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

Exhibit F - Part 1 of 2

Exhibit F

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.**

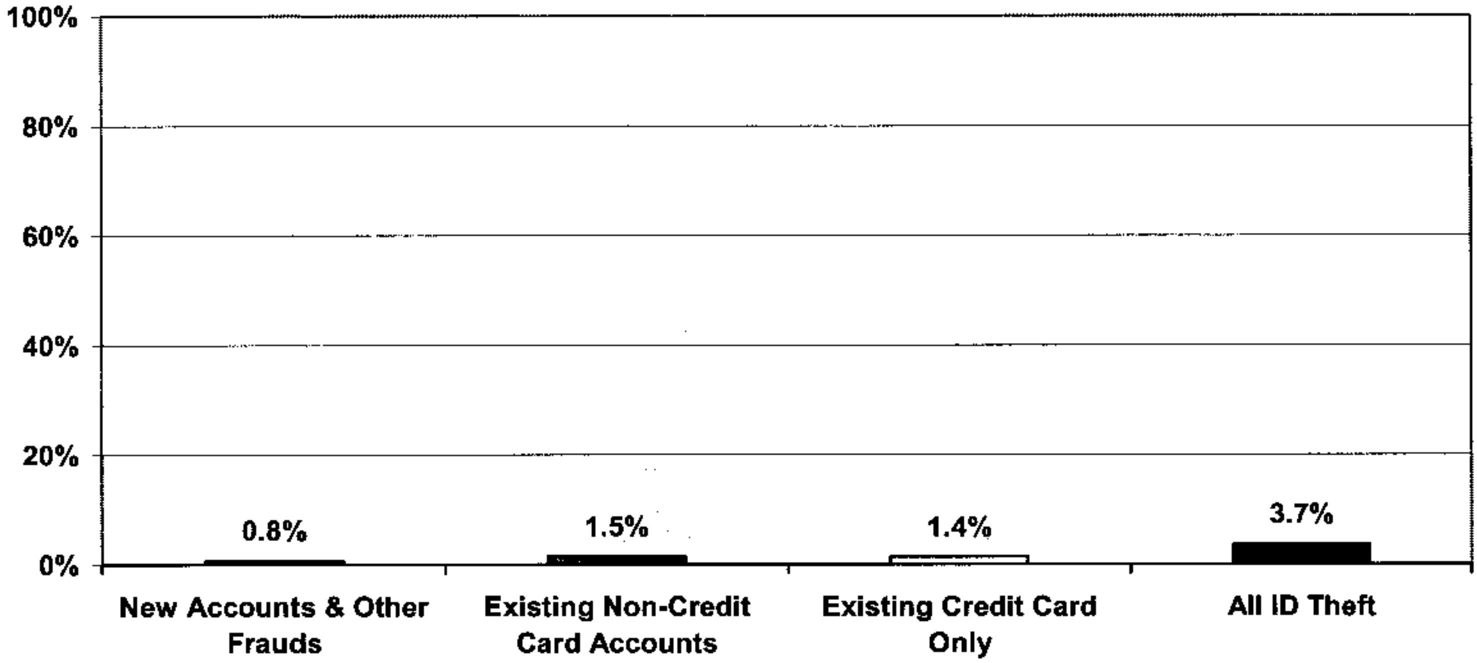
  The 2003 survey found that victims had, on average, out-of-pocket expenses of $500. In the 2006 survey, the average victim loss was $371. The same methodological differences that pertain to the amount the thief obtained also apply to these average loss estimates, that is, measuring loss as a range versus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

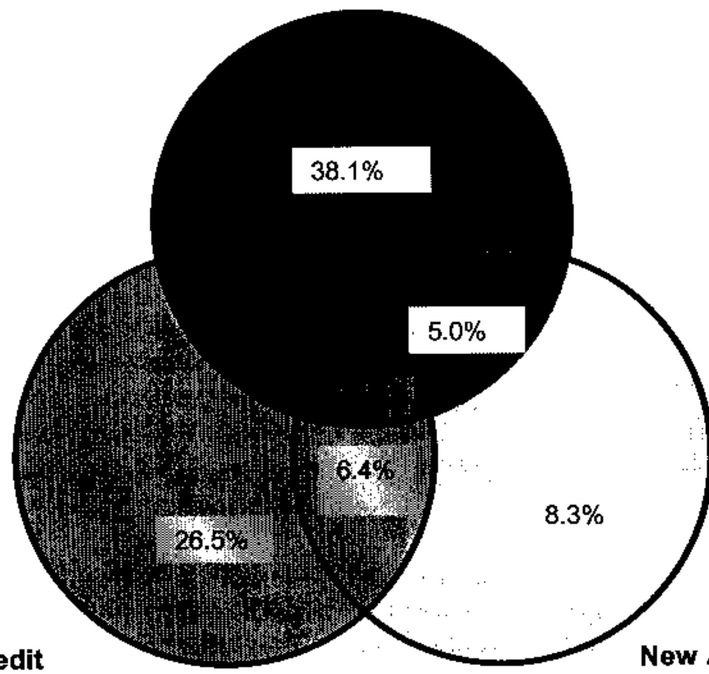
- The "New Accounts & Other Frauds" category is considered to be the most serious, followed by the "Existing Non-Credit Card Accounts" category. "Existing Credit Cards Only" is considered the least serious type of victimization. Placing victims in only one category means that, for example, victims who 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

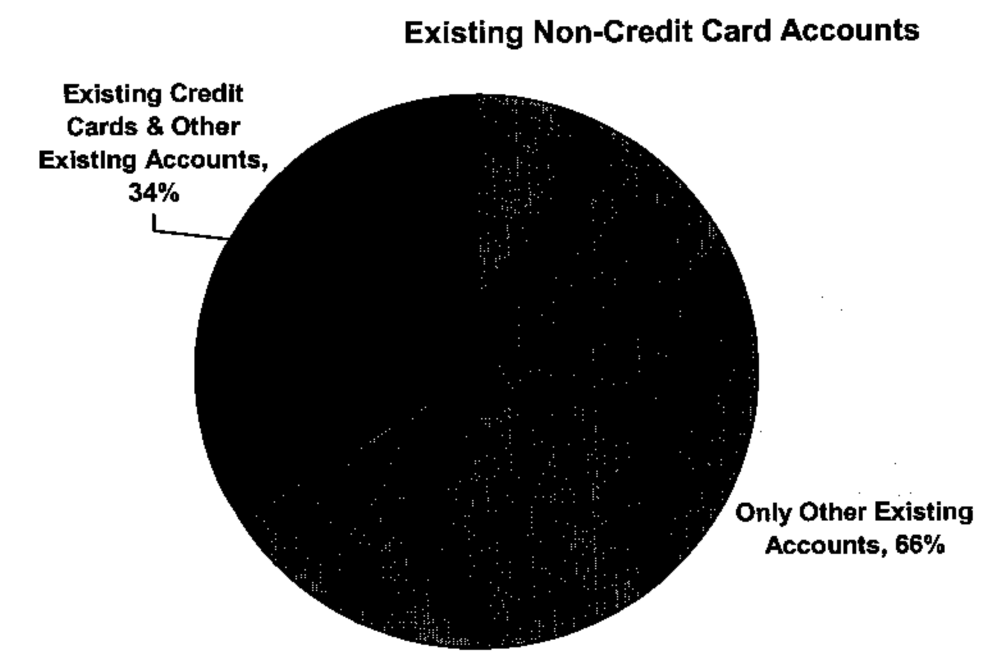


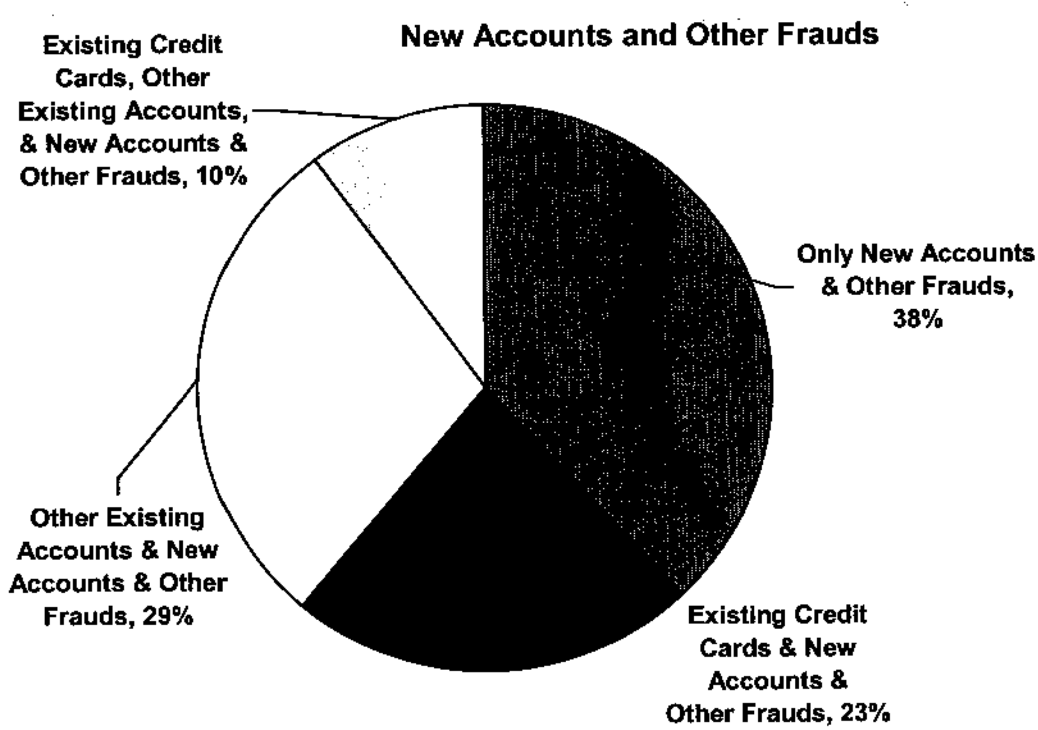
- For most purposes, this report groups victims according to the most serious form of ID theft that they suffered. However, many victims suffer multiple types of ID theft, and this diagram illustrates the overlap in types.
- 58.9% of all victims experienced the misuse of an existing credit card.
- A 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



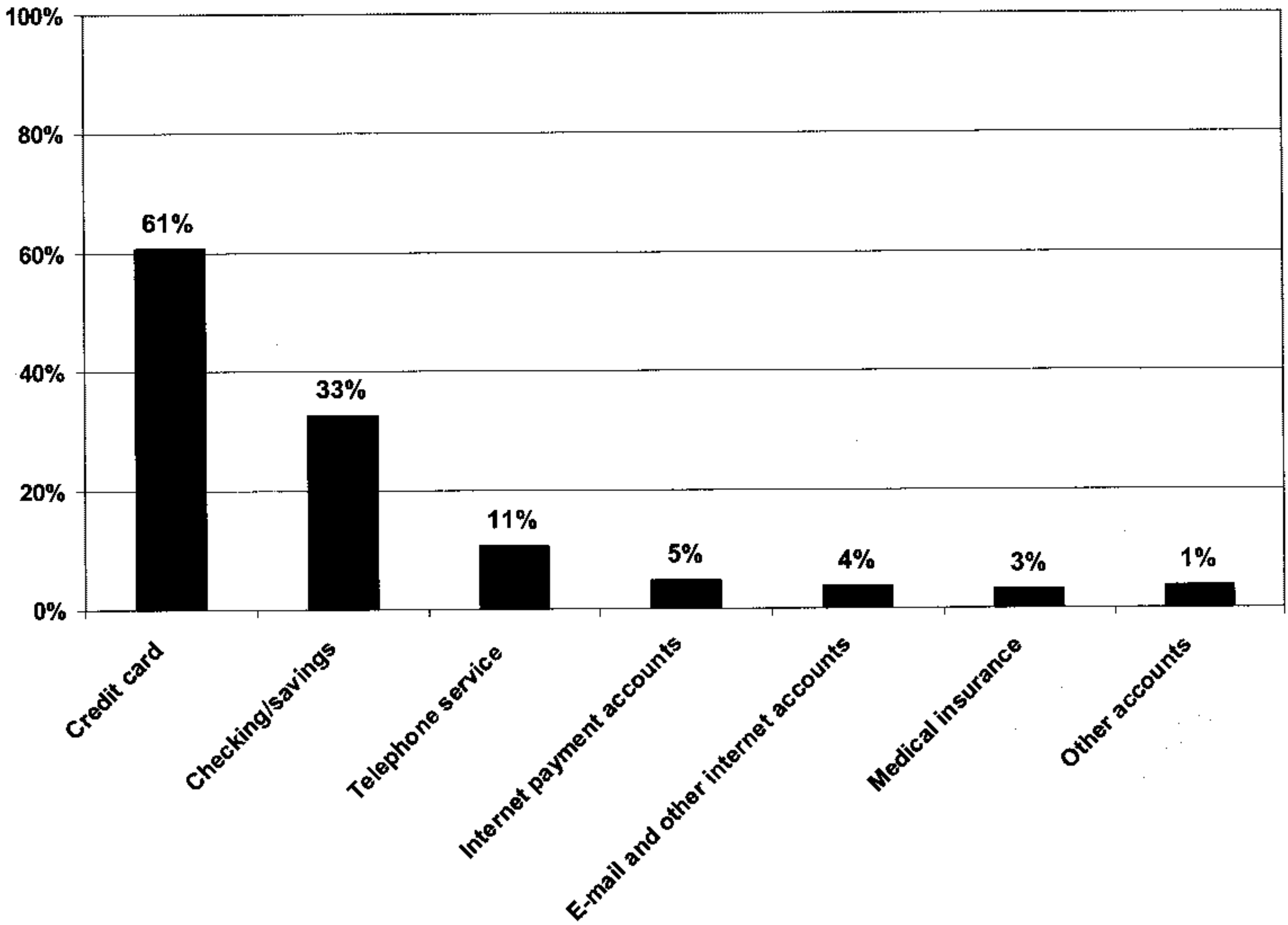


- As mentioned above, each victim is classified as belonging to only one of the categories of ID Theft, based on the most serious problem the victim reported. Some victims in the two more serious categories have had their information misused in ways that relate to more than one category.

- 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.

---

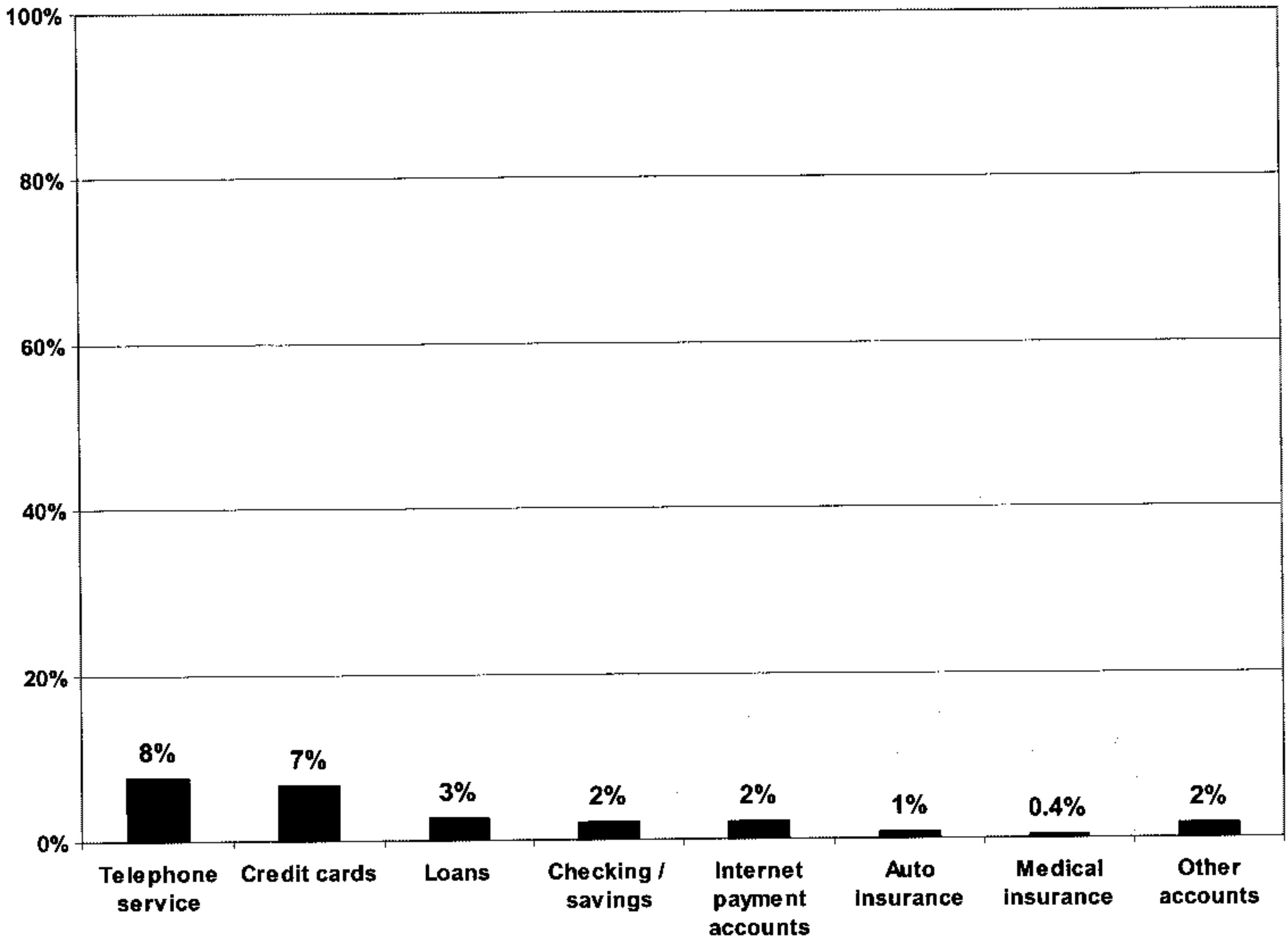
[4] The figures on this and the succeeding pages are based on the responses of all survey participants who reported discovering the misuse of their personal information between the beginning of 2001 and when they were interviewed—a total of 559 individuals. The data in Figures 1-3 are based only on those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

---

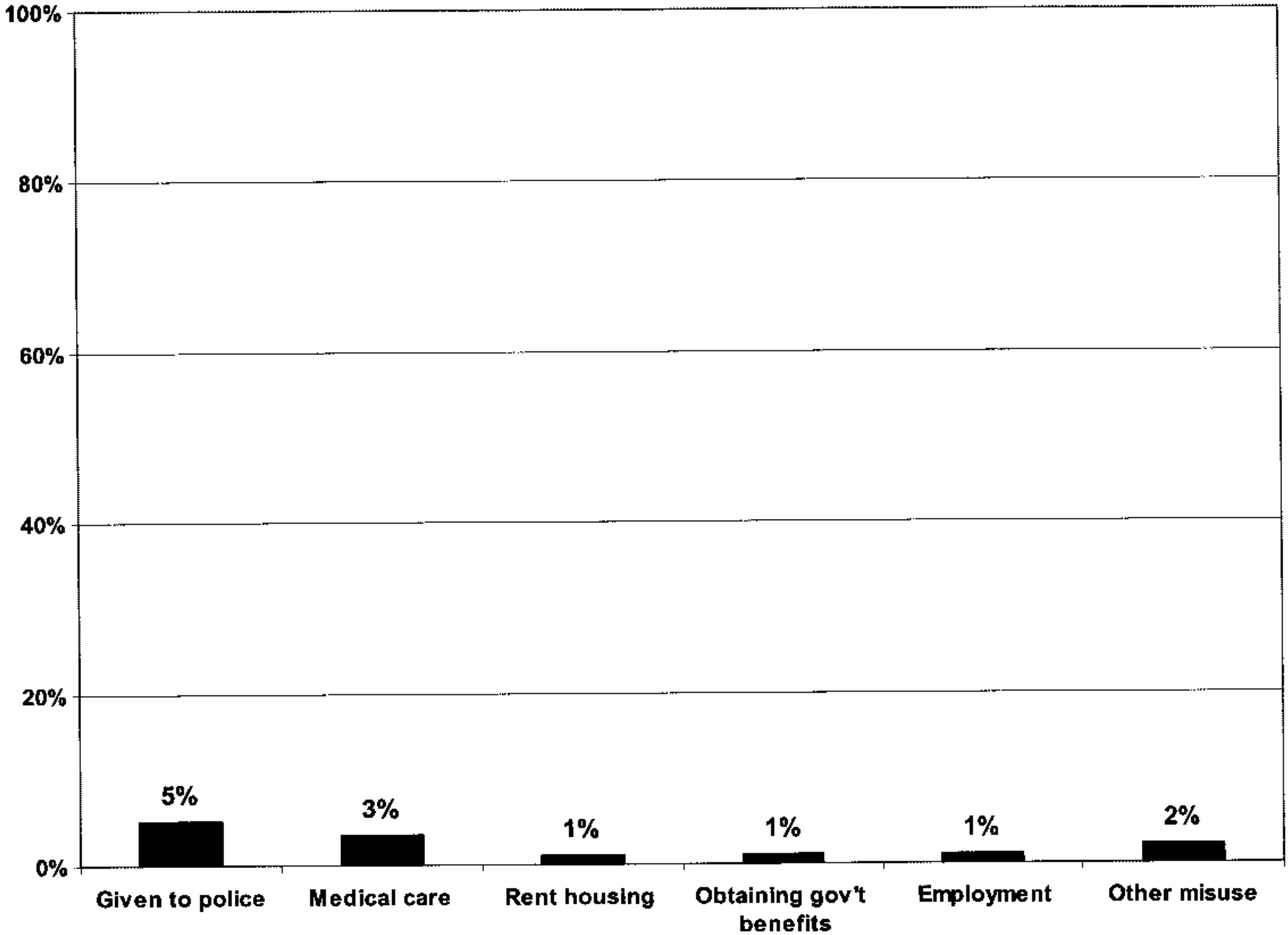
[7] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed.

[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]



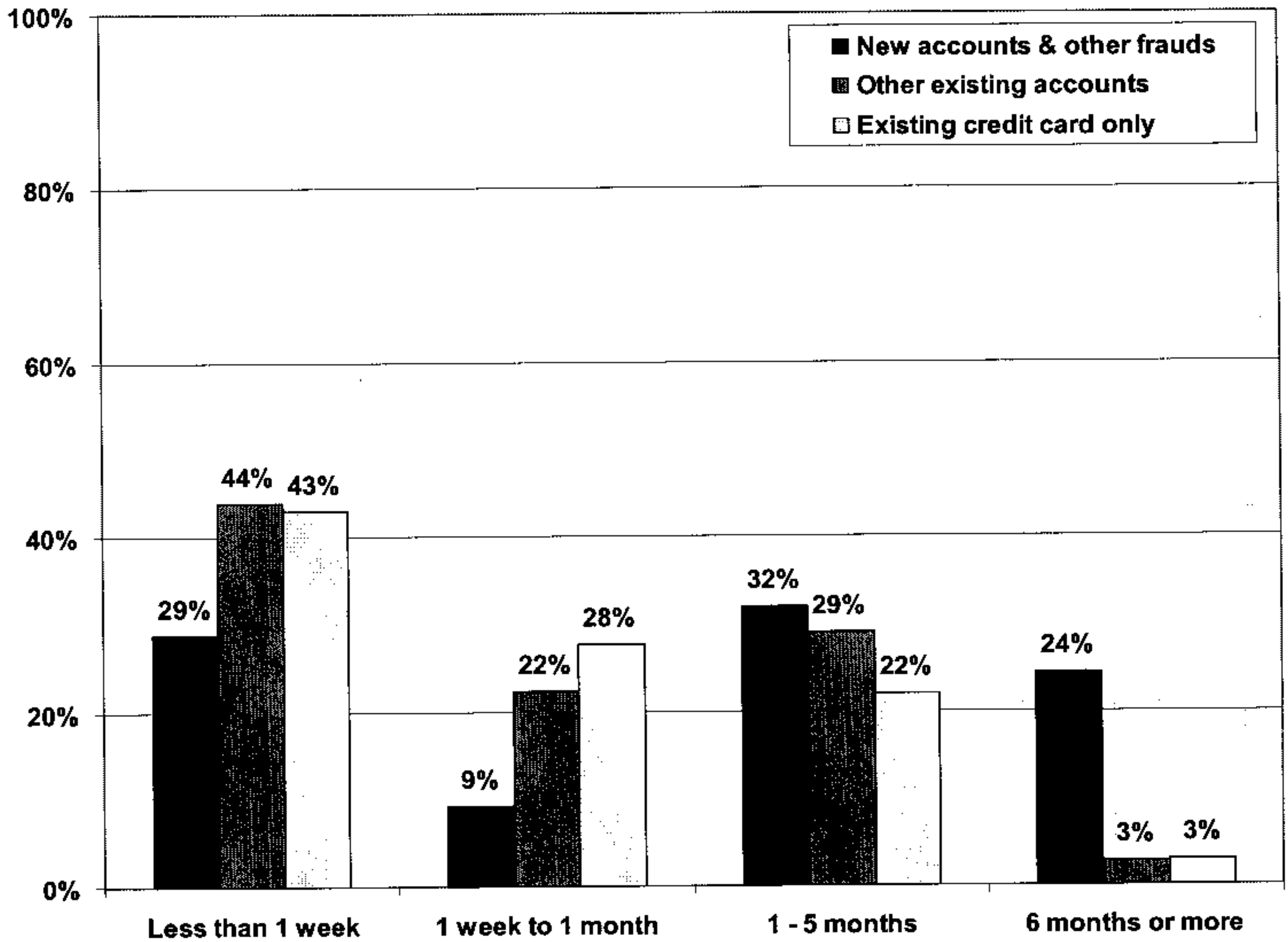
- Twelve percent of victims reported one or more misuse other than accessing new or existing financial accounts in the victim's name, and specified what type(s) of fraudulent activities were committed. The most common forms of non-account misuse were:
  - Five percent of victims said that they were aware 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.

---

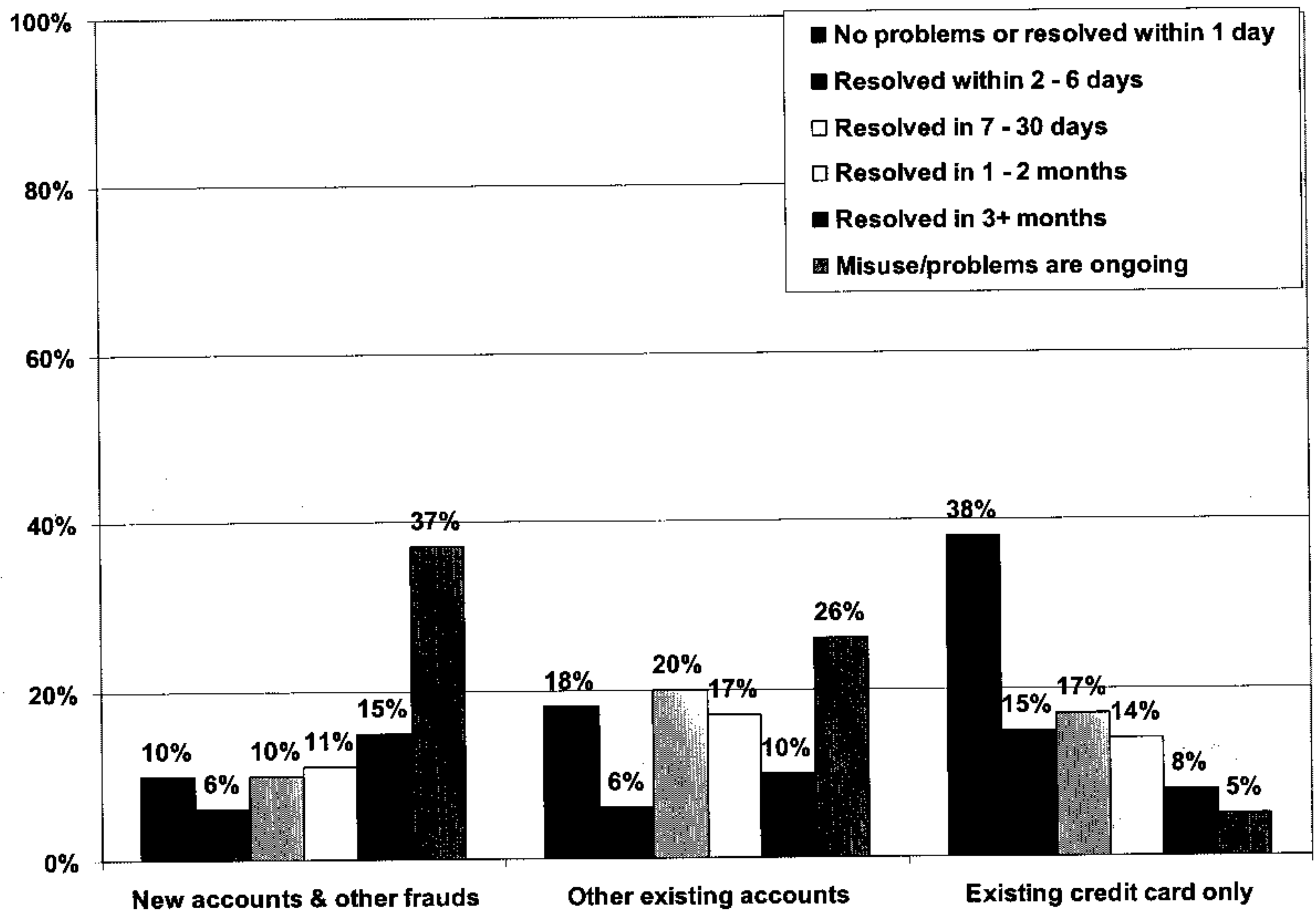
[11] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed. Figures for Existing Credit Cards Only, Existing Non-Credit Card Accounts, and New Accounts & Other Frauds are 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]



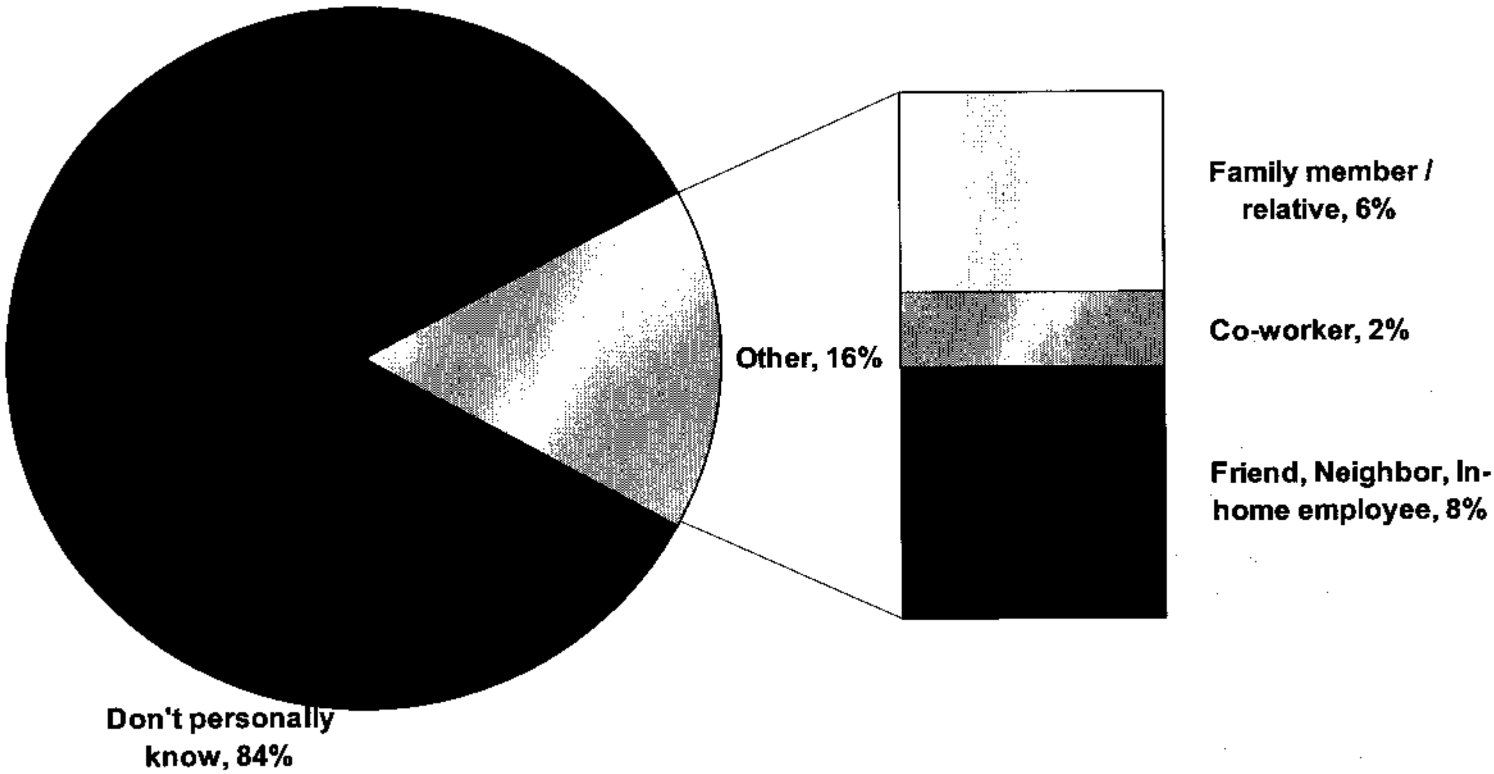
- Almost one-quarter of all victims (23%) said that either they had no problems or they were able to resolve any problems experienced as a result of being a victim of ID theft within one day of discovering that their personal information was being misused.
  - While 38% of victims in the Existing Credit 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]



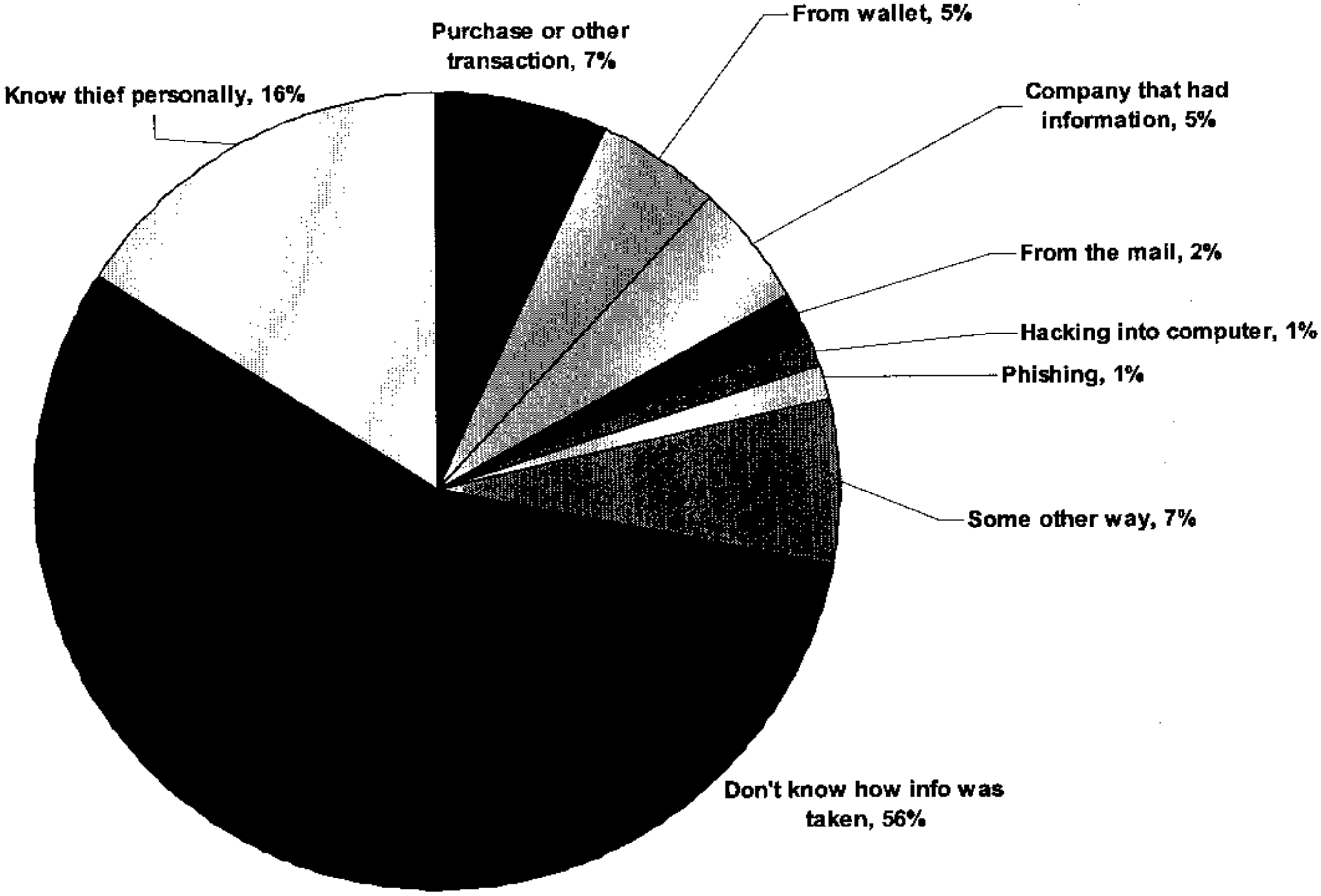
- ID theft victims generally are either unaware of the identity of the thief or do not personally know the thief. Over three-quarters of all ID theft victims (84%) reported that he or she did not personally know the thief, regardless of whether they had information about the thief's identity.
- Sixteen 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.

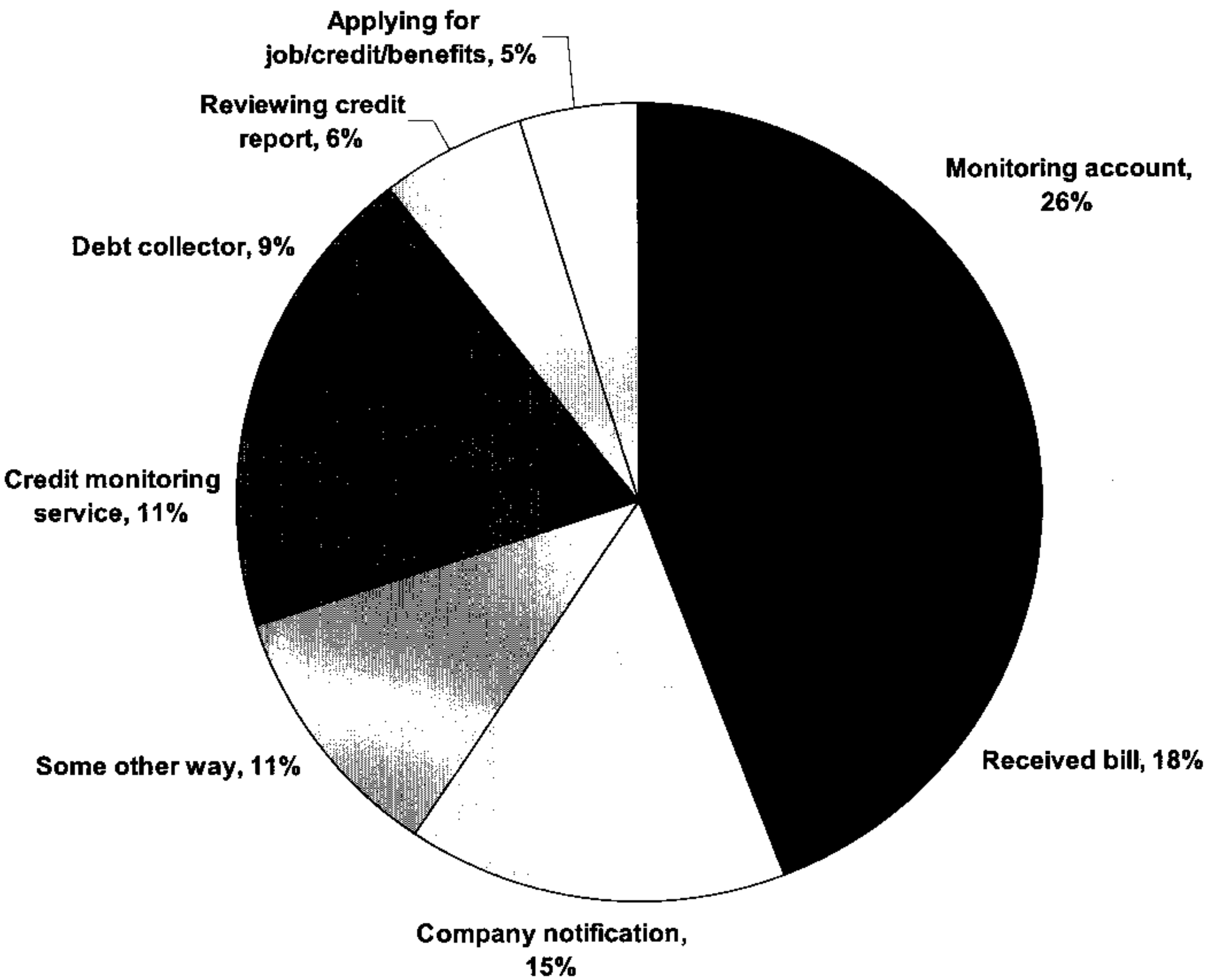
[17] The remaining 1% of respondents either refused to answer or stated that they did not know whether they knew how their information was obtained.

- 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]

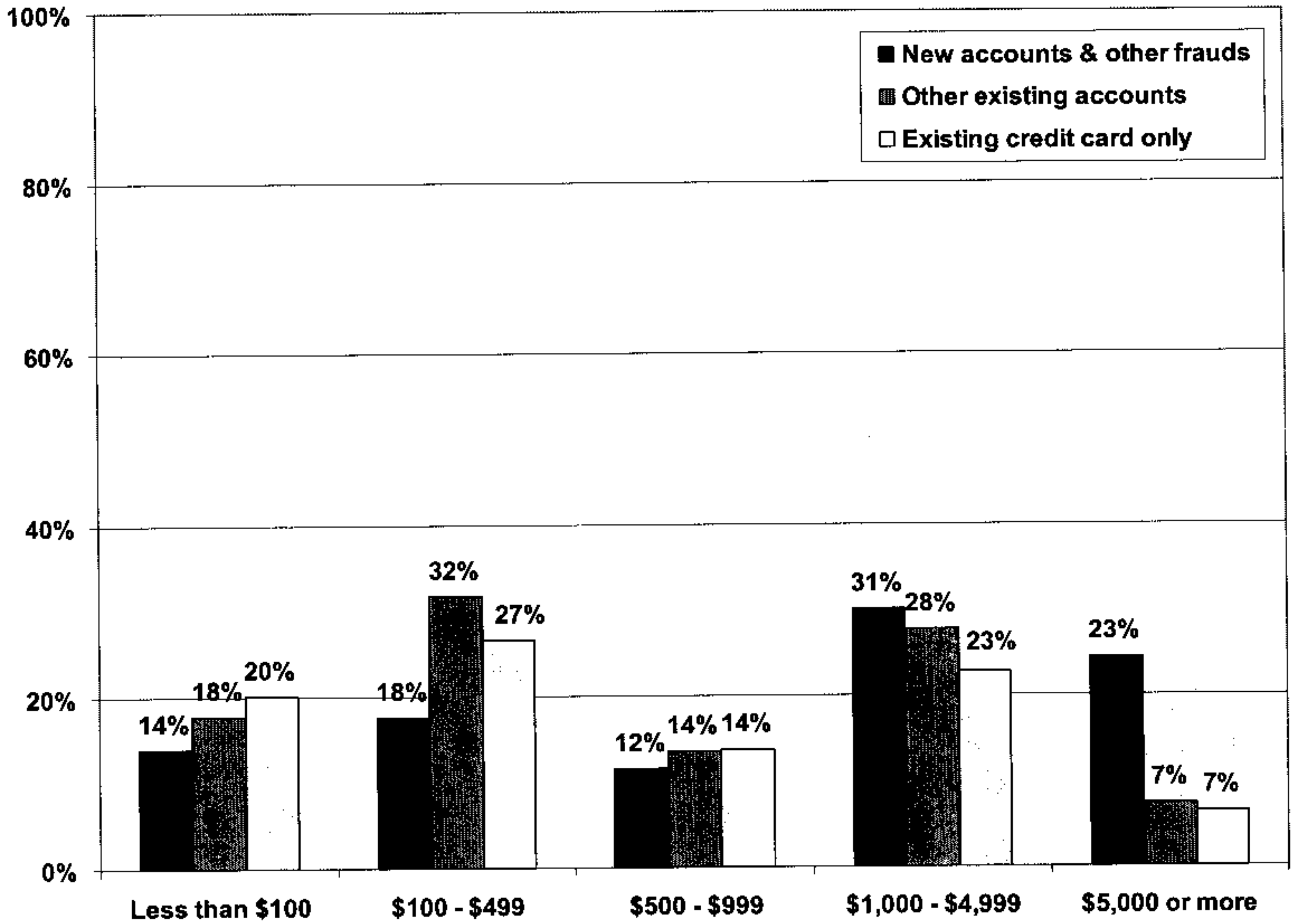
- In the Existing Non-Credit Card Accounts category, 41% of victims said that they discovered the misuse by monitoring their accounts.

- 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]



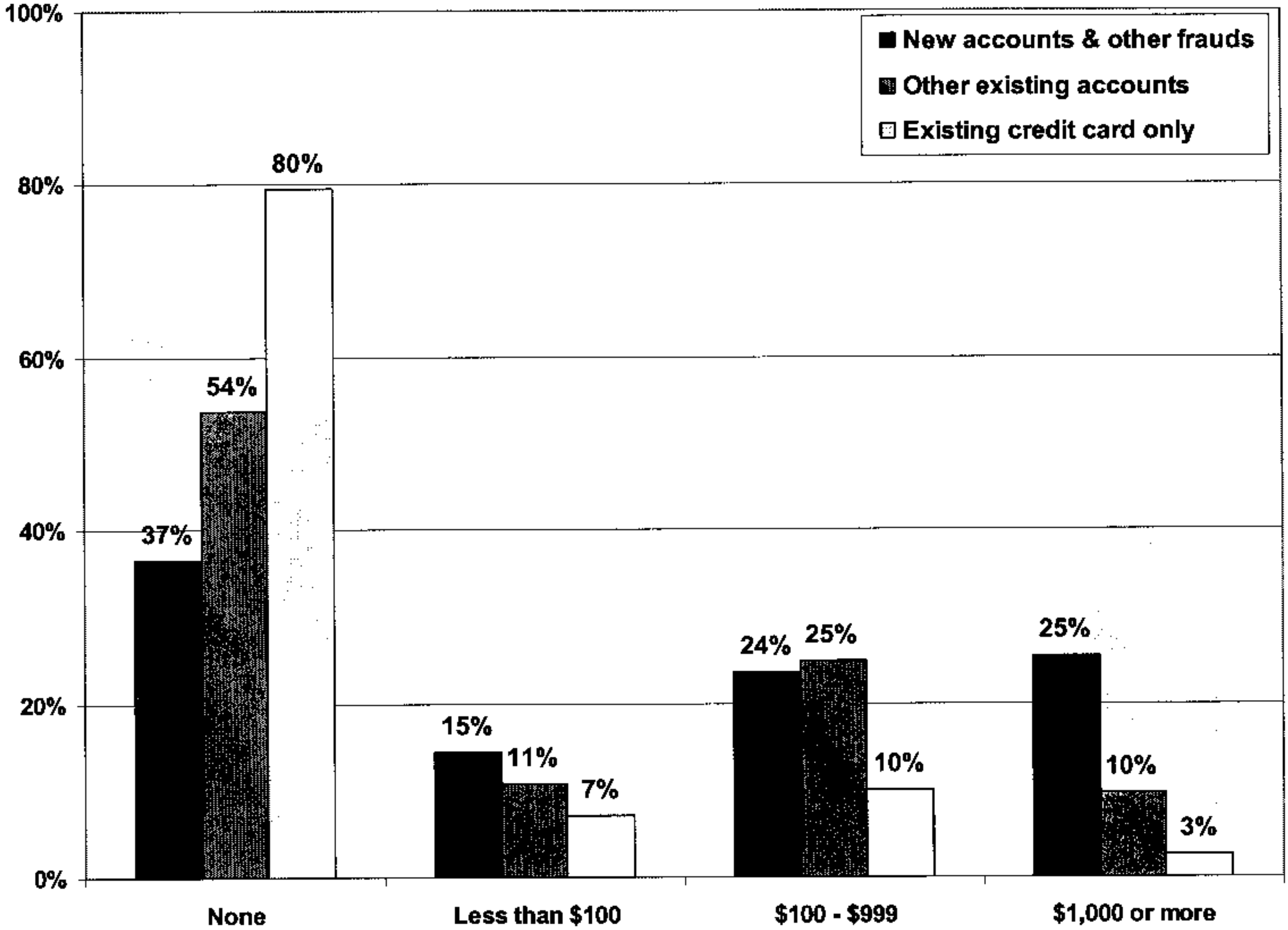
- Victims were asked to estimate the value of the goods and services that the thief obtained from businesses, including financial institutions, using the victim's personal information. These figures include amounts where the business assumed the loss and amounts where the victim actually paid the debt 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]



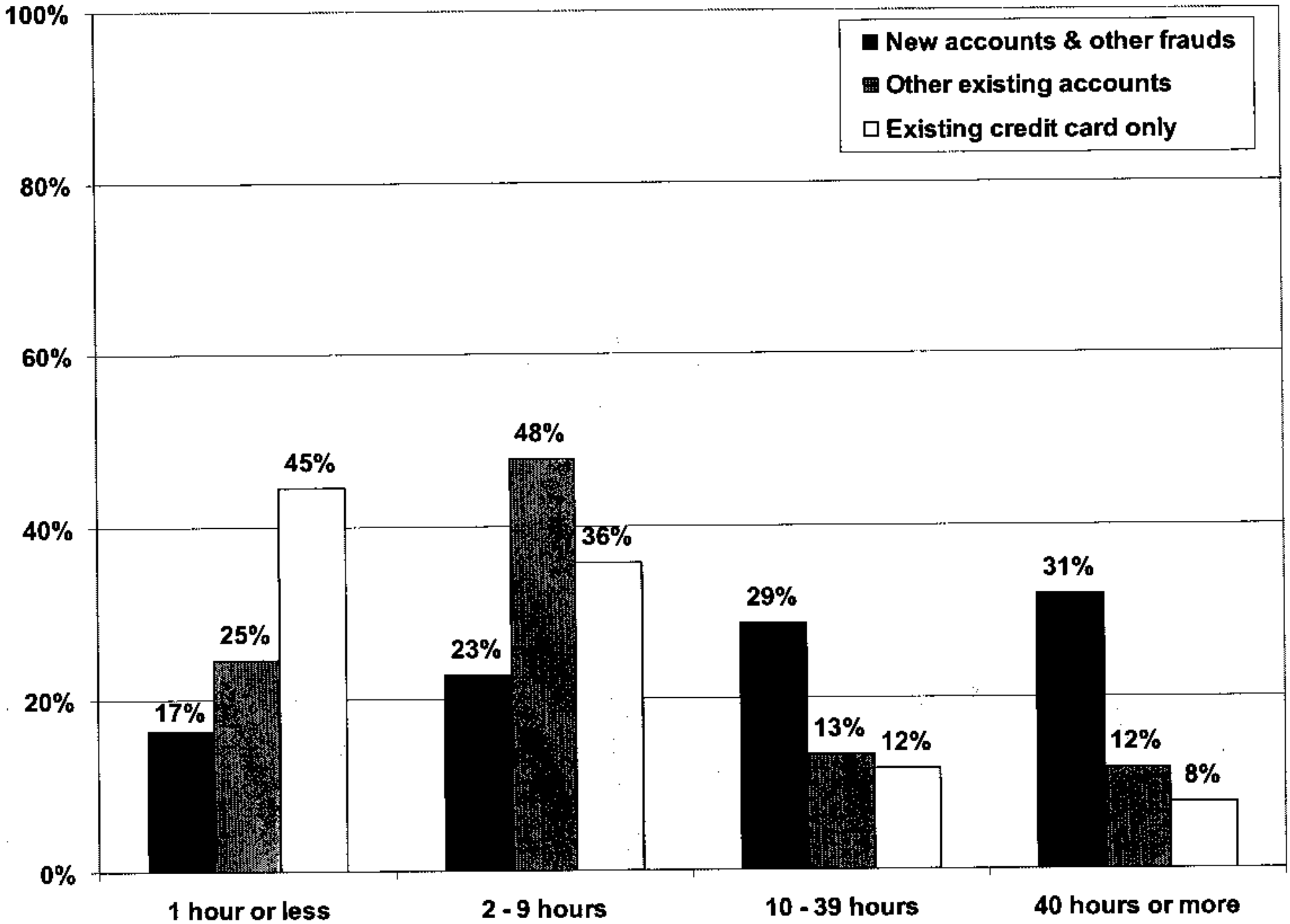
- Survey participants were asked about their total out-of-pocket expenses, which include lost wages, legal fees, and payments of any fraudulent debts, as well as miscellaneous expenses such as postage and notarization fees.
- The majority of victims (59%) incurred no out-of-pocket expenses.

[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]
  - Nineteen percent said that they spent 10 or more hours resolving problems related to ID theft.
  - Nineteen percent said that they experienced one or more of the other types of problems included in Figure 15.
  - 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]

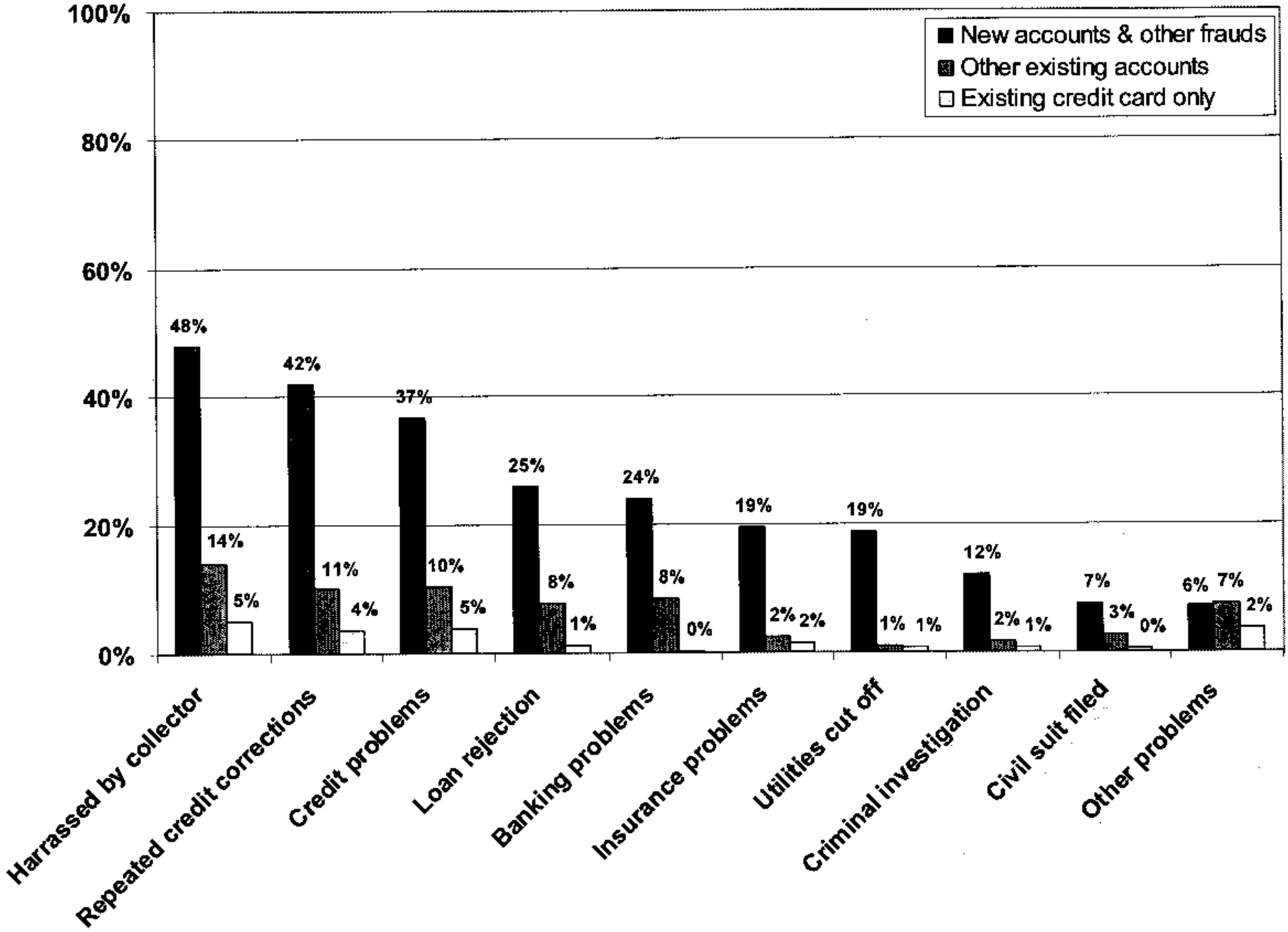


- This graph shows the estimated hours spent by victims in resolving problems stemming from ID theft. It does not refer to the amount of time that passed from when the victims discovered the crime to when their problems where resolved.
- When asked about the amount of time spent resolving problems stemming 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.

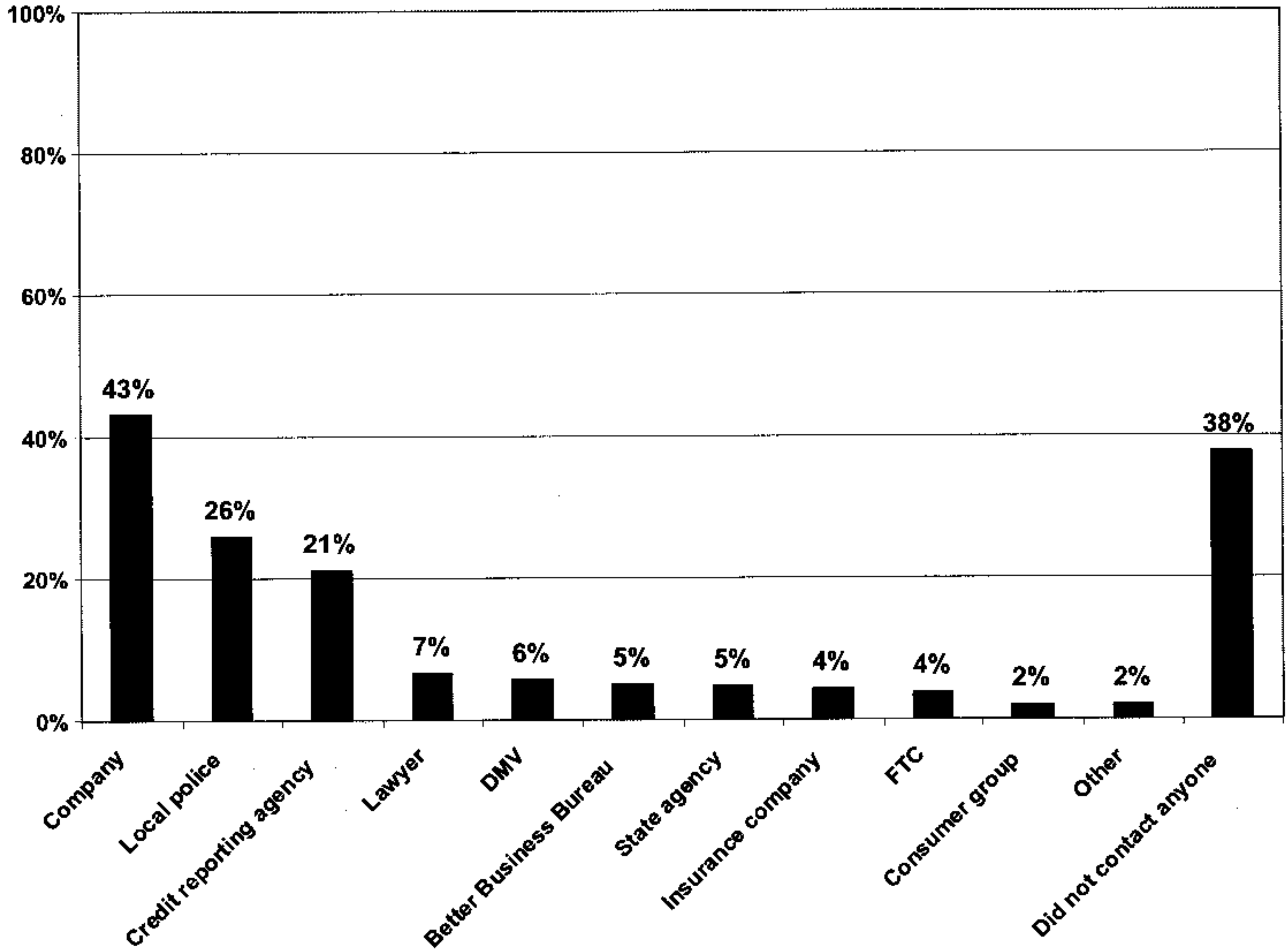
  - 10% of ID theft victims reported suffering banking problems, such as being refused for a checking account or having checks rejected.
  - 7% of victims reported having insurance problems, such as having been turned down for insurance or having to pay higher rates.

- 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]

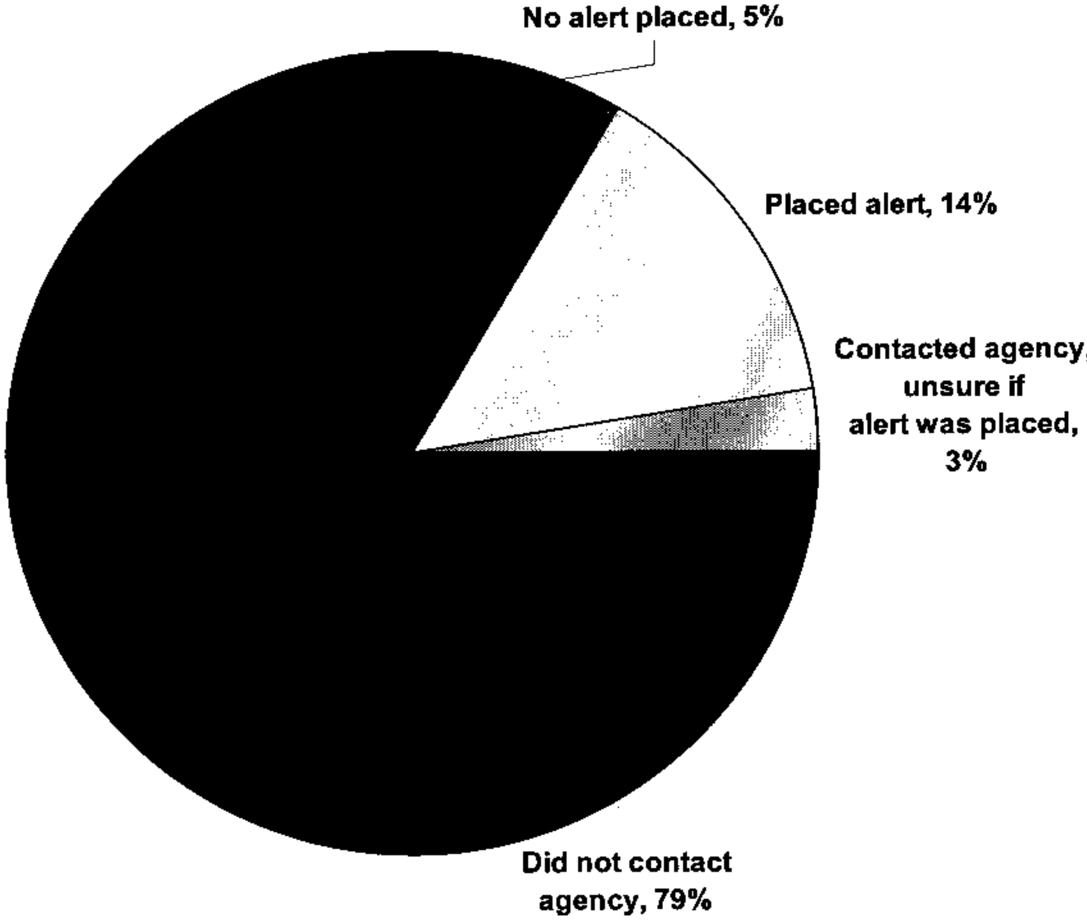
---

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]

---

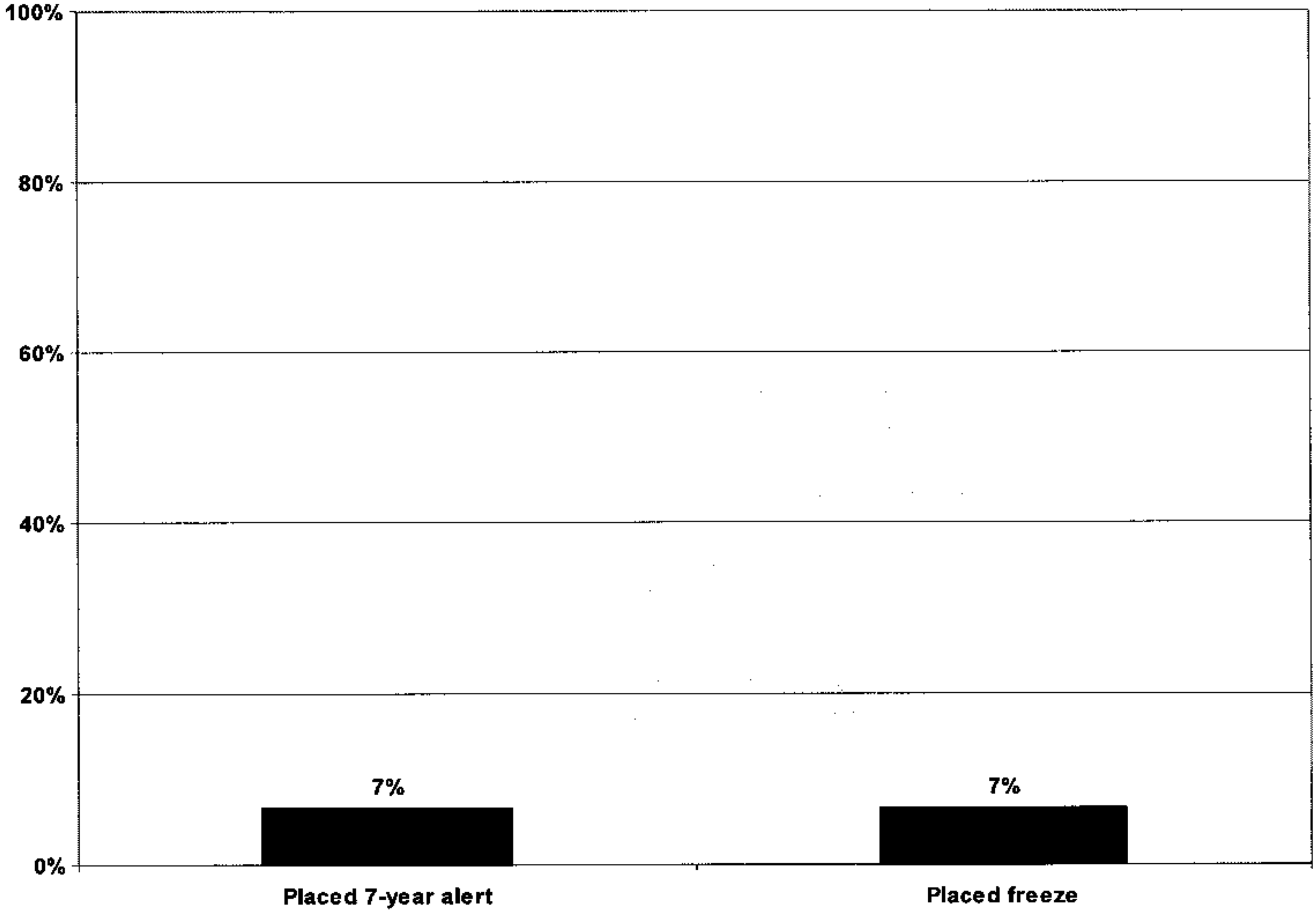
[30] Overall figures are based on the responses of the 559 individuals surveyed who indicated that their personal information had been misused between 2001 and the date they were interviewed.

[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.

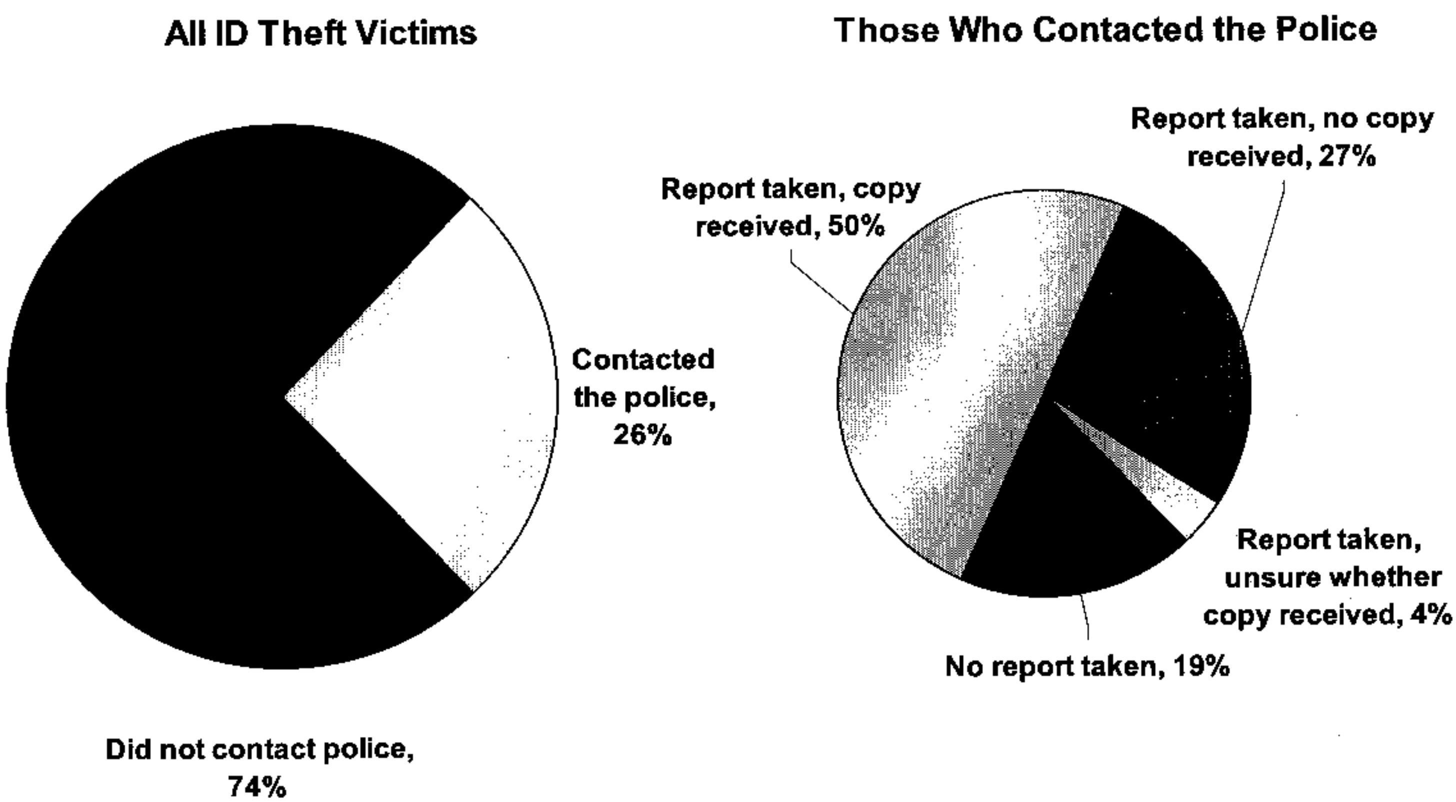
- Relatively few ID Theft victims took advantage of either extended alerts or credit freezes:
  - Seven percent of ID Theft victims placed extended alerts on their credit reports.
  - Seven percent of ID Theft victims placed a freeze on their credit reports.
  - Each of these actions was taken by 15% 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]



- 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.