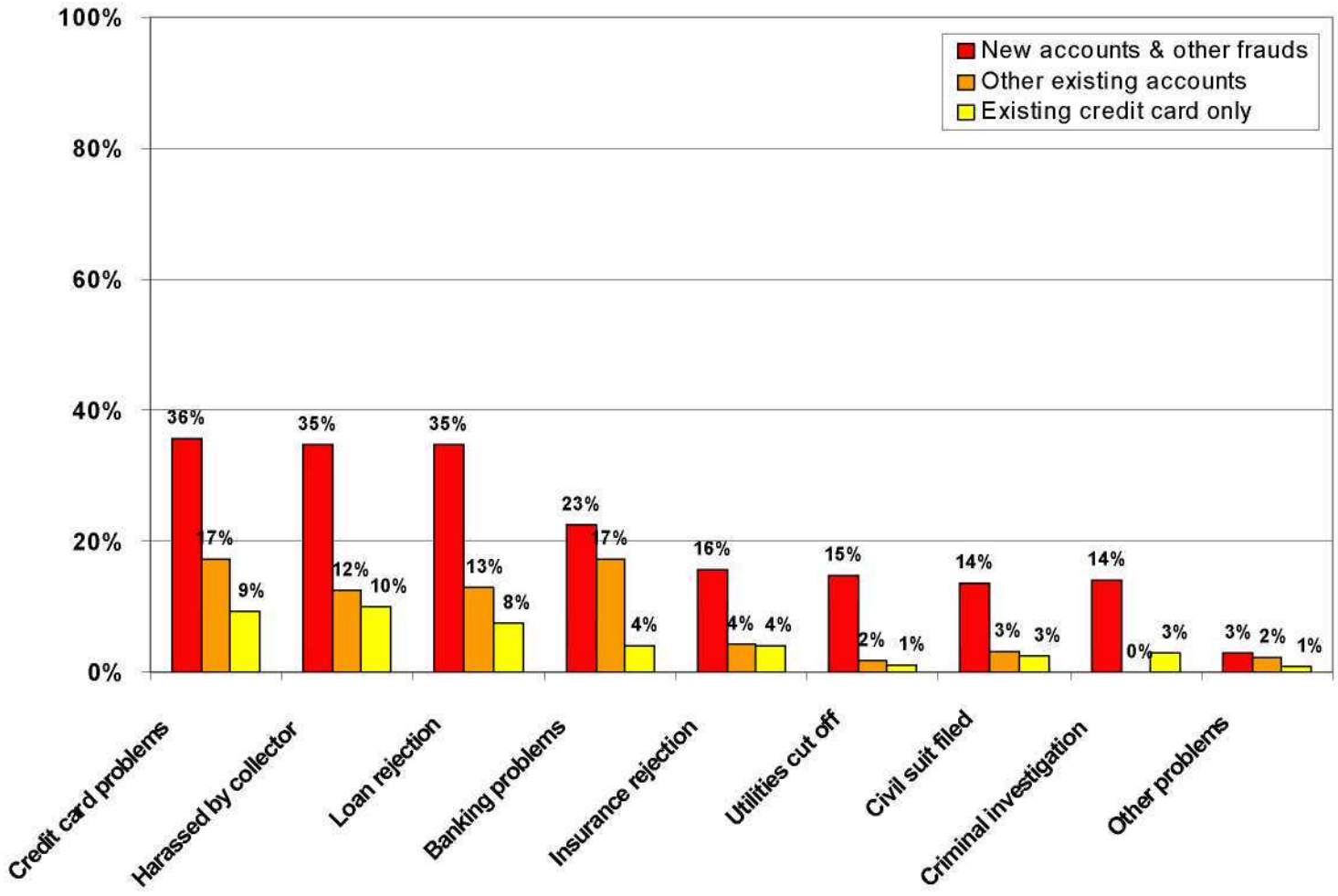


- When asked about the amount of time they spent resolving problems stemming from the misuse of their personal information, the median amount of time reported by victims was 2 to 9 hours.
- 35% of all victims reported that they were able to resolve all problems in one hour or less. Those who were existing credit card only victims (50%) and respondents age 55+ (46%) were significantly more likely to be able to settle Identity Theft issues in one hour or less.
- 29% of all victims required 2 to 9 hours to resolve their problems.
- 30% of all victims spent more than 10 hours.
- 6% of all victims spent over 240 hours of their time, working to resolve problems stemming from Identity Theft.
- The amount of time needed to resolve problems depends on how quickly the misuse is discovered. 76% of victims who discovered the misuse of their information less than a month after it began spent less than 10 hours resolving their problems. Where the misuse

was discovered 1 to 5 months after the misuse began, 59% of victims spent less than 10 hours resolving their problems. Where it took 6 or more months to discover the misuse, only 20% of victims were able to resolve their problems in this amount of time. (How long it took victims of the different types of ID Theft to discover the misuse of their information is discussed on page 19.)

- Victims whose information was used to open new accounts or commit other types of fraud required significantly more time to resolve their problems. Nearly half of these victims needed 10 hours or more to resolve problems, while only 15% were able to resolve their problems in an hour or less. Victims of this type of ID Theft reported that they spent an average of 60 hours resolving problems.

Q32 - Other problems experienced

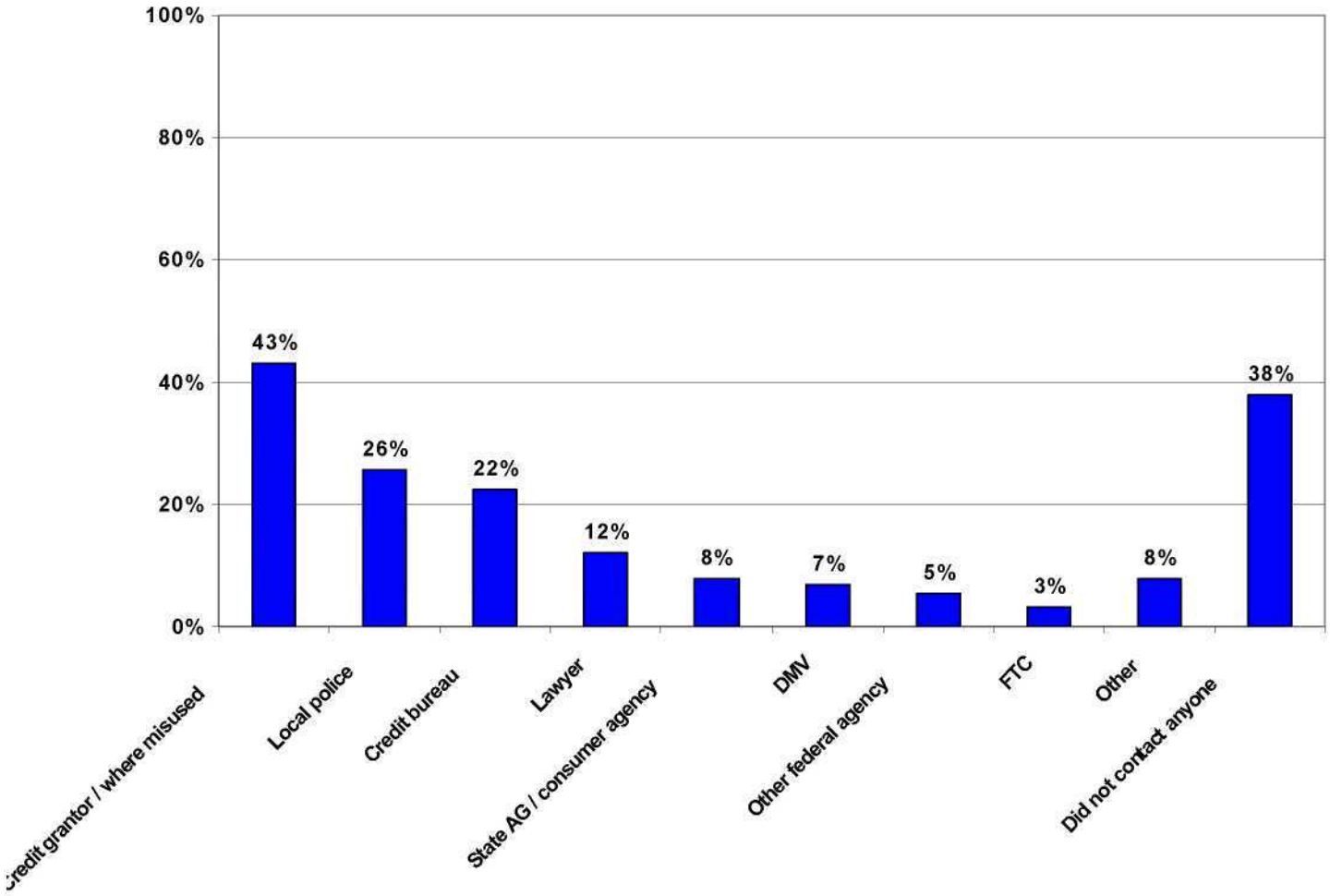


- Victims were asked whether they had experienced various types of problems as a result of having their personal information misused. These included having problems obtaining or using a credit card, being turned down for a loan, or having problems opening a bank account or cashing checks. A total of 36% of all Identity Theft victims reported having at least one of the problems identified.
- Those who experienced more serious forms of Identity Theft - having new accounts opened in their names or having other forms of fraud committed using their personal information - are far more likely to report having one or more the identified problems (64%) than those who only had existing credit card accounts misused (18%) or had other existing accounts misused (32%).
- The number of victims reporting one or more of these problems increases as the value of loss increases. When the loss is less than $1,000, 23% reported problems, compared to 43% for those where the loss was between $1,000 and $5,000, and 74% when the loss was $5,000 or more.

- The number of problems also depends on the extent and type of misuse of the victim's information. Just 17% of those who had only 1 to 3 existing credit card accounts misused reported other problems as well. However, 76% of those who experienced four or more distinct misuses of their personal information reported other problems as a result of their victimization.
- When the crime is detected more quickly, fewer problems emerge. Among those who discovered the Identity Theft within one month of the initial crime, 26% reported having one or more of these problems. This compares to 76% of victims having such problems when the misuse is not discovered for at least 6 months.
- One-in-five Identity Theft victims said they have experienced problems obtaining or using credit cards in the wake of having their personal information misused. Credit card problems were worst for those who experienced four or more distinct misuses of their information (58% reported problems).
- Similarly, 20% of Identity Theft victims reported being harassed by a debt collector.
- 18% report being turned down for a loan; another 13% have had other banking problems such as being turned down for a new bank account, having checks rejected or appearing on a bad check list.
- Lower income households reported having more problems with being harassed by a debt collector (34% of those with incomes of less than $50,000) and being turned down for a loan (29% of those with incomes below $25,000).
- Non-whites reported more problems than whites. Also, younger victims (especially those between 25 and 34) were more likely to experience these types of problems than older victims.

Actions Taken

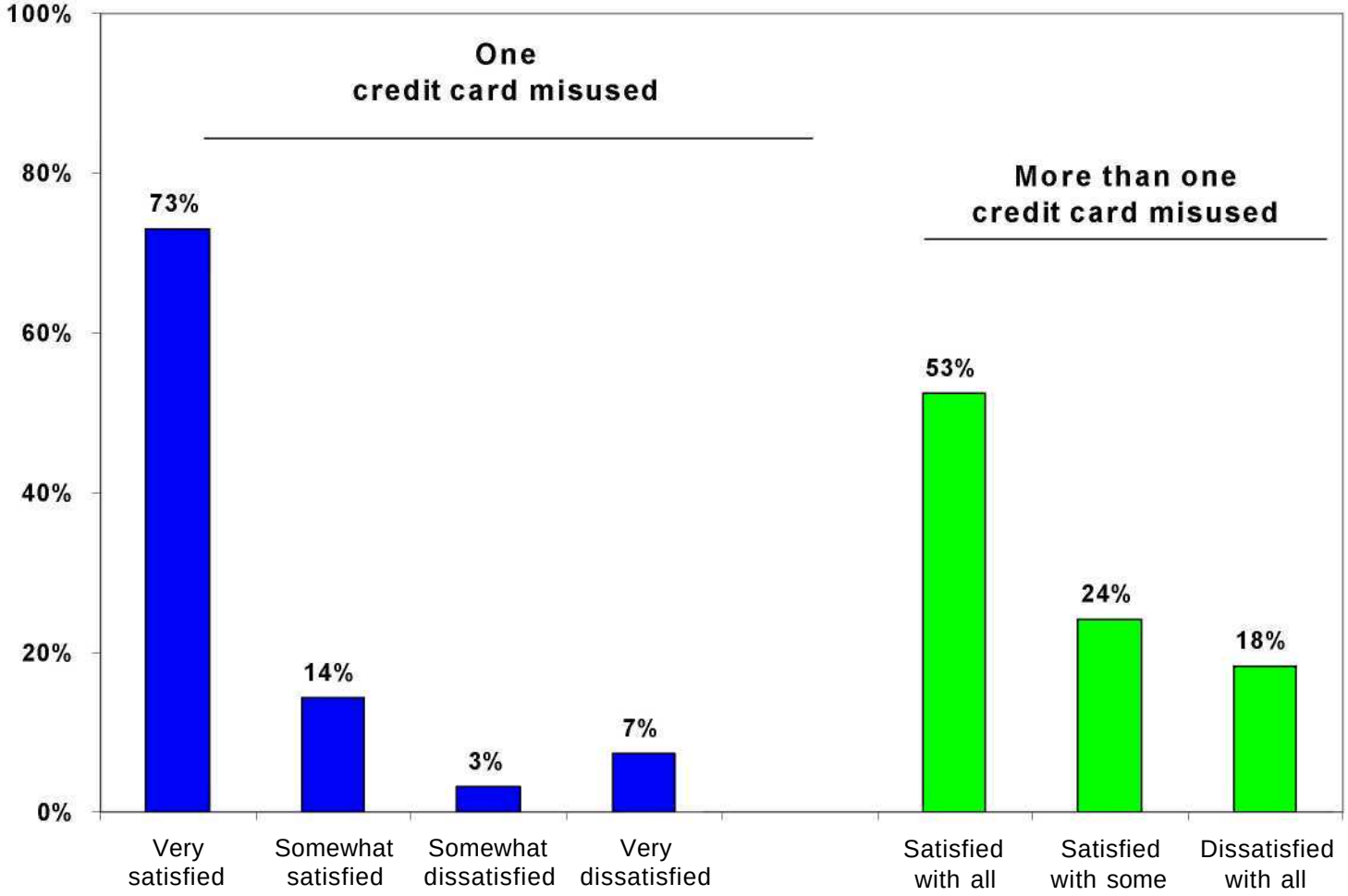
Q33 / Q33a - Contacts reporting Identity Theft



- Among Identity Theft victims, the most commonly reported contact was with the company that had issued an existing credit card or other account that was misused or that issued a new account to the thief (43%). (This also includes contacts with stores where a new or existing card was used.) Victims with household incomes of $25,000 or less were less likely to contact such companies.
- About one-quarter of victims called the police. Victims of "New Accounts & Other Frauds" ID Theft were most likely to contact local law enforcement (43% vs. 17% among those who had only existing accounts misused).
- Victims of the more serious forms of Identity Theft were also more likely to contact a credit bureau (37%). Somewhat surprisingly, only 13% of victims who had existing credit card accounts misused said they contacted a credit reporting agency.
- The FTC was contacted by 3% of Identity Theft victims, while 5% contacted other federal agencies, including the Postal Service and the Social Security Administration.

- 38% of victims reported that they did not report that they had been victims of ID Theft to anyone.
- Older victims were less likely to report that they were victimized than younger victims. Of victims age 18-24, only 17% did not report their experience, while 66% of victims 65 and over did not tell anyone.
- Where the loss that resulted from the ID Theft totaled $5,000 or more, 81% of victims reported their experience to someone. When the loss was less than $1,000, only 54% of victims reported what had happened to anyone.

Q34 / Q34a - Satisfaction with credit card company

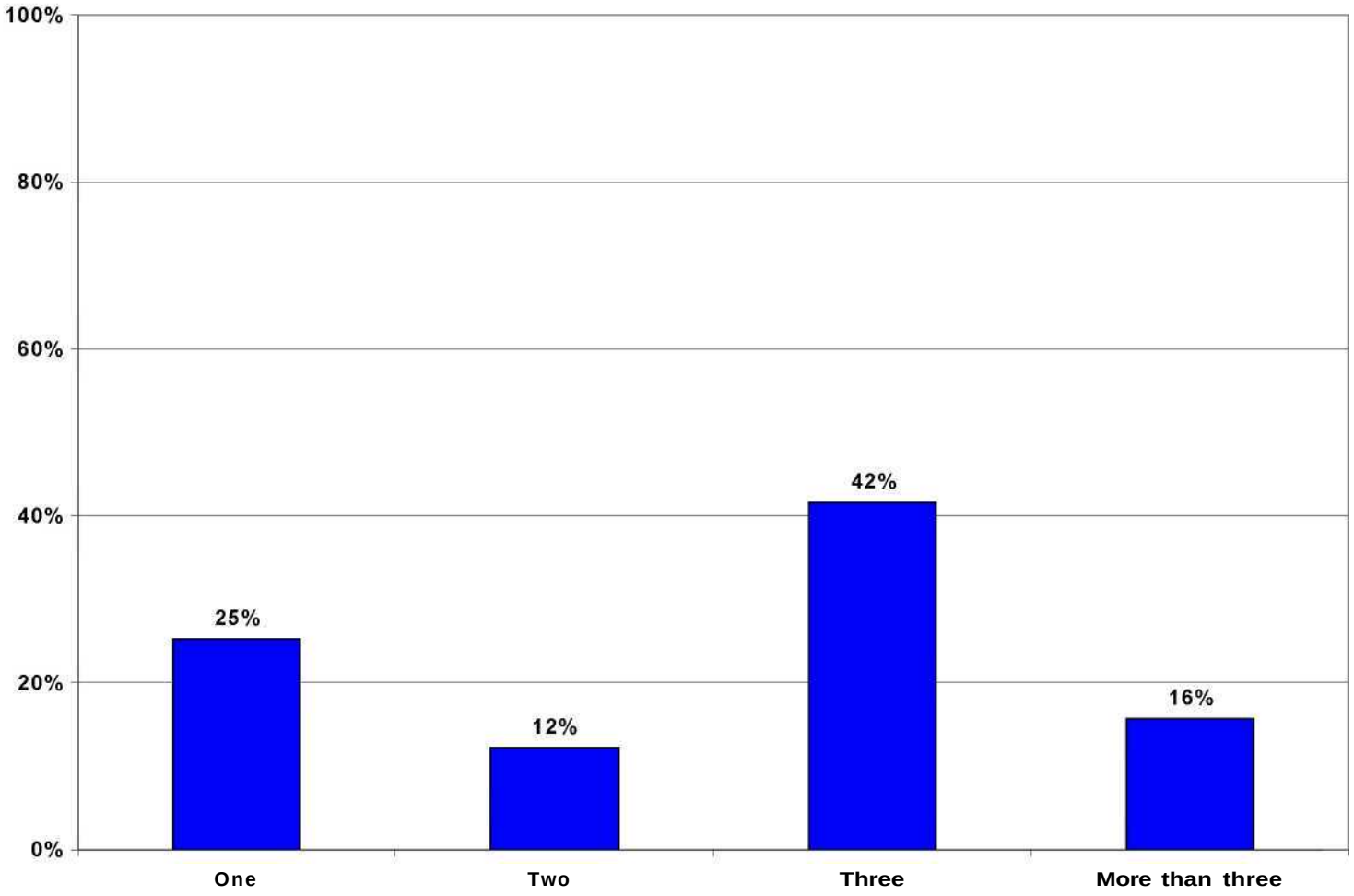


- Among those who had just one existing credit card misused or who had one new credit card account opened in their name (56% of all Identity Theft victims), those who reported contacting the credit card company were overwhelmingly satisfied with the company's response - 73% were "very satisfied" with how the credit card company responded to the report of misuse.
- Satisfaction was somewhat lower among victims who had more than one existing or new credit card misused. 53% of these victims were satisfied with all of the companies they contacted. Satisfaction was mixed for 24% of these victims, while 18% were dissatisfied with all of the credit card companies to whom they reported the misuse of their credit cards.
- Victims of the "New Accounts & Other Frauds" form of Identity Theft reported slightly lower levels of satisfaction than existing credit card only victims. 78% of those who experienced the more serious form of ID Theft reported that they were satisfied with the response of the credit card companies - either "very" or "somewhat" satisfied for those who only had one

card misused or satisfied with all of the companies where multiple cards were misused. For those who only experienced misuse of existing credit cards, the satisfaction level was 91%.

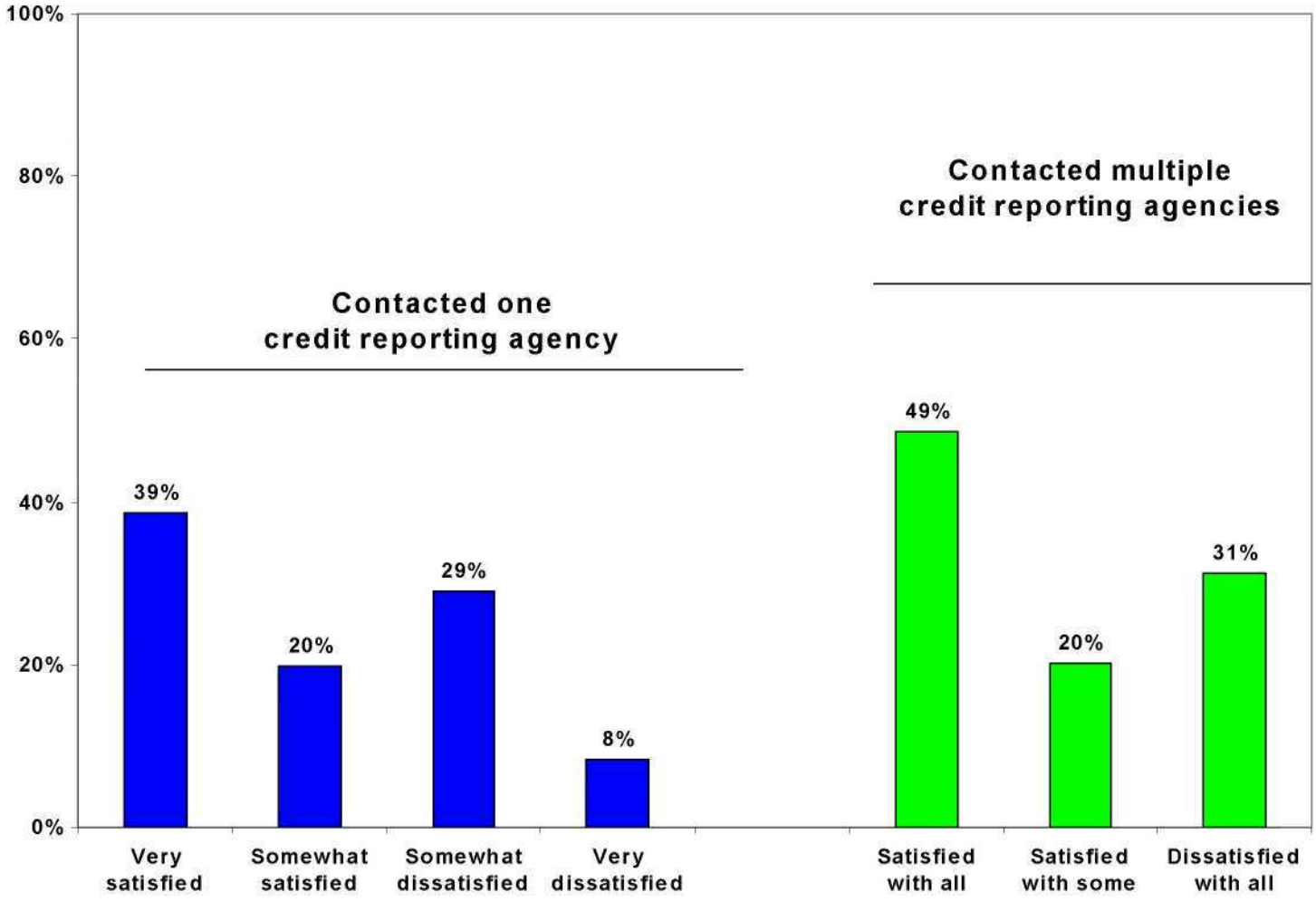
- Satisfaction is also somewhat lower when higher amounts are involved. When the loss exceeded $5,000, 57% of victims said they were satisfied with the responses of the credit card companies. 89% of victims were satisfied where the losses were under $5,000.

Q36 / Q33a - Credit bureaus contacted



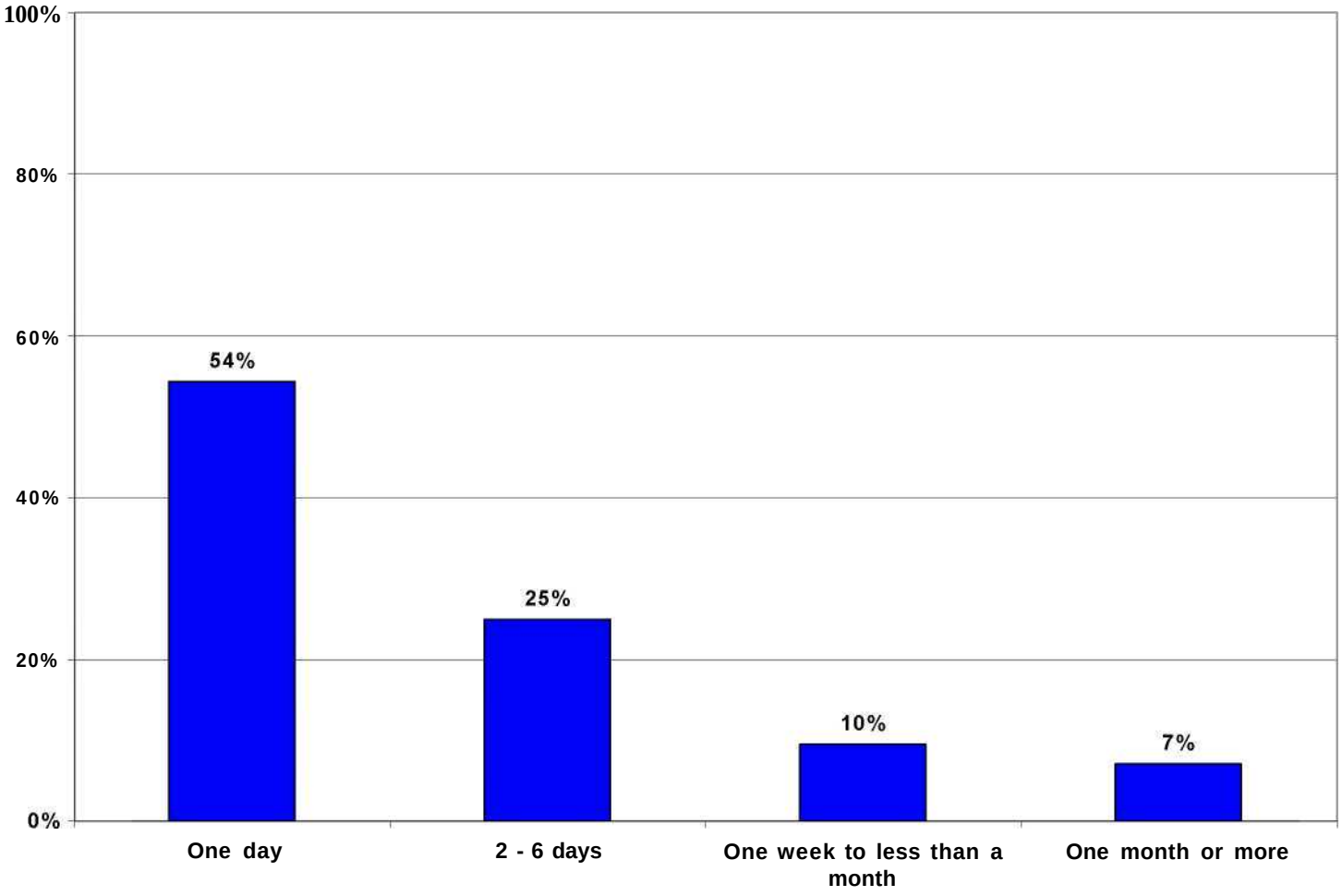
- Among Identity Theft victims, 22% said they contacted at least one credit bureau. Of those who contacted a credit bureau, 25% contacted a single credit reporting agency, 12% contacted two, and 57% contacted three or more agencies. (The remaining 5% said they did not know how many credit bureaus they contacted.)
- Victims were most likely to contact a credit bureau when a loss of $5,000 or greater was involved (48% contacted one or more credit bureaus) or where there were four or more distinct misuses of the victim's personal information (47%).
- 37% of those who experienced "New Accounts & Other Frauds" Identity Theft contacted at least one credit bureau. However, just 13% of those who had only existing credit cards misused contacted a credit bureau.
- The greater the values associated with the case of Identity Theft, the more likely the victim was to contact a credit bureau. In cases involving losses of less than $1,000, 15% made contact, compared to 21 % in thefts involving $1,000 - $5,000, and 48% when the amount lost was $5,000 or greater.

Q37 / Q37a - Satisfaction with credit bureaus



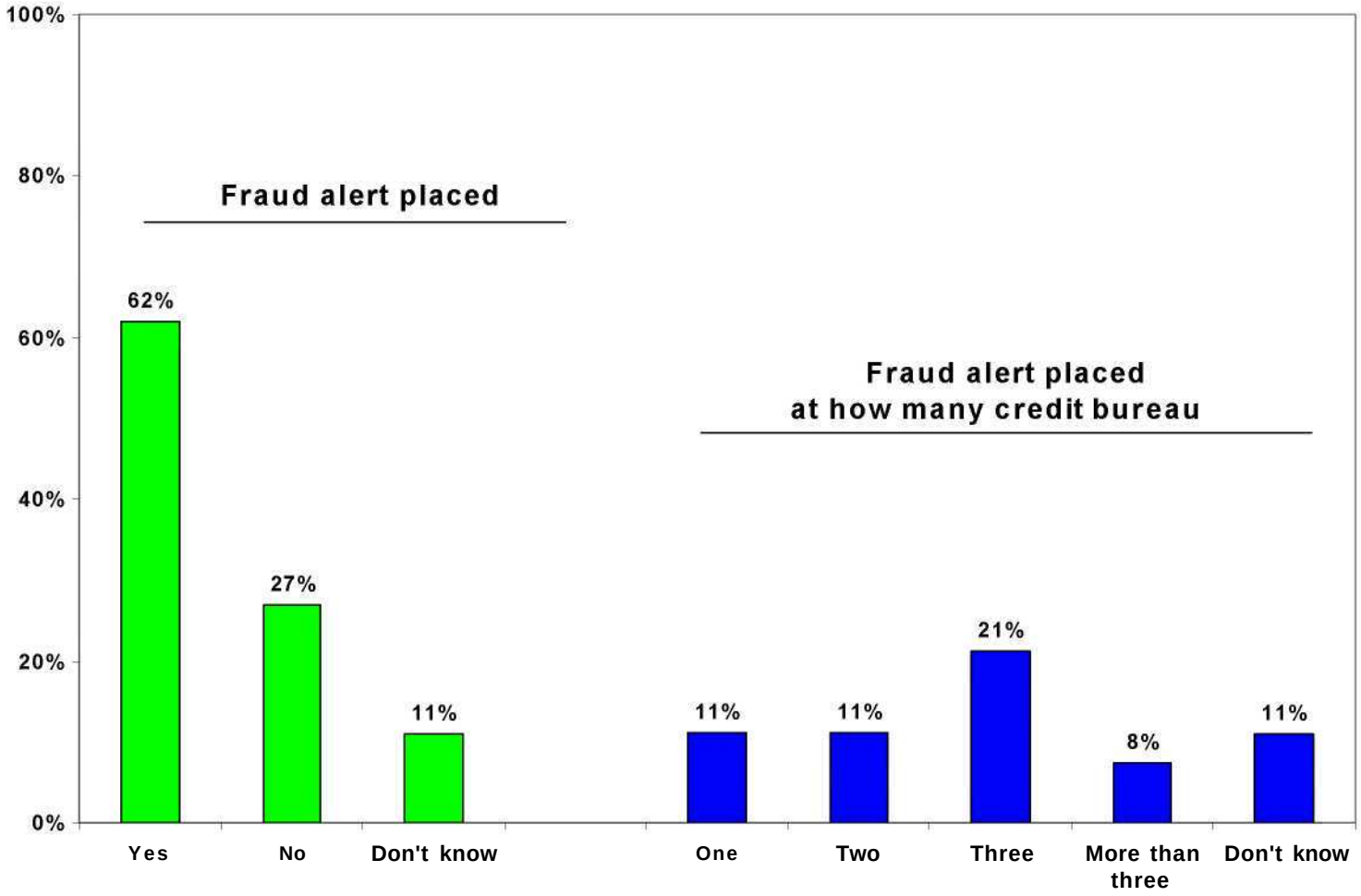
- Among ID Theft victims who reported contacting a single credit reporting agency, a majority (58%) said they were either "very" or "somewhat" satisfied with the way their report was handled by the agency.
- Among those who contacted more than one credit reporting agency, nearly half (49%) were satisfied with all agencies they spoke to, 20% expressed satisfaction with some of their contacts but not others, and 31% were dissatisfied with all of the credit reporting agencies contacted.

Q35 - Time before contacting credit bureaus



- Of those ID Theft victims who contacted a credit bureau, 54% did so within one day of discovering the misuse of their personal information.
- A small percentage of those who contacted credit bureaus (7%) did so only one month or more after discovering that they had been victimized. (4% did not indicate how much time passed before contacting the credit bureaus.)

Q38 / Q39 - Fraud alert placed



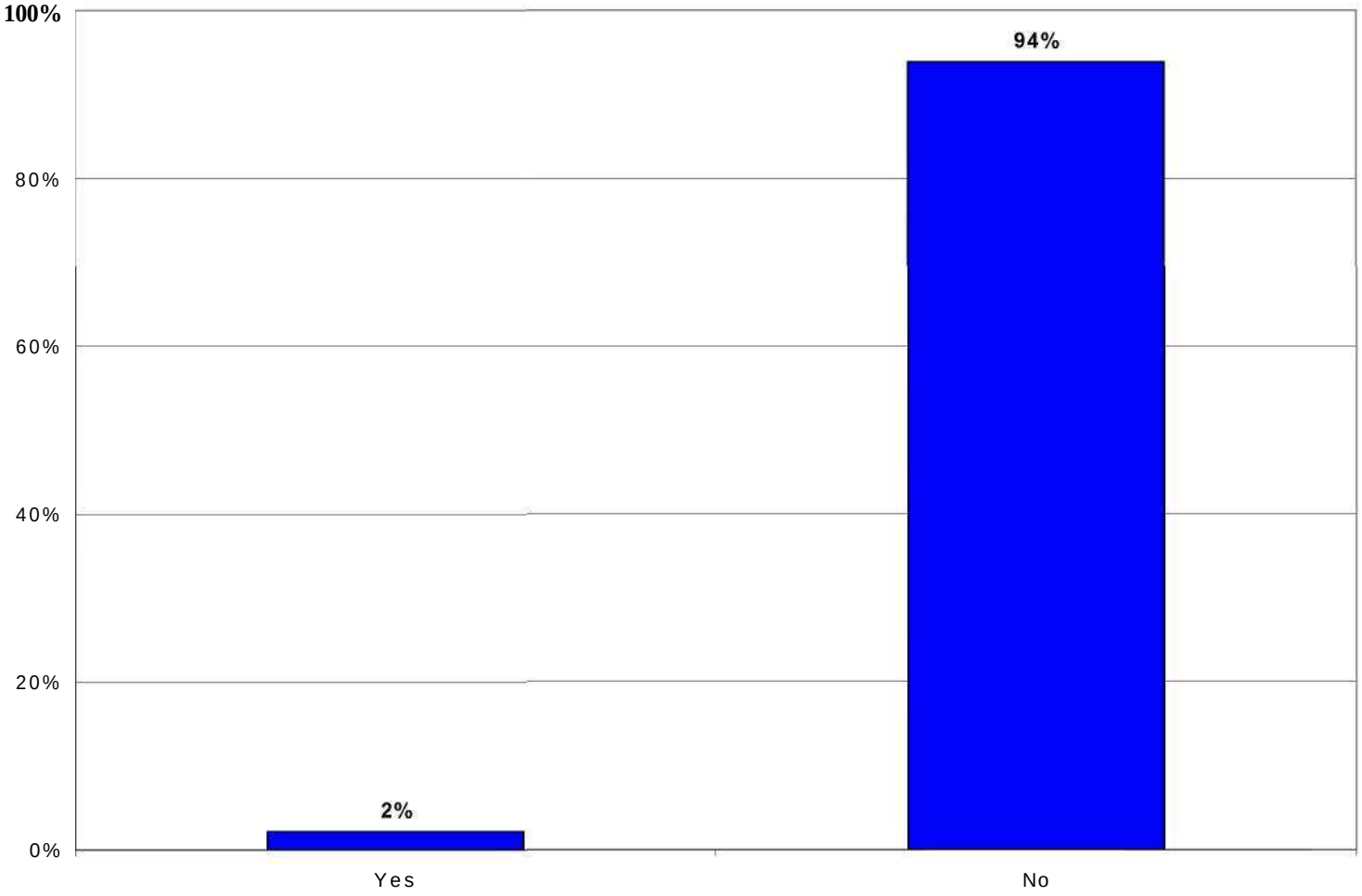
- Of the 22% of ID Theft victims who contacted credit bureaus, 62% said that a fraud alert was placed on their credit report at one or more of the credit bureaus.

- 70% of those who suffered "New Accounts & Other Frauds" ID Theft and contacted a credit bureau had a fraud alert placed on their records. Of those who only suffered the misuse of an existing credit card account, only 46% had a fraud alert placed on their records.

- Victims were more likely to have a fraud alert placed when their personal information was misused multiple times. 71 % of those who contacted a credit bureau and had experienced four or more distinct misuses of their personal information had a fraud alert placed on their records, while only 42% of those with only one to three distinct misuses had an alert placed.

- Over 40% of victims who contacted credit bureaus requested fraud alerts from more than one credit bureau.

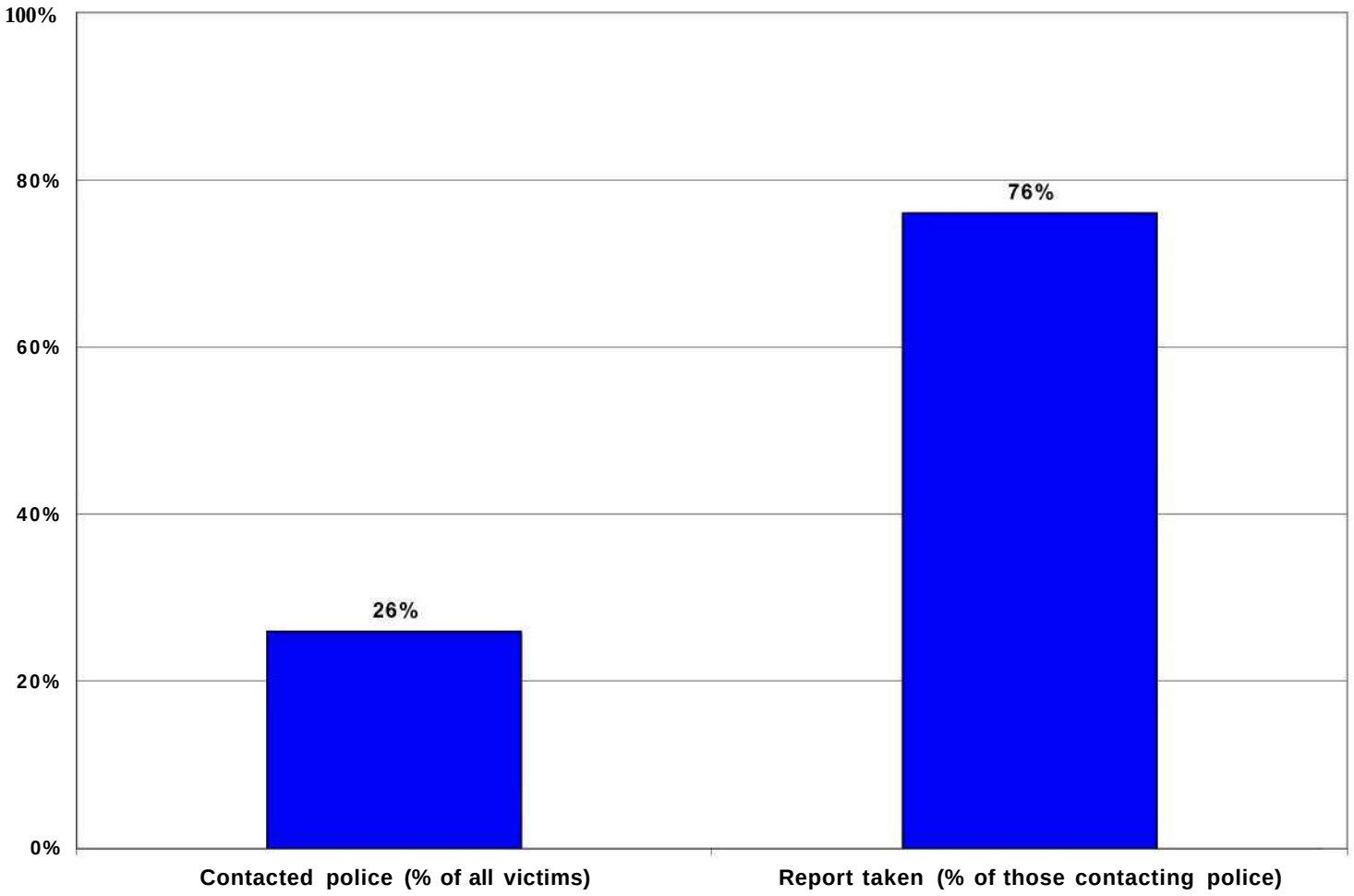
Q40 - Accounts opened after fraud alert



- Of the 22% of ID Theft victims who contacted credit bureaus, 62% said that a fraud alert was placed on their credit report at one or more of the credit bureaus.

- Just 2% of respondents who requested a fraud alert said that accounts were opened in their name after the fraud alert was implemented. (Care should be exercised in interpreting this result. The number of survey participants who asked for a fraud alert was fairly small - 62 - and only one of these 62 said that additional accounts were opened after a fraud alert was placed.)

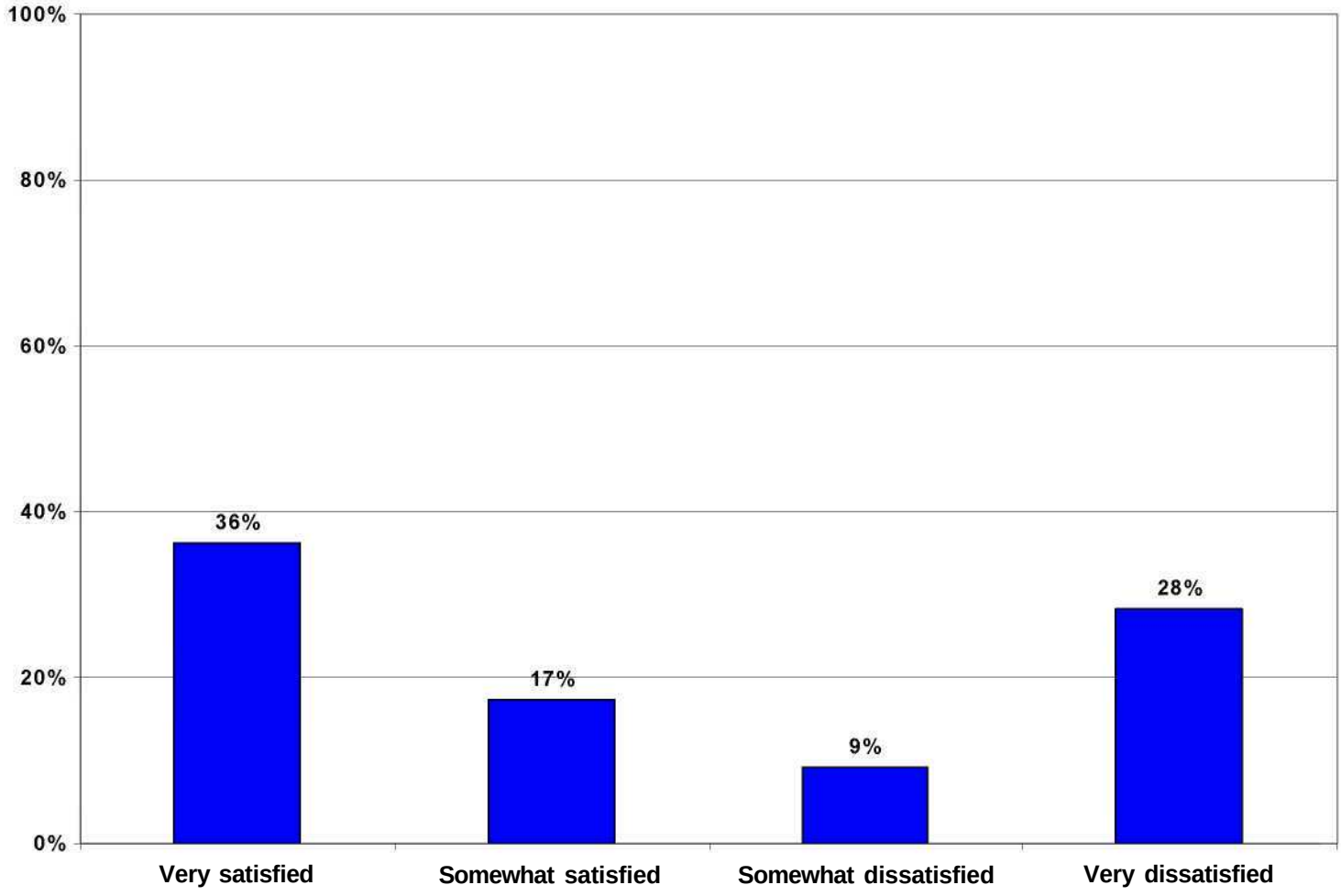
Q33a / Q41 - Contact with local law enforcement



- A total of 26% of all Identity Theft victims contacted a local law enforcement agency.
- 17% of victims who suffered only the misuse of existing credit cards contacted local law enforcement, while 43% of those whose information was used to open new accounts or commit other types of fraud did so.
- Victims in cases involving greater amounts were more likely to contact local law enforcement. A majority (54%) of victims where the value lost was $5,000 or more contacted the police, compared to 16% of victims in cases involving less than $1,000.
- Of the 26% of victims who contacted a local law enforcement agency, three quarters said that the local agency took the complaint and filed a report describing the Identity Theft. (A report was slightly more likely to be taken if the victim's information was used to open new accounts or to commit other frauds than if only existing accounts - whether credit card or other accounts - were misused (82% v 73%).)
- Non-white victims were more likely than whites to contact the police (34% of non-white victims v 23% of white victims).

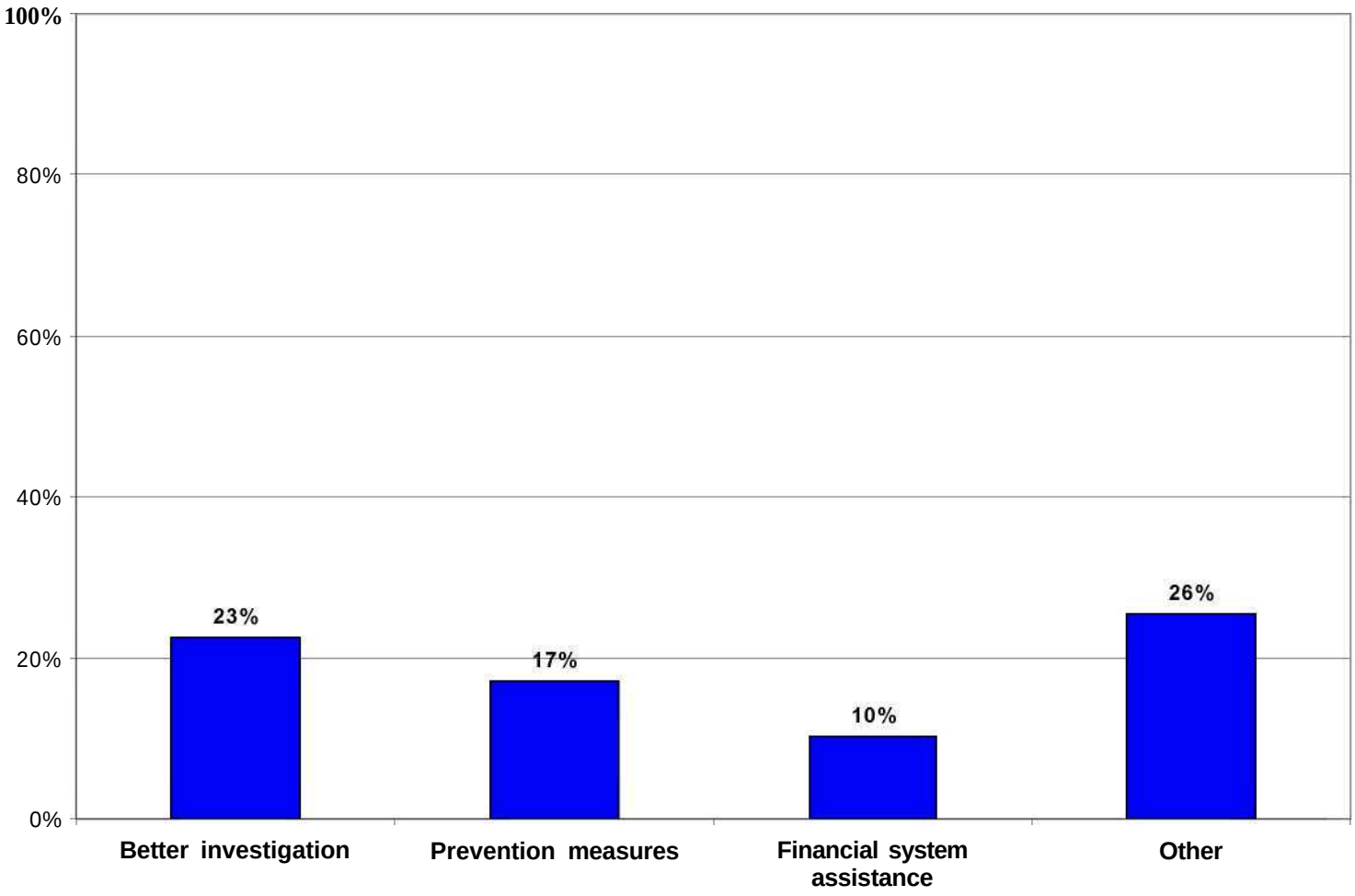
- Police were more likely to take a report if the misuse was discovered more quickly. A report was taken in 83% of cases where the misuse was discovered within 5 months of the initial misuse of the victim's information. Where it took 6 months or more to discover the misuse, reports were only taken in 47% of cases.

Q42 - Satisfaction with local law enforcement response



- Of the 26% of victims who contacted local law enforcement 53% said they were "very" or "somewhat" satisfied.
- However, a substantial percentage of the 26% of victims who contacted local law enforcement were "very" dissatisfied with the response of local law enforcement.

Q44 - Most important action that would have helped



- When asked what could have been done to help fix the problems victims experienced as a result of Identity Theft, the action most frequently cited by victims who spent at least 10 hours of their time resolving problems was to improve the investigation by law enforcement after the crime had been committed. Specific proposals mentioned included a stronger commitment to catching the thief or thieves, better follow-up and communication with the victim, and increased assistance from local law enforcement. On a related note, victims also recommended stiffer penalties for offenders.
- Many victims thought better awareness on their own part of how to prevent and respond to identity theft would have been most helpful. Specific areas where greater awareness was cited included taking greater security precautions in handling their personal information, such as destroying materials that contain personal information instead of simply putting them in the trash, not placing personal information on the Internet, and securing their personal information in their homes and at work. Maintaining greater vigilance, such as monitoring their mail, billing cycles, and credit reports more carefully was also cited. Lastly, knowing who to contact, and notifying the affected companies and credit reporting agencies

more quickly when they detected something wrong, was identified as an important factor in recovering from identity theft.

- Other victims mentioned things financial institutions could do to detect and prevent the crime. Respondents cited improved authentication measures, such as photographs on credit cards and more thorough identification procedures by employees during credit transactions. Respondents also mentioned financial institutions, including credit reporting agencies, making greater efforts to monitor their account activity and notify them when unusual transactions occurred.
- Many respondents thought that improved follow-up and assistance by the financial community as they attempted to repair their records would help. Specific proposals included making the recovery process easier by reducing the number of documents the victim had to sign, and listening to the victim and treating them with more understanding and less suspicion.

Appendix A: Questionnaire

FEDERAL TRADE COMMISSION
INCIDENCE OF IDENTITY THEFT STUDY

Federal TradeCommission

TOTAL SAMPLE

Now I'd like to ask you some questions on the topic of Identity Theft.

1. Has anyone ever misused your credit card or credit card number to place charges on your account without your permission? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE.)**

Yes	1	
No	2	1
Don't know	X	I -> **(SKIP TO QU. 3a)**
Refused	R	J

1a. How many of your existing credit card accounts were affected? **(ENTER EXACT NUMBER FROM 1 TO 25. DO NOT ACCEPT RANGE. IF RESPONDENT IS UNSURE, ENCOURAGE BEST GUESS.)**

# _ _ _ _ _ **(V A L I D RANGE 1 TO 25)**	
Don't know	X
Refused	R

2. Did the misuse of your credit cards involve the use of a credit card that you had lost or that had been stolen? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE.)**

Yes	1
No	2
Don't know	X
Refused	R

3. Did someone attempt to "TAKE OVER" the credit card account that had been misused by, for example, changing the billing address on the account or having themselves added as an authorized user of the account? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE FOR EACH.)**

Yes.....1
No.....2
Don't know.....X
Refused.....R

3a. Has anyone ever misused any of your existing accounts other than a credit card account - for example, a bank or wireless telephone account - without your permission to run up charges or to take money from your accounts? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE.) **Note: Not asked in Wave 1.**

Yes.....1
No.....2
Don't know.....X
Refused.....R

4. Have you ever been the victim of a different form of Identity Theft, one that involved more than just the misuse of existing accounts or numbers? That is, has anyone used your personal information without your permission, to obtain NEW credit cards or loans in your name, run up debts in your name, open other accounts, or otherwise commit theft, fraud, or some other crime? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE.)**

Yes.....1
No.....2
Don't know.....X
Refused.....R

ASK QU. 5 IF "YES" TO QU. 3a, AND/OR QU. 4; OTHERWISE, TERMINATE.

IF "YES" TO QU. 4, INSERT TEXT A FOR QU. 5.
IF "YES" TO QU. 3a AND "NO", "DON'T KNOW", OR "REFUSED" TO QU. 4, INSERT TEXT B FOR QU. 5.

5. I would like to get some more information about the misuse of **(INSERT TEXT).** Has your personal information been MISUSED within the last five years? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE.)**

Yes.....1
No.....2
Don't know.....X
Refused.....R

(TEXTS:)

A. Your personal information
B. Your credit cards or other accounts. When we talk about the misuse of your personal information in the following questions, please think about the misuse of your credit card or other accounts

6. Can you tell me how long ago it was that you DISCOVERED that your 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.

	Less than 6 months ago	1	
	6 to 11 months ago	2	
	1 year to less than 2 years ago	3	
	2 years to less than 3 years ago	4	
	3 years to less than 4 years ago	5	
	4 years to less than 5 years ago	6	
	5 years to less than 6 years ago, or	7	
	6 or more years ago	8	1
(DO NOT	[Don't know	X	I -> **(SKIP TO QU. 9)**
READ) →	L Refused	R	J

7. 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.)**

	One day or less	1
	More than a day but less than a week	2
	At least a week, but less than one month	3
	1 to 2 months	4
	3 to 5 months	5
	6 to 11 months	6
	1 year to less than 2 years	7
	2 years to less than 3 years	8
	3 years to less than 4 years	9
	4 years to less than 5 years, or	10
	5 or more years	11
(DO NOT	[Don'tknow	X
READ)^	L Refused	R

8. Did you know that someone had taken your personal information without your permission before the misuse began? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE.)**

Yes.....1
No.....2
Don't know.....X
Refused.....R

9. Has the misuse of your personal information stopped, or is someone still misusing your personal information? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE.)**

Misuse has stopped.....1
Still misusing information.....2 1
Don't know.....X I -> **(SKIP TO LOGIC BEFORE QU. 13.)**
Refused.....R J

10. Over what period of time was your information misused? **(READ LIST IF NECESSARY. ENTER SINGLE RESPONSE.)**

	One day or less	1
	More than one day, but less than a week	2
	At least a week, but less than one month	3
	1 to 2 months	4
	3 to 5 months	5
	6 to 11 months	6
	1 year to less than 2 years	7
	2 years to less than 3 years	8
	3 years to less than 4 years	9
	4 years to less than 5 years, or	10
	5 or more years	11
(DO NOT READ)^	[Don'tknow	X
	L Refused	R

11. Is the misuse of your personal information still causing you problems? For example, are you still spending time clearing up credit accounts or your credit report? Or, have you managed to resolve all of the problems caused by the misuse of your information? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE.)**

Still experiencing problems	1
All problems are resolved	2
Did not experience any problems	3
Don't know	X
Refused	R

ASK QU. 12 IF "ALL PROBLEMS ARE RESOLVED" (CODE 2) IN QU, 11; OTHERWISE, SKIP TO LOGIC BEFORE QU. 13.

12. 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.)**

	One day or less	1
	More than one day, but less than a week	2
	At least a week, but less than one month	3
	1 to 2 months	4
	3 to 5 months	5
	6 to 11 months	6
	1 year to less than 2 years	7
	2 years to less than 3 years	8
	3 years to less than 4 years	9
	4 years to less than 5 years, or	10
	5 or more years	11
(DO NOT READ) →	[Don'tknow	X
	L Refused	R

ASK QU. 13 IF "LESS THAN 6 YEARS" CODES 1-7 IN QU. 6; OTHERWISE, TERMINATE.

13. How did you first find out you were a victim of identity theft? **(RECORD VERBATIM. PROBE FOR CLARIFICATION. IF RESPONDENT IS UNSURE, ENCOURAGE BEST GUESS.)**

14. Do you know the identity of the person who misused your personal information without your permission? **(DO NOT READ LIST. ENTER SINGLE RESPONSE.) (INTERVIEWER NOTE: IF RESPONDENT HESTIATES, PROBE:)** "This means you can either personally know the victim or just know the identity of the person, such as their name, etc."

Yes	1		
No	2	1	
Don't know	X	I	-> **(SKIP TO QU. 16)**
Refused	R	J	

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

A Complete Stranger outside your workplace.....1
A Family Member or Relative.....2
Someone at your Workplace.....3
A Friend, Neighbor or In Home Employee.....4
Someone at a Company or Financial Institution
that has your personal information.....5
(ASK LAST) ? [Or, someone else **(SPECIFY)**_____.....6
(DO NOT [Don'tknow.....X
READ)^ L Refused.....R

IF "YES" TO QU. 2; AUTOPUNCH "YES" IN QU. 16 AND SKIP TO QU. 17; OTHERWISE, CONTINUE.

16. Do you know how the person obtained your personal information?

Yes.....1
No.....2 1
Don'tknow.....X I -> **(SKIP TO LOGIC BEFORE QU. 18)**
Refused.....R J

17. How was your personal information obtained? **(RECORD VERBATIM. PROBE FOR CLARIFICATION. IF RESPONDENT IS UNSURE, ENCOURAGE BEST GUESS.)**

QU. 18 & 18a NOT ASKED.

ASK QU. 19 IF "YES" TO QU. 3a; OTHERWISE, SKIP TO QU. 24.

19. You indicated that one or more of your existing accounts other than credit card accounts had been misused. Of those accounts you already had did the person run up charges on, or otherwise misuse, any of the following accounts.

Did the person misuse your… **(INSERT AND RANDOMIZE ACCOUNTS)? (DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE FOR EACH ACCOUNT.)**

	Yes	No	Don't Know	Refused
Checking or Savings Accounts	1	2	X	R
Insurance Accounts, including Medical, Auto, and Life	1	2	X	R
Internet or E-Mail Accounts	1	2	X	R

ASK QU. 19a FOR EACH "ACCOUNT" MENTIONED IN QU. 19; OTHERWISE, SKIP TO QU. 20.

19a. How many of your **(INSERT AND RANDOMIZE ACCOUNTS)** were affected? **(ENTER EXACT NUMBER FROM 1 TO 25. DO NOT ACCEPT RANGE. IF RESPONDENT IS UNSURE, ENCOURAGE BEST GUESS.)**

_ _ _ _ _ **(V A L I D RANGE 1 TO 25)**
Don't know.....X
Refused.....R

(ACCOUNTS:)
Checking or Savings Accounts
Insurance Accounts, including Medical, Auto, and Life
Internet or E-Mail Accounts

20. Did the person run up charges on, or otherwise misuse, your telephone service accounts? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE.)**

Yes.....1
No.....2 1
Don't know.....X I -> **(SKIP TO QU. 22)**
Refused.....R J

20a. How many of those were Wireless Telephone Service Accounts? **(ENTER EXACT NUMBER FROM 0 TO 25. DO NOT ACCEPT A RANGE.)**

_ _ _ _ _ **(V A L I D RANGE 0 TO 25)**
Don't know.....X
Refused.....R

20b. How many of those were conventional Telephone Service Accounts, whether local or long distance? **(ENTER EXACT NUMBER FROM 0 TO 25. DO NOT ACCEPT A RANGE.)**

_ _ _ _ _ **(V A L I D RANGE 0 TO 25)**
Don't know.....X
Refused.....R

QU. 21 NOT ASKED.

22. Did the person run up charges on, or otherwise misuse any other accounts that you had? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE.)**

Yes.....1
No.....2 1
Don't know.....X -> **(SKIP TO QU. 23)**
Refused.....R J

22a. What type of other charges did the person run up or otherwise misuse for any other accounts that you had? **(RECORD VERBATIM. PROBE FOR CLARIFICATION. IF RESPONDENT IS UNSURE, ENCOURAGE BEST GUESS.)**

22b. How many of these other accounts were affected? **(ENTER EXACT NUMBER FROM 1 TO 25. DO NOT ACCEPT A RANGE.)**

_____**(VALID RANGE 1 TO 25)**
Don't know.....X
Refused.....R

QU. 23 NOT ASKED.

24. Did the person use your information to obtain any **(INSERT AND RANDOMIZE ACCOUNT)? (DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE FOR EACH ACCOUNT.)**

	Yes	No	Don't Know	Refused
New Credit Card Accounts, whether bank cards or cards that were issued by a particular store	1	2	X	R
New Checking or Savings Accounts	1	2	X	R
NewLoans	1	2	X	R
New insurance policies	1	2	X	R
New Internet or Email Accounts	1	2	X	R

ASK QU. 24b FOR EACH ACCOUNT MENTIONED IN QU. 24; OTHERWISE, SKIP TO QU. 25.

24b. How many **(INSERT AND RANDOMIZE ACCOUNTS)** were obtained using your information? **(ENTER EXACT NUMBER FROM 1 TO 25. DO NOT ACCEPT A RANGE. IF RESPONDENT IS UNSURE, ENCOURAGE BEST GUESS.)**

_ _ _ _ _ **(V A L I D RANGE 1 TO 25)**
Don't know.....X
Refused.....R

(ACCOUNTS:)
New Credit Card Accounts
New Checking or Savings Accounts
New Loans
New insurance policies
New Internet or Email Accounts

25. Did the person open any NEW telephone service accounts? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE.)**

Yes.....1
No.....2 1
Don't know.....X I -> **(SKIP TO QU. 27)**
Refused.....R J

25a. How many of these were new wireless telephone accounts? (ENTER EXACT NUMBER FROM 0 TO 25. DO NOT ACCEPT RANGE. IF RESPONDENT IS UNSURE, ENCOURAGE BEST GUESS.)

_ _ _ _ (V A L I D RANGE 0 TO 25)
Don't know.....X
Refused.....R

25b. How many of these were conventional telephone accounts, whether local or long distance service? (ENTER EXACT NUMBER FROM 0 TO 25. DO NOT ACCEPT RANGE. IF RESPONDENT IS UNSURE, ENCOURAGE BEST GUESS.)

_ _ _ _ _ (V A L I D RANGE 0 TO 25)
Don't know.....X
Refused.....R

QU. 26 NOT ASKED.

27. Did the person open any other accounts? (DO NOT READ LIST. ENTER SINGLE RESPONSE.)

Yes.....1
No.....2
Don't know.....X
Refused.....R

ASK QU. 27a IF "YES" IN QU. 27; OTHERWISE SKIP TO LOGIC BEFORE QU. 28.

27a. What type of other accounts did the person OPEN? **(RECORD VERBATIM PROBE FOR CLARIFICATION.)**

27b. How many other accounts did the person open? **(ENTER EXACT NUMBER FROM 1 TO 25. DO NOT ACCEPT RANGE. IF RESPONDENT IS UNSURE, ENCOURAGE BEST GUESS.)**

 # _ _ _ _ _ (V A L I D RANGE 1 TO 25)
Don't know.....X
Refused.....R

ASK QU. 28 IF "YES" IN QU. 4 OR "YES" IN QU. 3a, OTHERWISE, SKIP TO QU. 29.

28. As far as you know, did the person use your information in any of the following ways?

Did the person... **(INSERT AND RANDOMIZE)? (DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE FOR EACH.)**

		Yes	No	Don't Know	Refused
	File a fraudulent tax return	1	2	X	R
	Obtain medical care	1	2	X	R
	Obtain employment	1	2	X	R
	Provide your name and identifying information to law enforcement when they were caught and charged with a crime	1	2	X	R
	Rent an apartment or house	1	2	X	R
(ALWAYS ASK LAST)→	Obtain a drivers license, social security card or other government documents	1	2	X	R
(ALWAYS ASK LAST)→	[Do anything else **(SPECIFY)**_____	**1**	**2**	**X**	**R**

29. 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 have obtained. (READ LIST IF NECESSARY. ENTER SINGLE RESPONSE.) (INTERVIEWER NOTE: IF $1,000 OR OVER, PLEASE PROBE:) I just want to verify that the total amount is (INSERT AMOUNT)?

	Less than $100	1
	$100-$499	2
	$500-$999	3
	$1,000-$4,999	4
	$5,000 - $9,999	5
	$10,000-$24,999	6
	$25,000 - $49,999	7
	$50,000 - $99,999, or	8
	$100,000 or more	9
(DO NOT READ)^	[Don'tknow	X
	L Refused	R

30. How much money did you pay out of pocket as a result of the identity theft? In thinking about this answer, include costs for things such as postage, copying, notarizing documents, and legal fees, as well as payment of any fraudulent debts in order to avoid further problems. **(READ LIST IF NECESSARY. ENTER SINGLE RESPONSE.) (INTERVIEWER NOTE: IF $1,000 OR OVER, PLEASE PROBE:)** I just want to verify that the total amount is **(INSERT AMOUNT)?**

	$0	1
	Less than $50	2
	$50-$99	3
	$100-$499	4
	$500-$999	5
	$1,000-$4,999	6
	$5,000 - $9,999	7
	$10,000 or more	8
(DO **NOT**	[Don'tknow	X
READ)^	L Refused	R

31. How many hours of your own time have you spent resolving credit, financial, and other problems caused by the theft of your information? **(READ LIST IF NECESSARY. ENTER SINGLE RESPONSE.)**

	1 hour or less	1
	2 to 9 hours	2
	10 to 39 hours	3
	40 to 79 hours	4
	80 to 159 hours	5
	160 to 239 hours	6
	240 hours or more	7
(DO **NOT**	[Don'tknow	X
READ)^	L Refused	R

32. What other types of problems have you experienced as a result of the improper use of your personal information?

Have you...**(INSERT AND RANDOMIZE)? (DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE FOR EACH.)**

		Yes	No	Don't Know	Refused
	Been turned down for a loan	1	2	X	R
	Had banking problems, such as being turned down for a checking or savings account, or having checks rejected for insufficient funds or because your name appeared on a bad check list	1	2	X	R
	Had credit problems, such as being turned down for a credit card, having an account closed by the issuer, paying a higher interest rate, or having a credit card rejected when you sought to use it	1	2	X	R
	Had phone or utilities cut off or been denied new service	1	2	X	R
	Been turned down for insurance or had to pay higher rates	1	2	X	R
	Been harassed by a debt collector or creditor	1	2	X	R
	Had a civil suit filed against you or a judgment entered against you	1	2	X	R
(ALWAYS ASK LAST) ->	Been the subject of a criminal investigation, warrant, proceeding, or conviction	1	2	X	R
(ALWAYS ASK LAST) ->	Had any other types of problems **(SPECIFY)**_____	**1**	**2**	**X**	**R**

33. Did you contact anyone in attempting to report or resolve this incident? **(DO NOT READ LIST. ENTER SINGLE RESPONSE.)**

Yes.....1
No.....2 1
Don't know.....X -> **(SKIP TO QU. 34)**
Refused.....R J

33a. Whom did you contact?

Did you... **(INSERT AND RANDOMIZE)? (DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE FOR EACH.)**

		Yes	No	Don't Know	Refused
	Consult a lawyer or other professional	1	2	X	R
	Notify one or more companies where an account was opened or misused, including a company that issued a credit card	1	2	X	R
	Notify one or more credit reporting agencies	1	2	X	R
	Notify the Department of Motor Vehicles	1	2	X	R
(ALWAYS ASK IN THIS ORDER) →	Notify the State Attorney General or a state or local consumer agency	1	2	X	R
	Notify the FTC	1	2	X	R
	Notify another federal agency **(SPECIFY)**_____	1	2	X	R
(ALWAYS ASK LAST) →	Notify your local police or the local law enforcement in another jurisdiction	1	2	X	R
	Contact or notify someone else **(SPECIFY)**_____	1	2	X	R

ASK QU. 34 IF "YES" TO QU. 1 OR "YES" TO "NEW CREDIT CARD ACCOUNT OPENED" IN QU. 24 AND THE SUM OF QU. 1a AND THE NUMBER GIVEN FOR "NEW CREDIT CARD ACCOUNT OPENED IN QU. 24b IS EQUAL TO 1; OTHERWISE, SKIP TO LOGIC BEFORE QU. 34a.

34. How satisfied were you with the response of the credit card company when you reported that your personal information had been misused? **(READ LIST. ENTER SINGLE RESPONSE.)**

	Very satisfied	4	
	Somewhat satisfied	3	
	Somewhat dissatisfied	2	
	Very dissatisfied	1	? **(SKIP TO QU. 35)**
(DO NOT	f Don't know	X	
READ) ->	L Refused	R	

IF "YES" TO QU. 1 OR "YES" TO "NEW CREDIT CARD ACCOUNT OPENED" IN QU. 24 AND THE SUM OF QU. 1a AND NUMBER GIVEN FOR "NEW CREDIT CARD ACCOUNT OPENED" IN QU. 24b IS GREATER THAN ONE; OTHERWISE, SKIP TO LOGIC BEFORE QU. 35.

34a. Thinking about the result of your contact with the credit card companies, would you say you were..**(READ LIST.)? (ENTER SINGLE RESPONSE.)**

	Satisfied with the responses of all of the companies when you reported that your personal information had been misused	3
	Satisfied with the responses of some of the companies, but not others, or	2
	Dissatisfied with the responses of all of the Com panies	1
(DO **NOT**	[Don't know	X
READ)^	L Refused	R

ASK QU. 35 IF "YES", "NOTIFIED ONE OR MORE CREDIT REPORTING AGENCIES" IN QU. 33a; OTHERWISE, SKIP TO LOGIC BEFORE QU. 41.

35. How long after you learned someone was using your personal information did you first contact any of the credit reporting agencies? **(READ LIST IF NECESSARY.) (ENTER SINGLE RESPONSE.)**

	One day or less	1
	More than one day, but less than a week	2
	At least a week, but less than one month	3
	1 to 5 months	4
	6 to 11 months	5
	1 year to less than 2 years, or	6
	2 years or more	7
(DO NOT READ)^	[Don'tknow	X
	L Refused	R

36. How many credit reporting agencies did you contact? **(READ LIST. ENTER SINGLE RESPONSE.)**

	One	1	
	Two	2	1
	Three, or	3	|-> **(SKIP TO QU. 37a)**
	More than three	4	J
(DO NOT	[Don'tknow	X	1
READ) ->	L Refused	R	J -> **(SKIP TO QU. 38)**

37. How satisfied were you with the responses of the credit reporting agency when you reported that your personal information had been misused? **(READ LIST. ENTER SINGLE RESPONSE.)**

	Very satisfied	4	1
	Somewhat satisfied	3	
	Somewhat dissatisfied, or	2	**>(SKIP TO QU. 38)**
	Very dissatisfied	1	
(DO **NOT**	[Don'tknow	X	
READ)^	L Refused	R	J

ASK QU. 37a IF CODES (2-4) TWO TO MORE THAN THREE IN QU. 36; OTHERWISE, SKIP TO QU. 38.

37a. Thinking about the result of your contact with the credit reporting agencies, would you say you were... **(READ LIST. ENTER ENTER SINGLE RESPONSE.)**

	Satisfied with the responses of all of the agencies when you reported that your personal information had been misused	3
	Satisfied with the responses of some of the agencies, but not others, or	2
	Dissatisfied with the responses of all of the agencies	1
(DO **NOT**	[Don'tknow	X
READ)^	L Refused	R

38. Was a fraud alert placed on your credit report? **(DO NOT READ LIST. ENTER SINGLE RESPONSE.)**

Yes	1	
No	2	1
Don't know	X	I -> **(SKIP TO QU. 41)**
Refused	R	J

ASK QU. 39 IF QU. 36 IS "TWO, "THREE" OR "MORE THAN THREE" (CODES 2-4) AND "YES" TO QU. 38.

IF QU. 36 IS "ONE" AND QU. 38 IS "YES", AUTOPUNCH ONE IN QU. 39 AND CONTINUE TO QU. 40. ANSWER GIVEN IN QU. 39 MUST BE EQUAL TO OR LESS THAN ANSWER GIVEN IN Qu.36.

39. At how many of the credit reporting agencies you contacted was a fraud alert placed on your credit report? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE FOR EACH.)**

One	1	
Two	2	
Three	3	
More than Three	4	
(DO NOT READ)^ [Don'tknow	X	
L Refused	R	

40. Did the person who took your personal information successfully open any additional accounts after you placed the fraud alert on your credit report? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE FOR EACH.)**

Yes	1
No	2
Don't know	X
Refused	R

ASK QU. 41 IF QU. 33a "CONTACTED THE LOCAL POLICE OR OTHER LOCAL LAW ENFORCEMENT AGENCY"; OTHERWISE, SKIP TO QU. 43.

41. Did your local law enforcement agency take a police report from you about your identity theft? **(DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE FOR EACH.)**

Yes.....1
No.....2
Don't know.....X
Refused.....R

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

Very satisfied.....4
Somewhat satisfied.....3
Somewhat dissatisfied, or.....2
Very dissatisfied.....1
(DO **NOT READ)^** [Don'tknow.....X
L Refused.....R

43. How concerned are you that the identity thief will start to misuse your information again? **(READ LIST. ENTER SINGLE RESPONSE.)**

	Very concerned	4
	Somewhat concerned	3
	Not very concerned, or	2
	Not at all concerned	1
(DO NOT READ)^	[Don't know	X
	L Refused	R

ASK QU. 44 IF QU. 31 IS 10 HOURS OR GREATER (CODES 3-7); OTHERWISE, TERMINATE.

44. What is the MOST IMPORTANT action or resource that would have helped you fix your problems more easily? **(RECORD VERBATIM. PROBE FOR CLARIFICATION. IF RESPONDENT IS UNSURE, ENCOURAGE BEST GUESS.)**

Appendix B: Methodology Description

Federal Trade Commission

TeleNation Methodology
** *
An Overview

SAMPLE

Each week TeleNation completes 3 national telephone surveys. Each survey (wave of TeleNation) consists of a minimum of 1,000 interviews with adults 18 years of age or older; 481 males and 519 females. TeleNation uses a single-stage, random digit-dial (RDD) sample technique to select each sample from all available residential telephone numbers in the contiguous United States. This non-clustered approach insures true random selection among all telephone numbers and provides a truly independent sample for each wave. Up to three attempts are made on the selected telephone numbers.

INTERVIEW

TeleNation interviews are conducted over a 3 day period via Synovate's CATI network through its Telephone Research Services. TeleNation employs AUTOQUEST®, Synovate's computer assisted telephone interviewing system, to conduct telephone interviews. This CATI software insures consistent execution of the questionnaire and efficient sample management. The interview, itself, consists of non-competing client-specific questions and a shared set of standard demographic questions. TeleNation provides transitional phrases between survey segments to insure smooth interview flow.

TABULATION

TeleNation survey results are tabulated by two standard demographic banners.

A. GENDER, AGE, INCOME, MARITAL STATUS, CHILD IN HOUSEHOLD
B. REGION, RACE, EDUCATION, EMPLOYMENT STATUS, PRIMARY GROCERY SHOPPER, HOME OWNERSHIP, INTERNET ACCESS

TeleNation's standard data tabulations are provided in a weighted format. The data are weighted on an individual multi-dimensional basis to give appropriate representation of the interaction between various demographic factors. The multi-dimensional array covers age within income, within the four national census regions, within gender, resulting in 160 different cells. The current population survey from the U.S. Census Bureau is used to determine the weighting targets for each of these 160 cells.