

1 Bobby Saadian, SBN 250377
2 bobby@wilshirelawfirm.com
3 Justin F. Marquez, SBN 262417
4 justin@wilshirelawfirm.com
5 Robert J. Dart, SBN 264060
6 rdart@wilshirelawfirm.com
7 Thiago M. Coelho, SBN 324715
8 thiago@wilshirelawfirm.com
9 **WILSHIRE LAW FIRM**
10 3055 Wilshire Blvd., 12th Floor
11 Los Angeles, California 90010
12 Telephone: (213) 381-9988
13 Facsimile: (213) 381-9989

14 *Attorneys for Plaintiffs*
15 *and Proposed Class*

16 **UNITED STATES DISTRICT COURT**

17 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

18 MICHELLE ANDERSON, JAKE
19 THOMAS, TOM AINSWORTH,
20 individually and on behalf of all
21 others similarly situated,

22 Plaintiff,

23 v.

24 KIMPTON HOTEL &
25 RESTAURANT GROUP, LLC,
26 a Delaware corporation; and
27 DOES 1 to 10, inclusive,

28 Defendants.

CASE NO.:

CLASS ACTION

COMPLAINT

DEMAND FOR JURY TRIAL

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd., 12th Floor
Los Angeles, CA 90010-1137

1 *IHG takes your privacy seriously and works to protect you.*

2 - Kimpton Hotel & Restaurant Group, LLC, Privacy Agreement

3 Plaintiffs Michelle Anderson Jake Thomas, Tom Ainsworth (“Plaintiffs”),
4 individually and on behalf of all others similarly situated, bring this action based
5 upon personal knowledge as to themselves and their own acts, and as to all other
6 matters upon information and belief, based upon, *inter alia*, the investigations of
7 his attorneys.

8 **NATURE OF THE ACTION**

9 1. As of March 2018, Kimpton Hotels & Restaurants (“Defendant”)
10 owned or managed 66 properties in the world. Every day, hundreds of customers
11 book hotel rooms with Defendant through Defendant’s centralized reservation
12 system. Consumers expect the highest quality of services and discretion when
13 booking a hotel room with Defendant. What consumers did not expect is that during
14 the period between August 10, 2016 and March 9, 2017, their personal information
15 would be collected by an unauthorized third party. The data of customers that
16 stayed at Defendant’s hotels was accessed and misused due to a data breach.

17 2. Plaintiffs, individually and on behalf of those similarly situated
18 persons (hereafter “Class Members”), bring this Class Action to secure redress
19 against Defendant for its reckless and negligent violation of customer privacy
20 rights. Plaintiff and Class Members are customers who booked hotel reservations
21 with Defendant during the period of August 10, 2016 to March 9, 2017 (“Data
22 Breach”).

23 3. Plaintiffs and Class Members suffered injuries. The security breach
24 compromised hotel customers’ full name, credit and debit card account numbers,
25 card expiration dates, card verification codes, emails, phone numbers, full
26 addresses, and other private identifiable information (“PII”).

27 4. As a result of Defendant’s wrongful actions and inactions, customer
28 information was stolen. Plaintiffs and Class Members who booked rooms at

1 Defendant’s hotels have had their PII compromised, have had their privacy rights
2 violated, have been exposed to the risk of fraud and identify theft, and have
3 otherwise suffered damages.

4 5. Further, Plaintiffs and Class Members did not receive the full benefit
5 for the cost of their reservation, since proper security measures were not taken, and
6 the value of their PII has been diminished.

7 **THE PARTIES**

8 6. Plaintiff Michelle Anderson is a California citizen residing in San
9 Benito, California. Plaintiff is a long-time customer of Defendant who has given
10 her PII to Defendant. One of her reservations was to Kimpton’s Sir Francis Drake
11 Hotel in San Francisco, California during the time of the Data Breach. Shortly after
12 and during that time, Plaintiff’s PII was accessed by hackers by accessing
13 Defendant’s database or server. Hackers proceeded to misuse her PII. As a result,
14 Plaintiff has to purchase credit and personal identity monitoring service to alert her
15 to potential misappropriation of her identity and to combat risk of further identity
16 theft. At a minimum, Plaintiff has suffered damages because she will be forced to
17 incur the cost of monitoring service. Exposure of Plaintiff’s PII has placed her at
18 imminent, immediate and continuing risk of further identity theft-related harm,
19 including through “phishing.” Further, Plaintiff would not have reserved a room
20 with Defendant’s hotel if she had known of the improper security or the data breach
21 during the time of the booking, she instead would have booked her room at another
22 hotel. Finally, Plaintiff’s PII value has been diminished due to the breach and
23 misuse. Plaintiff has experienced signs that her PII has already been misused.
24 Plaintiff had only given consent to give her PII to Defendant for one reason: to
25 reserve a room at the hotel of her choice, and nothing more.

26 7. Plaintiff Jake Thomas is an Arizona citizen residing in Mesa, Arizona.
27 Plaintiff is a long-time customer of Defendant who has given his PII. Some of his
28 reservations during the time of the Data Breach include:

- i. Kimpton Buchanan in San Francisco, California;
- ii. Kimpton Solamar in San Diego, California;
- iii. Kimpton Amara Resort and Spa in Arizona;
- iv. Kimpton Monaco in Denver, Colorado;
- v. Kimpton Monaco in Philadelphia, Pennsylvania;
- vi. Kimpton Ink48 in New York; and
- vii. Kimpton Van Vandt in Texas.

8. Shortly after and during that time, Plaintiff Jake Thomas' PII was accessed by hackers through Defendant's database or server. Hackers proceeded to misuse his PII in various ways. As a result, Plaintiff has to purchase credit and personal identity monitoring service to alert him to potential misappropriation of his identity and to combat risk of further identity theft. At a minimum, Plaintiff has suffered damages because he will be forced to incur the cost of monitoring service. Exposure of Plaintiff's PII has placed him at imminent, immediate and continuing risk of further identity theft-related harm, including through "phishing." Further, Plaintiff would not have reserved any hotel rooms with Defendant if he had known of the improper security or the data breach during the time of the booking, he instead would have booked his room at another hotel. Finally, Plaintiff's PII value has been diminished due to the breach and misuse. Plaintiff has experienced signs that his PII has already been misused. Plaintiff had only consented to provide his PII to Defendant and only to Defendant for one reason: to reserve rooms at the hotel of his choice.

9. Plaintiff Tom Ainsworth is a California citizen residing in Danville, California. Plaintiff is a long-time customer of Defendant who has given his PII to Defendant. One of his reservations was to Kimpton's Sir Francis Drake Hotel in San Francisco, California during the time of the Data Breach. Shortly after and during that time, Plaintiff's PII was accessed by hackers by accessing Defendant's database or server. Hackers proceeded to misuse his PII, and Plaintiff has multiple

1 fraudulent activities on the same account that was used to make reservation to
2 Defendant's hotel. As a result, Plaintiff has to purchase credit and personal identity
3 monitoring service to alert him to potential misappropriation of his identity and to
4 combat risk of further identity theft. At a minimum, Plaintiff has suffered damages
5 because he will be forced to incur the cost of monitoring service. Exposure of
6 Plaintiff's PII has placed him at present as well as imminent, immediate and
7 continuing risk of further identity theft-related harm, including through "phishing."
8 Further, Plaintiff would not have reserved a room with Defendant's hotel if he had
9 known of the improper security or the data breach during the time of the booking,
10 he instead would have booked her room at another hotel. Finally, Plaintiff's PII
11 value has been diminished due to the breach and misuse. Plaintiff's PII has been
12 misused by the hackers that hacked Defendant's database. Plaintiff had only given
13 consent to give his PII to Defendant for one reason: to reserve a room at the hotel
14 of his choice, and nothing more.

15 10. Plaintiffs brings this action on their own behalf and on behalf of all
16 others similarly situated, namely all other individuals who have made a booking at
17 any of Defendant's hotels during the period of August 10, 2016 to March 9, 2017.

18 11. Defendant Kimpton Hotel & Restaurant Group is a Delaware limited
19 liability corporation, with its headquarters at 222 Kearny Street, #200, San
20 Francisco, CA, 94108. Defendant conducts a large amount of its business in
21 California, and the United States as a whole.

22 JURISDICTION AND VENUE

23 12. This Court has subject matter jurisdiction over the state law claims
24 asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2),
25 since some of the Class Members are citizens of a State different from the
26 Defendant and, upon the original filing of this complaint, members of the putative
27 Plaintiff class resided in states around the country; there are more than 100 putative
28 class members; and the amount in controversy exceeds \$5 million.

1 13. The Court also has personal jurisdiction over the parties because, on
2 information and belief, Defendant conducts a major part of its national operations
3 with regular and continuous business activity in California, through a number of
4 hotels and with an advertising budget not exceeded in other jurisdictions throughout
5 the United States.

6 14. Venue is appropriate in this District because, among other things: (a)
7 Plaintiff Michelle Anderson is a resident of this District and a citizen of this state;
8 (b) Defendant directed its activities at residents in this District; and (c) many of the
9 acts and omissions that give rise to this Action took place in this judicial District
10 for reservations in this district.

11 15. Venue is further appropriate in this District pursuant to 28 U.S.C. §
12 1391 because Defendant conducts a large amount of its business in this District, and
13 because Defendant has substantial relationships in this District.

14 **SUBSTANTIVE ALLEGATIONS**

15 ***A. The Kimpton's Data Breach***

16 16. Kimpton uses an online reservation system that facilitates the booking
17 of hotel reservations made by its customers through hotels, online travel agencies,
18 and similar booking services. On July 28, 2017, Defendant informed its customers,
19 including Plaintiffs, that hackers may have accessed reservation information
20 between August 10, 2016 and March 9, 2017, and the unlawful access may have
21 involved payment card information for hotel reservations, including names, card
22 numbers, card expiration dates, card security codes, email addresses, phone numbers,
23 and mailing addresses.

24 17. In addition to the eight-month period, the unauthorized third-parties
25 would have had access to booking information up to 60 days prior to the breach, as
26 the online reservation system only deletes reservation details 60 days after the hotel
27 stay.
28

1 18. Over millions of consumers that frequent Kimpton’s website looking
2 to make hotel reservations, Kimpton collects massive amounts of confidential and
3 personal information from internet users. For each new online reservation or hotel
4 booking Kimpton requires that consumers provide first and last names, telephone
5 number, address and email address to secure the hotel reservation. Consumers are
6 also required to reserve the hotel with sensitive information using a payment card.
7 Kimpton’s credit and debit safety provides an assurance that payment information
8 collected is secured, stated by Defendant itself, “**Credit and Debit Card Safety**
9 We at IHG are committed to keeping your personal information safe . . . [i]t
10 encrypts all of your personal information, including payment card number, name,
11 and address, so that it cannot be read as the information travels over the Internet.”
12 Attached hereto as **Exhibit A**, Privacy Agreement.

13 19. Additionally, when reserving a hotel reservation, consumers are
14 required to certify that they have read and accept the Terms of Use and Privacy
15 Statement before their hotel reservation can be confirmed. Consumers have a
16 reasonable expectation that required information provided will be kept safe.

17 20. According to Kimpton’s Privacy Agreement:

18 **How we secure your information**

19 We are committed to protecting the confidentiality and security of the
20 information that you provide to us. To do this, technical, physical and
21 organizational security measures are put in place to protect against any
22 unauthorized access, disclosure, damage or loss of your information.
23 The collection, transmission and storage of information can never be
24 guaranteed to be completely secure, however, we take steps to ensure
25 that appropriate security safeguards are in place to protect your
26 information.

27 21. Consumers place value in data privacy and security, and they consider
28 it when making decisions on what hotel to use for lodging and hospitality. If
Plaintiffs had the foreknowledge that Kimpton does not take all obligatory
precautions to properly safeguard PII from unauthorized access as promised in their
Privacy Agreement they could have made other decisions on where to stay for

1 travel. Absent this information, Plaintiffs were unable to make an informed
2 decision on whether or not to stay at Kimpton Hotels.

3 22. Kimpton was fully aware of the importance of data protection. In its
4 Privacy Agreement, Kimpton promises consumers that it takes their privacy
5 “seriously” and implements systems and procedures to safeguard user’s personal
6 information. According to Kimpton’s own Privacy Agreement: “the privacy and
7 security of your information is very important to us. Whether you are booking a
8 room or are a member of one of our loyalty programs, we want you to trust that the
9 information that you have provided to us is being properly managed and protected.”
10 *Id.* Further explained, “**Data Privacy and Site Security**[:] IHG takes your privacy
11 seriously and works to protect you. All personal information you provide is
12 encrypted and secure.”¹

13 23. Plaintiffs and Class Members read the Privacy Agreement as well as
14 relied on it and agreed to it prior to reserving their hotel rooms.

15 24. Kimpton misrepresented its data security practices that Plaintiffs relied
16 on or were misled by the representation that adequate safeguards were in place to
17 protect sensitive information. As demonstrated by its security breach, Plaintiffs
18 private and sensitive PII was left inadequately protected by Kimpton, and
19 improperly disclosed to unauthorized parties. As a result of this, Plaintiffs were
20 placed in continuing and increased risk of harm of rampant identity theft and
21 identity fraud. Kimpton misled consumers into believing their sensitive
22 information would remain safe when booking or reserving a hotel online as well as
23 not disclosed to unauthorized parties.

24 ***B. Stolen Information Is Valuable to Hackers and Thieves***

25 25. It is well known, and the subject of many media reports, that payment
26 card data is highly coveted and a frequent target of hackers. Especially in the

27 _____
28 ¹ Although IHG is Kimpton’s parent company, all customers are directed to IHG’s Privacy Agreement from Kimpton’s website.

1 technology industry, the issue of data security and threats thereto is well known.
2 Despite well-publicized litigation and frequent public announcements of data
3 breaches, Defendant opted to maintain an insufficient and inadequate system to
4 protect the PII of Plaintiff and Class Members.

5 26. Plaintiffs and Class Members value their PII, as in today’s electronic-
6 centric world, their PII is required for numerous activities, such as new registrations
7 to websites, or opening a new bank account, as well as signing up for special deals.

8 27. Legitimate organizations and criminal underground alike recognize
9 the value of PII. Otherwise, they would not aggressively seek or pay for it.

10 28. Credit or debit card information is highly valuable to hackers. Credit
11 and debit card information that is stolen from the point of sale are known as
12 “dumps.” See Krebs on Security April 16, 2016, Blog Post, *available at*
13 <https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/>,

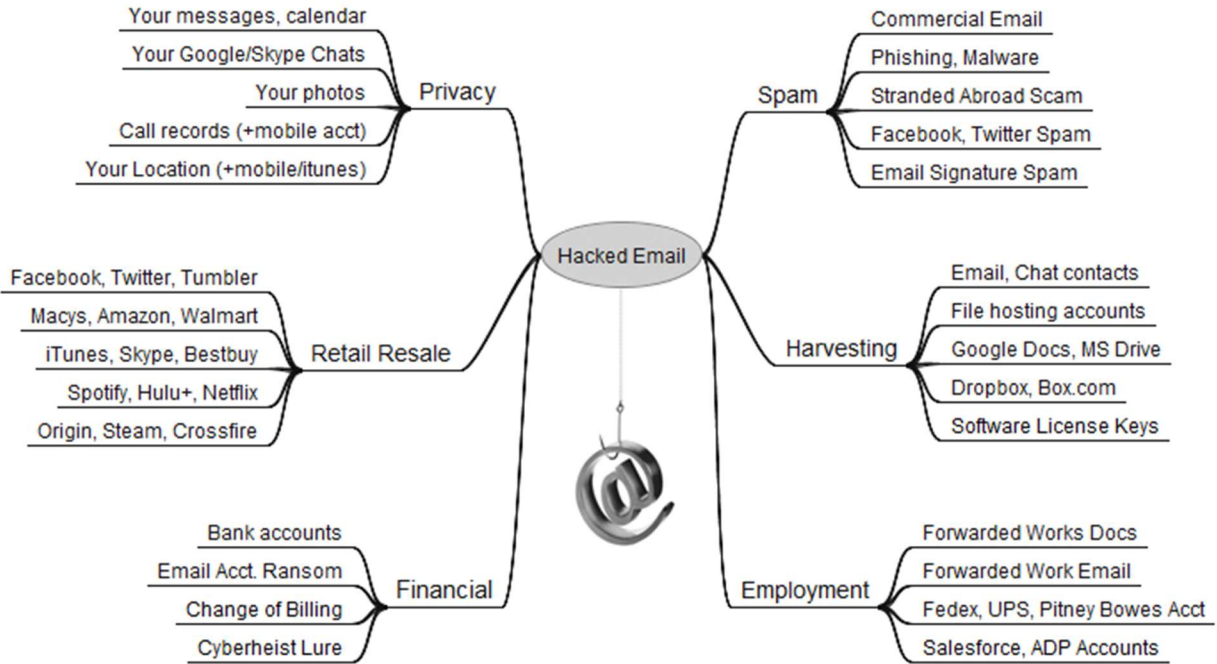
14 attached hereto as **Exhibit B**. Credit and debit card dumps can be sold in the
15 cybercrime underground for a retail value of about “\$20 apiece.” *Id.* This
16 information can also be used to clone a debit or credit card. *Id.*

17 29. Once someone buys PII, it is then used to gain access to different areas
18 of the victim’s digital life, including bank accounts, social media, and credit card
19 details. During that process, other sensitive data may be harvested from the victim’s
20 accounts, as well as from those belonging to family, friends, and colleagues.

21 30. In addition to PII, a hacked email account can be very valuable to cyber
22 criminals. Since most online accounts require an email address not only as a
23 username, but also as a way to verify accounts and reset passwords, a hacked email
24 account could open up a number of other accounts to an attacker.²

25
26
27 ² Identity Theft and the Value of Your Personal Data, Trend Micro (Apr. 30, 2015),
28 <https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data>.

31. As shown below, a hacked email account can be used to link to many other sources of information for an identity thief, including any purchase or account information found in the hacked email account.³



32. Hacked information can also enable thieves to obtain other personal information through “phishing.” According to the Report on Phishing available on the United States, Department of Justice’s website: “AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers and credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers.”⁴

³ Brian Krebs, The Value of a Hacked Email Account, Krebs on Security (June 13, 2013, 3:14 PM), <https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/>.

⁴ https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf

1 ***C. The Data Breach Has and Will Result in Additional Identity Theft and***
2 ***Identity Fraud***

3 33. Defendant failed to implement and maintain reasonable security
4 procedures and practices appropriate to protect the PII of Plaintiffs and the Class
5 Members. Further, Defendant disclosed PII to unauthorized parties which they
6 lacked the consent to do so.

7 34. The ramification of Defendant’s failure to keep Plaintiffs and the Class
8 Members’ data secure is severe.

9 35. According to Javelin Strategy and Research, “one in every three people
10 who is notified of being a potential fraud victim becomes one . . . with 46% of
11 consumers who had cards breached becoming fraud victims that same year.” 2013
12 Identity Fraud Report, attached hereto as **Exhibit C**. “Someone Became an Identity
13 Theft Victim Every 2 Seconds Last Year,” Fox Business, Feb. 5, 2014 *available at*
14 [http://www.foxbusiness.com/personal-finance/2014/02/05/someone-became-](http://www.foxbusiness.com/personal-finance/2014/02/05/someone-became-identitytheft-victim-every-2-seconds-last-year.html)
15 [identitytheft-victim-every-2-seconds-last-year.html](http://www.foxbusiness.com/personal-finance/2014/02/05/someone-became-identitytheft-victim-every-2-seconds-last-year.html) attached hereto as **Exhibit D**.

16 36. It is incorrect to assume that reimbursing a consumer for a financial
17 loss due to fraud makes that individual whole again. On the contrary, after
18 conducting a study, the Department of Justice’s Bureau of Justice Statistics (“BJS”)
19 found that “among victims who had personal information used for fraudulent
20 purposes, 29% spent a month or more resolving problems.” *See* “Victims of
21 Identity Theft,” U.S. Department of Justice, Dec 2013, *available at*
22 <https://www.bjs.gov/content/pub/pdf/vit12.pdf> attached hereto as **Exhibit E**. In
23 fact, the BJS reported, “resolving the problems caused by identity theft [could] take
24 more than a year for some victims.” *Id.* at 11.

25 ***D. Annual Monetary Losses from Identity Theft are in the Billions of***
26 ***Dollars***

27 37. Javelin Strategy and Research reports that losses from identity theft
28 reached \$21 billion in 2013. Ex. C. There may be a time lag between when harm

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

1 occurs and when it is discovered, and also between when PII is stolen and when it
2 is used. According to the U.S. Government Accountability Office (“GAO”), which
3 conducted a study regarding data breaches:

4 [L]aw enforcement officials told us that in some cases, stolen data may
5 be held for up to a year or more before being used to commit identity
6 theft. Further, once stolen data have been sold or posted on the Web,
7 fraudulent use of that information may continue for years. As a result,
8 studies that attempt to measure the harm resulting from data breaches
cannot necessarily rule out all future harm.

9 See GAO, Report to Congressional Requesters, at 33 (June 2007), *available* at
10 <http://www.gao.gov/new.items/d07737.pdf>, attached hereto as **Exhibit F**.

11 38. Plaintiffs and the Class Members now face years of constant
12 surveillance of their financial and personal records, monitoring, and loss of rights.
13 The Class is incurring and will continue to incur such damages in addition to any
14 fraudulent credit and debit card charges incurred by them and the resulting loss of
15 use of their credit and access to funds, whether or not such charges are ultimately
16 reimbursed by the credit card companies.

17 ***E. Plaintiffs and Class Members Suffered Damages***

18 39. The data breach was a direct and proximate result of Defendant’s
19 failure to properly safeguard and protect Plaintiff’s and Class Members’ PII from
20 unauthorized access, use, and disclosure, as required by various state and federal
21 regulations, industry practices, and the common law. The data breach was also a
22 result of Defendant’s failure to establish and implement appropriate administrative,
23 technical, and physical safeguards to ensure the security and confidentiality of
24 Plaintiff’s and Class Members’ PII to protect against reasonably foreseeable threats
25 to the security or integrity of such information.

26 40. Plaintiffs and Class Members would have reserved a different hotel if
27 they were aware that their PII would not have been kept safe at the time of the
28

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

1 reservation. With multiple comparable hotels for similar or even lower prices than
2 Kimpton, Plaintiffs and Class Members would have no difficulty finding a different
3 hotel which would adequately protect their PII.

4 41. Plaintiffs and Class Members' PII is private and sensitive in nature and
5 was inadequately protected by Defendant. Defendant did not obtain Plaintiffs' and
6 Class Members' consent to disclose their PII, except to certain persons not relevant
7 to this action, as required by applicable law and industry standards.

8 42. As a direct and proximate result of Defendant's wrongful action and
9 inaction and the resulting data breach, Plaintiffs and the Class Members have been
10 placed at an imminent, immediate, and continuing risk of harm from identity theft
11 and identity fraud, requiring them to take the time and effort to mitigate the actual
12 and potential impact of the subject data breach on their lives by, among other things,
13 placing "freezes" and "alerts" with credit reporting agencies, contacting their
14 financial institutions, or modifying financial accounts, and closely reviewing and
15 monitoring their credit reports and accounts for unauthorized activity.

16 43. Defendant's wrongful actions and inaction directly and proximately
17 caused the theft and dissemination into the public domain of Plaintiffs' and the
18 Class Members' PII, causing them to suffer, and continue to suffer, economic
19 damages and other actual harm for which they are entitled to compensation,
20 including:

- 21 a. Theft of their PII;
- 22 b. The imminent and certainly impending injury flowing from potential
23 fraud and identity theft posed by their PII being placed in the hands of
24 criminals and already misused via the sale of Plaintiffs' and Class
25 Members' PII on the Internet black market;
- 26 c. The untimely and inadequate notification of the data breach;
- 27 d. The improper disclosure of their PII;
- 28 e. Loss of privacy;

- 1 f. Ascertainable losses in the form of out-of-pocket expenses and the
2 value of their time reasonably incurred to remedy or mitigate the effects
3 of the data breach;
- 4 g. Ascertainable losses in the form of deprivation of the value of their PII,
5 for which there is a well-established national and international market;
- 6 h. Overpayments to Defendant for bookings and purchases during the
7 period of the subject data breach in that implied in the price paid for
8 such booking by Plaintiffs and the Class Members to Defendant was
9 the promise that some amount of the booking charge would be applied
10 to the costs of implementing reasonable and adequate safeguards and
11 security measures that would protect customers' PII, which Defendant
12 and its affiliates did not implement and, as a result, Plaintiff and Class
13 Members did not receive what they paid for and were overcharged by
14 Defendant; and
- 15 i. Loss of the benefit of the bargain in which Plaintiffs and Class
16 Members would have chosen a different hotel for their booking if they
17 were aware that their PII would have been stolen.

18 **CLASS ACTION ALLEGATIONS**

19 44. Plaintiffs bring this action on their own behalf and pursuant to the
20 Federal Rules of Civil Procedure Rule 23(a), (b)(2), (b)(3), and (c)(4). Plaintiffs
21 intend to seek certification of a California Class, Arizona Class, Colorado Class,
22 Pennsylvania Class, New York class, and the Texas Class ("the Classes"). The
23 Classes are initially defined as follows:

24 The California Class, initially defined as:

25 All persons residing in California who booked rooms at any of
26 Defendant's hotels from the time period August 10, 2016 to
27 March 9, 2017 (the "California Class").
28

1 The Arizona Class, initially defined as:

2 All persons residing in Arizona who booked rooms at any of
3 Defendant's hotels from the time period August 10, 2016 to
4 March 9, 2017 (the "Arizona Class").

4 The Colorado Class, initially defined as:

5 All persons residing in Colorado who booked rooms at any of
6 Defendant's hotels from the time period August 10, 2016 to
7 March 9, 2017 (the "Colorado Class").

7 The Pennsylvania Class, initially defined as:

8 All persons residing in Pennsylvania who booked rooms at any
9 of Defendant's hotels from the time period August 10, 2016 to
10 March 9, 2017 (the "Pennsylvania Class").

10 The New York Class, initially defined as:

11 All persons residing in New York who booked rooms at any of
12 Defendant's hotels from the time period August 10, 2016 to
13 March 9, 2017 (the "New York Class").

14 The Texas Class, initially defined as:

15 All persons residing in Texas who booked rooms at any of
16 Defendant's hotels from the time period August 10, 2016 to
17 March 9, 2017 (the "Texas Class").

17 45. Excluded from each of the above Classes is Defendant, including any
18 entity in which Defendant has a controlling interest, is a parent or subsidiary, or
19 which is controlled by Defendant, as well as the officers, directors, affiliates, legal
20 representatives, heirs, predecessors, successors, and assigns of Defendant. Also
21 excluded are the judge and the court personnel in this case and any members of their
22 immediate families. Plaintiffs reserve the right to amend the Class definitions if
23 discovery and further investigation reveal that the Classes should be expanded or
24 otherwise modified.

25 46. *Numerosity*. Fed. R. Civ. P. 23(a)(1). The members of the Classes are
26 so numerous that the joinder of all members is impractical. While the exact number
27 of Class Members is unknown to Plaintiffs at this time, Defendant has
28 acknowledged that customers' PII was stolen for a period of 8 months. The

1 disposition of the claims of Class Members in a single action will provide
2 substantial benefits to all parties and to the Court. The Class Members are readily
3 identifiable from information and records in Defendant’s possession, custody, or
4 control, such as reservation receipts and confirmations.

5 47. *Commonality*. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions
6 of law and fact common to the Classes, which predominate over any questions
7 affecting only individual Class Members. These common questions of law and fact
8 include, without limitation:

- 9 a. Whether Defendant, on the one hand, and Plaintiffs and Class
10 Members, on the other hand, had an enforceable contract;
- 11 b. Whether Defendant breached its contracts with Plaintiffs and Class
12 Members by improperly sharing or transmitting the PII of Plaintiffs
13 and Class Members to unauthorized entities or persons;
- 14 c. Whether Defendant took reasonable steps and measures to safeguard
15 Plaintiffs’ and Class Members’ PII;
- 16 d. Whether Defendant violated California’s Unfair Competition Law by
17 failing to implement reasonable security procedures and practices;
- 18 e. Whether Defendant violated common and statutory law by failing to
19 promptly notify Class Members that their PII had been compromised;
- 20 f. Which security procedures and which data-breach notification
21 procedure should Defendant be required to implement as part of any
22 injunctive relief ordered by the Court;
- 23 g. Whether Defendant knew or should have known of the security breach
24 prior to the disclosure;
- 25 h. Whether Defendant has complied with any implied contractual
26 obligation to use reasonable security measures;
- 27 i. Whether Defendant’s acts and omissions described herein give rise to
28 a claim of negligence;

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

- 1 j. Whether Defendant knew or should have known of the security breach
- 2 prior to its disclosure;
- 3 k. Whether Defendant had a duty to promptly notify Plaintiff and Class
- 4 Members that their PII was, or potentially could be, compromised;
- 5 l. What security measures, if any, must be implemented by Defendant to
- 6 comply with its contractual obligations;
- 7 m. The nature of the relief, including equitable relief, to
- 8 which Plaintiff and the Class Members are entitled; and
- 9 n. Whether Plaintiff and the Class Members are entitled to damages, civil
- 10 penalties, and/or injunctive relief.

11 48. *Typicality*. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of
12 those of other Class Members because Plaintiffs' PII, like that of every other Class
13 Member, was misused and/or disclosed by Defendant.

14 49. *Adequacy of Representation*. Fed. R. Civ. P. 23(a)(4). Plaintiffs will
15 fairly and adequately represent and protect the interests of the members of the
16 Classes. Plaintiffs have retained competent counsel experienced in litigation of
17 class actions, including consumer and data breach class actions, and Plaintiffs
18 intend to prosecute this action vigorously. Plaintiffs' claims are typical of the
19 claims of other members of the Classes and Plaintiffs has the same non-conflicting
20 interests as the other Class Members. Therefore, the interests of the Classes will be
21 fairly and adequately represented by Plaintiffs and his counsel.

22 50. *Superiority of Class Action*. Fed. R. Civ. P. 23(b)(3). A class action is
23 superior to other available methods for the fair and efficient adjudication of this
24 controversy since joinder of all the members of the Classes is impracticable.
25 Furthermore, the adjudication of this controversy through a class action will avoid
26 the possibility of inconsistent and potentially conflicting adjudication of the
27 asserted claims. There will be no difficulty in the management of this action as a
28 class action.

1 51. Damages for any individual class member are likely insufficient to
2 justify the cost of individual litigation so that, in the absence of class treatment,
3 Defendant’s violations of law inflicting substantial damages in the aggregate would
4 go un-remedied.

5 52. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and
6 (b)(2), because Defendant has acted or refused to act on grounds generally
7 applicable to the Classes, so that final injunctive relief or corresponding declaratory
8 relief is appropriate as to the Classes as a whole.

9 **FIRST CLAIM FOR RELIEF**

10 **Breach of Contract**

11 (On Behalf of Plaintiffs, and all of the Classes)

12 53. Plaintiffs allege and incorporates herein by reference each and every
13 allegation contained in paragraphs 1 through 52, inclusive, of this Complaint as if
14 set forth fully herein.

15 54. Defendant solicited and invited Plaintiffs and the members of the
16 Classes to reserve hotel rooms in one of Defendant’s hotels. Plaintiffs and Class
17 Members accepted Defendant’s offers and reserved hotel rooms at one of
18 Defendant’s hotels.

19 55. When Plaintiffs and Class Members reserved hotel rooms at one of
20 Defendant’s hotels, they provided their PII at Defendant’s request. During the
21 reservation of rooms with Defendant, they were required to accept the Privacy
22 Statement.

23 56. The Privacy Statement provided, among other things, Defendant
24 promised that Plaintiffs’ and Class Members’ PII would be secure and kept
25 confidential. Specifically, Defendant stated “[w]e are committed to protecting the
26 confidentiality and security of the information that you provide to us.” Ex. A.

27 57. The Privacy Statement constituted a clear contractual promise to
28 safeguard and protect the Class Members’ PII from disclosure to third parties.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

1 58. Each reservation by Plaintiffs and Class Members was made pursuant
2 to the mutually agreed-upon contract with Defendant under which Defendant
3 agreed to safeguard and protect Plaintiffs' and Class Members' PII.

4 59. Plaintiffs and Class Members would not have provided and entrusted
5 their PII to Defendant in the absence of the contract.

6 60. Plaintiffs and Class Members would not have reserved rooms with
7 Defendant if they knew that they could not rely on the Privacy Statement. Plaintiffs
8 and Class Members did not rely on any other statements or contracts, aside from
9 the Privacy Statement.

10 61. Plaintiffs and Class Members fully performed their obligations under
11 the contracts with Defendant.

12 62. Defendant breached the contract which was made with Plaintiffs and
13 Class Members by failing to safeguard and protect the PII of Plaintiffs and Class
14 Members. It further breached its contract when it disclosed the PII of Plaintiffs and
15 Class Members to unauthorized parties.

16 63. Plaintiffs and Class Members have lost the benefit of the bargain by
17 failing to enjoy the protection of their PII as promised in the contract, as instead
18 their PII was compromised at every reservation. Further, Plaintiffs and Class
19 Members have spent more on booking Defendant's rooms than they would have if
20 they had known that Defendant was not providing the reasonable security that
21 Plaintiffs and Class Members expected. Plaintiffs and Class Members would also
22 not have reserved rooms with Defendant if proper disclosure of their PII being
23 stolen would have been known.

24 64. As a direct and proximate result of Defendant's breaches of the
25 contracts between Defendant and Plaintiffs and Class Members, Plaintiffs and Class
26 Members sustained actual losses and damages in an amount according to proof at
27 trial but in excess of the minimum jurisdictional requirement of this Court. At a
28 minimum, Plaintiffs and Class Members allege loss of money for the hotel

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd., 12th Floor
Los Angeles, CA 90010-1137

1 reservation, overpayment to the hotel reservation, imminent, immediate, and
2 continuing risk of identity theft-related harm, and loss of value of their PII.

3 **SECOND CLAIM FOR RELIEF**

4 **Violation of Cal. Civil Code § 1798.81.5(c)**

5 (On Behalf of Plaintiffs, and the California Class)

6 65. Plaintiffs repeat and incorporate herein by reference each and every
7 allegation contained in paragraphs 1 through 51, inclusive, of this Complaint as if
8 set forth fully herein.

9 66. Cal. Civ. Code §1798.81.5(b) requires that “A business that owns,
10 licenses, or maintains personal information about a California resident shall
11 implement and maintain reasonable security procedures and practices appropriate
12 to the nature of the information, to protect the personal information from
13 unauthorized access, destruction, use, modification, or disclosure.”

14 67. Plaintiffs and the Class Members are “customer[s]” within the
15 meaning of Cal. Civil Code §1798.80(c) and are California residents.

16 68. Defendant is a “business” within the meaning of Cal. Civil Code
17 §1798.80(a).

18 69. Plaintiffs and the Class Members’ PII constitutes “personal
19 information” within the meaning of Cal. Civil Code § 1798.80(e).

20 70. Defendant violated Cal. Civ. Code § 1798.81.5(b) by failing to
21 implement and maintain reasonable security procedures and practices appropriate
22 to the nature of the information to protect Plaintiffs and the Class Members’ PII
23 from unauthorized access, destruction, use, modification, or disclosure as evidenced
24 by the fact that the security of Plaintiffs and the Class Members’ PII was
25 compromised and exposed to at least one unauthorized party and perhaps more.

26 71. As a direct and proximate result of Defendant’s violation of Cal. Civ.
27 Code §1798.81.5(b), Plaintiffs and the Class Members’ PII was compromised and
28 exposed in connection with the data breach.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd., 12th Floor
Los Angeles, CA 90010-1137

1 72. As a result of the data breach and the exposure of their PII to
2 unauthorized third parties, Plaintiffs and the Class Members have been placed at an
3 imminent, immediate, and continuing risk of identity theft-related harm and are
4 thereby entitled to recover compensatory damages in an amount according to proof
5 at trial pursuant to Cal. Civ. Code §1798.84(b).

6 **THIRD CLAIM FOR RELIEF**

7 **Violation of California’s Unfair Competition Law Cal. Bus. & Prof. Code §**
8 **17200 Unlawful Business Practices**

9 (On Behalf of Plaintiffs and the California Class)

10 73. Plaintiffs allege and incorporates herein by reference, each and every
11 allegation contained in paragraphs 1 through 51, inclusive, of this Complaint as if
12 set forth fully herein.

13 74. Defendant has violated Cal. Bus. & Prof. Code § 17200 *et seq.* by
14 engaging in unlawful business acts and practices that constitute acts of "unfair
15 competition" as defined in Cal. Bus. & Prof. Code § 17200.

16 75. Defendant violated Cal. Civ. Code § 1798.81.5(b) by failing to
17 implement and maintain reasonable security procedures and practices appropriate
18 to the nature of Plaintiffs and the Class Members' PII to protect their PII from
19 unauthorized access, destruction, use, modification, or disclosure.

20 76. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45),
21 Defendant had a duty to provide fair and adequate computer systems and data
22 security practices to safeguard Plaintiffs' and the Class Members' PII.

23 77. Defendant breached its duties to Plaintiffs and the Class Members
24 under the Federal Trade Commission Act (15 U.S.C. § 45).

25 78. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting
26 commerce," including, as interpreted and enforced by the FTC, the unfair act or
27 practice by businesses, such as Defendant, of failing to use reasonable measures to
28 protect Private Information. The FTC publications and orders described above also

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

1 form part of the basis of Defendant's duty in this regard.

2 79. Defendant violated Section 5 of the FTC Act by failing to use
3 reasonable measures to protect Private Information and not complying with
4 applicable industry standards, as described herein. Defendant's conduct was
5 particularly unreasonable given the nature and amount of PII in its stores obtained
6 and stored, and the foreseeable consequences of a data breach at a hotel chain as
7 large as Defendant's, including, specifically, the damages that would result to
8 Plaintiffs and Class members.

9 80. As a direct and proximate result of Defendant's unlawful acts and
10 practices, Plaintiffs and the Class Members were injured and lost money or
11 property, including but not limited to the reservation fees that they paid to
12 Defendant and the loss of their legally protected interest in the confidentiality and
13 privacy of their PII. Further, Plaintiffs and Class Members had relief on
14 Defendant's Privacy Statement and they lost the benefit of the bargain as they were
15 not disclosed or aware of the data breach or the theft of their PII at the time of the
16 booking, and had they known, they would not have reserved rooms with Defendant.

17 81. Plaintiffs and the Class Members seek disgorgement and restitution to
18 Plaintiffs and the Class Members of money or property that Defendant acquired
19 from Plaintiffs and the Class Members by means of its unlawful business practices.

20 82. Plaintiffs and the Class Members also seek injunctive relief against
21 Defendant.

22 **FOURTH CLAIM FOR RELIEF**

23 **Violation of Arizona Consumer Fraud Act,**

24 **A.R.S. §§ 44-1521, *et seq.***

25 (On Behalf of Plaintiff Jake Thomas and the Arizona Class)

26 83. Plaintiff alleges and incorporates herein by reference, each and every
27 allegation contained in paragraphs 1 through 51, inclusive, of this Complaint as if
28 set forth fully herein.

1 84. Defendant is a “person” as defined by A.R.S. § 44-1521(6).

2 85. Defendant advertised, offered, or sold goods or services in Arizona and
3 engaged in trade or commerce directly or indirectly affecting the people of Arizona.

4 86. Defendant engaged in deceptive and unfair acts and practices,
5 misrepresentation, and the concealment, suppression, and omission of material facts
6 affecting the people of Arizona in connection with the sale and advertisement of
7 “merchandise” (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5))
8 in violation of A.R.S. § 44-1522(A), including:

- 9 i. Failing to implement and maintain reasonable security and
10 privacy measures to protect Plaintiff and Arizona Class
11 Members’ PII, which was a direct and proximate cause of the
12 data breach;
- 13 ii. Failing to identify foreseeable security and privacy risks,
14 remediate identified security and privacy risks, and adequately
15 improve security and privacy measures following previous
16 cybersecurity incidents, which was a direct and proximate cause
17 of the data breach;
- 18 iii. Failing to comply with common law and statutory duties
19 pertaining to the security and privacy of Plaintiff and Arizona
20 Class members’ PII, including duties imposed by the FTC Act,
21 direct and proximate cause of the data breach;
- 22 iv. Misrepresenting that it would protect the privacy and
23 confidentiality of Plaintiff and Arizona Class members’ PII,
24 including by implementing and maintaining reasonable security
25 measures;
- 26 v. Misrepresenting that it would comply with common law and
27 statutory duties pertaining to the security and privacy of Plaintiff
28 and Arizona Class members’ PII, including duties imposed by

1 the FTC Act, 15 U.S.C. § 45;

2 vi. Omitting, suppressing, and concealing the material fact that it
3 did not reasonably or adequately secure Plaintiff and Arizona
4 Class members' Personal Information; and

5 vii. Omitting, suppressing, and concealing the material fact that it
6 did not comply with common law and statutory duties
7 pertaining to the security and privacy of Plaintiff and Arizona
8 Class members' PII, including duties imposed by the FTC Act,
9 15 U.S.C. § 45.

10 87. Defendant's representations and omissions were material because they
11 were likely to deceive reasonable consumers about the adequacy of Defendant's
12 data security and ability to protect the confidentiality of consumers' PII.

13 88. Defendant intended to mislead Plaintiff and Arizona Class members
14 and induce them to rely on its misrepresentations and omissions.

15 89. Had Defendant disclosed to Plaintiffs and Class members that its data
16 systems were not secure and, thus, vulnerable to attack, Defendant would have been
17 unable to continue in business and it would have been forced to adopt reasonable
18 data security measures and comply with the law. Instead, Defendant held itself out
19 as one of the premiere hotels and was trusted with sensitive and valuable PII
20 regarding hundreds of millions of consumers, including Plaintiff and the Arizona
21 Class.

22 90. Defendant acted intentionally, knowingly, and maliciously to violate
23 Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiffs and Arizona
24 Class members' rights.

25 91. As a direct and proximate result of Defendant's unfair and deceptive
26 acts and practices, Plaintiff and Arizona Class members have suffered and will
27 continue to suffer injury, ascertainable losses of money or property, and monetary
28 and non-monetary damages, including from fraud and identity theft; time and

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

1 expenses related to monitoring their financial accounts for fraudulent activity; an
2 increased, imminent risk of fraud and identity theft; and loss of value of their PII.

3 92. Plaintiff and Arizona Class members seek all monetary and
4 nonmonetary relief allowed by law, including compensatory damages;
5 disgorgement; punitive damages; injunctive relief; and reasonable attorneys’ fees
6 and costs.

7 **FIFTH CLAIM FOR RELIEF**

8 **Violation of Colorado Consumer Protection Act,**

9 **Colo. Rev. Stat. §§ 6-1-101, *et seq.***

10 (On Behalf of Plaintiff Jake Thomas and the Colorado Class)

11 93. Plaintiff alleges and incorporates herein by reference, each and every
12 allegation contained in paragraphs 1 through 51, inclusive, of this Complaint as if
13 set forth fully herein.

14 94. Defendant is a “person” as defined by Colo. Rev. Stat. § 6-1-102(6).

15 95. Defendant engaged in “sales” as defined by Colo. Rev. Stat. § 6-1-
16 102(10).

17 96. Plaintiff and Colorado Class members, as well as the general public,
18 are actual or potential consumers of the products and services offered by Defendant
19 or successors in interest to actual consumers.

20 97. Defendant engaged in deceptive trade practices in the course of its
21 business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

- 22 i. Knowingly making a false representation as to the
23 characteristics of services;
- 24 ii. Representing that services are of a particular standard, quality,
25 or grade, though Defendant knew or should have known that
26 there were or another;
- 27 iii. Advertising services with intent not to sell them as advertised;
28 and

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd., 12th Floor
Los Angeles, CA 90010-1137

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd., 12th Floor
Los Angeles, CA 90010-1137

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

iv. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

98. Defendant’s deceptive trade practices include:

- i. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Colorado Class members’ PII, which was a direct and proximate cause of the data breach;
- ii. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the Defendant data breach;
- iii. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Class members’ PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- iv. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Colorado Subclass members’ PII, including by implementing and maintaining reasonable security measures;
- v. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Class members’ PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- vi. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Colorado Class members’ PII; and

1 vii. Omitting, suppressing, and concealing the material fact that it
2 did not comply with common law and statutory duties pertaining
3 to the security and privacy of Plaintiff and Colorado Class
4 members' PII.

5 99. Defendant's representations and omissions were material because they
6 were likely to deceive reasonable consumers about the adequacy of Defendant's
7 data security and ability to protect the confidentiality of consumers' PII.

8 100. Defendant intended to mislead Plaintiff and Arizona Class members
9 and induce them to rely on its misrepresentations and omissions.

10 101. Had Defendant disclosed to Plaintiffs and Class members that its data
11 systems were not secure and, thus, vulnerable to attack, Defendant would have been
12 unable to continue in business and it would have been forced to adopt reasonable
13 data security measures and comply with the law. Instead, Defendant held itself out
14 as one of the premiere hotels and was trusted with sensitive and valuable PII
15 regarding hundreds of millions of consumers, including Plaintiff and the Colorado
16 Class.

17 102. Defendant acted intentionally, knowingly, and maliciously to violate
18 Colorado's Consumer Protection Act, and recklessly disregarded Plaintiffs and
19 Arizona Class members' rights.

20 103. As a direct and proximate result of Defendant's unfair and deceptive
21 acts and practices, Plaintiff and Arizona Class members have suffered and will
22 continue to suffer injury, ascertainable losses of money or property, and monetary
23 and non-monetary damages, including from fraud and identity theft; time and
24 expenses related to monitoring their financial accounts for fraudulent activity; an
25 increased, imminent risk of fraud and identity theft; and loss of value of their PII.

26 104. Plaintiff and Colorado Subclass members seek all monetary and
27 nonmonetary relief allowed by law, including the greater of: (a) actual damages, or
28 (b) \$500, or (c) three times actual damages (for Defendant's bad faith conduct);

1 injunctive relief; and reasonable attorneys’ fees and costs.

2 **SIXTH CLAIM FOR RELIEF**

3 **Violation of Pennsylvania Unfair Trade Practices and**

4 **Consumer Protection Law,**

5 **73 Pa. Cons. Stat. §§ 201-2 & 201-3, et seq.**

6 (On Behalf of Plaintiff Jake Thomas and the Pennsylvania Class)

7 105. Plaintiff alleges and incorporates herein by reference, each and every
8 allegation contained in paragraphs 1 through 51, inclusive, of this Complaint as if
9 set forth fully herein.

10 106. Defendant is a “person”, as meant by 73 Pa. Cons. Stat. § 201-2(2).

11 107. Plaintiff and Pennsylvania Class members purchased goods and
12 services in “trade” and “commerce,” as meant by 73 Pa. Cons. Stat. § 201-2(3).

13 108. Defendant engaged in unfair methods of competition and unfair or
14 deceptive acts or practices in the conduct of its trade and commerce in violation of
15 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

- 16 i. Representing that its goods and services have characteristics,
17 uses, benefits, and qualities that they do not have (73 Pa. Stat.
18 Ann. § 201-2(4)(v));
- 19 ii. Representing that its goods and services are of a particular
20 standard or quality if they are another (73 Pa. Stat. Ann. § 201-
21 2(4)(vii)); and
- 22 iii. Advertising its goods and services with intent not to sell them
23 as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

24 109. Defendant’s unfair or deceptive acts and practices include:

- 25 i. Failing to implement and maintain reasonable security and
26 privacy measures to protect Plaintiff and Pennsylvania Class
27 members’ Personal Information, which was a direct and
28 proximate cause of the data breach;

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

- ii. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the data breach;
- iii. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Class members’ Personal Information;
- iv. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Pennsylvania Class members’ Personal Information, including by implementing and maintaining reasonable security measures;
- v. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Class members’ PII;
- vi. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Pennsylvania Class members’ PII; and
- vii. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Class members’ Personal Information.

110. Defendant’s representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant’s data security and ability to protect the confidentiality of consumers’ PII.

111. Defendant intended to mislead Plaintiff and Pennsylvania Class members and induce them to rely on its misrepresentations and omissions.

112. Had Defendant disclosed to Plaintiffs and Class members that its data

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

1 systems or associated companies’ systems were not secure and, thus, vulnerable to
2 attack, Defendant would have been unable to continue in business and it would have
3 been forced to adopt reasonable data security measures and comply with the law.

4 113. Defendant acted intentionally, knowingly, and maliciously to violate
5 Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly
6 disregarded Plaintiff and Pennsylvania Class members’ rights. Defendant’s
7 numerous past data breaches put it on notice that its security and privacy protections
8 were inadequate.

9 114. As a direct and proximate result of Defendant’s unfair methods of
10 competition and unfair or deceptive acts or practices and Plaintiff’s and the
11 Pennsylvania Class’ reliance on them, Plaintiff and Pennsylvania Class members
12 have suffered and will continue to suffer injury, ascertainable losses of money or
13 property, and monetary and non-monetary damages, including from fraud and
14 identity theft; time and expenses related to monitoring their financial accounts for
15 fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss
16 of value of their PII.

17 115. Plaintiff and Pennsylvania Class members seek all monetary and non-
18 monetary relief allowed by law, including actual damages or statutory damages of
19 \$100 (whichever is greater), treble damages, attorneys’ fees and costs, and any
20 additional relief the Court deems necessary or proper.

21 **SEVENTH CLAIM FOR RELIEF**

22 **Violation of New York General Business Law,**

23 **N.Y. Gen. Bus. Law §§ 349, et seq.**

24 (On Behalf of Plaintiff Jake Thomas and the New York Class)

25 116. Plaintiff alleges and incorporates herein by reference, each and every
26 allegation contained in paragraphs 1 through 51, inclusive, of this Complaint as if
27 set forth fully herein.

28 117. Defendant engaged in deceptive acts or practices in the conduct of its

1 business, trade, and commerce or furnishing of services, in violation of N.Y. Gen.
2 Bus. Law § 349, including:

- 3 i. Failing to implement and maintain reasonable security and
4 privacy measures to protect Plaintiff and New York Class
5 members' Personal Information, which was a direct and
6 proximate cause of the data breach;
- 7 ii. Failing to identify foreseeable security and privacy risks,
8 remediate identified security and privacy risks, and adequately
9 improve security and privacy measures following previous
10 cybersecurity incidents, which was a direct and proximate cause
11 of the data breach;
- 12 iii. Failing to comply with common law and statutory duties
13 pertaining to the security and privacy of Plaintiff and New York
14 Class Members' PII;
- 15 iv. Misrepresenting that it would protect the privacy and
16 confidentiality of Plaintiff and New York Class members' PII,
17 including by implementing and maintaining reasonable security
18 measures;
- 19 v. Omitting, suppressing, and concealing the material fact that it
20 did not reasonably or adequately secure Plaintiff and New York
21 Class members' PII; and
- 22 vi. Omitting, suppressing, and concealing the material fact that it
23 did not comply with common law and statutory duties pertaining
24 to the security and privacy of Plaintiff and Class members' PII.

25 118. Defendant's representations and omissions were material because they
26 were likely to deceive reasonable consumers about the adequacy of Defendant's
27 data security and ability to protect the confidentiality of consumers' PII.
28

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

1 119. Defendant acted intentionally, knowingly, and maliciously to violate
2 New York’s General Business Law, and recklessly disregarded Plaintiff and New
3 York Class members’ rights.

4 120. As a direct and proximate result of Defendant’s deceptive and
5 unlawful acts and practices, Plaintiff and New York Class members have suffered
6 and will continue to suffer injury, ascertainable losses of money or property, and
7 monetary and non-monetary damages, including from fraud and identity theft; time
8 and expenses related to monitoring their financial accounts for fraudulent activity;
9 an increased, imminent risk of fraud and identity theft; and loss of value of their
10 PII.

11 121. Defendant’s deceptive and unlawful acts and practices complained of
12 herein affected the public interest and consumers at large, including the millions of
13 New Yorkers affected by the data breach.

14 122. The above deceptive and unlawful practices and acts by Defendant
15 caused substantial injury to Plaintiff and New York Subclass members that they
16 could not reasonably avoid.

17 123. Plaintiff and New York Subclass members seek all monetary and non-
18 monetary relief allowed by law, including actual damages or statutory damages of
19 \$50 (whichever is greater), treble damages, injunctive relief, and attorney’s fees and
20 costs.

21 **EIGHTH CLAIM FOR RELIEF**

22 **Violation of Texas’ Deceptive Trade Practices – Consumer Protection Act,**
23 **Texas Bus. & Com. Code §§ 17.41, *et seq.***

24 (On Behalf of Plaintiff Jake Thomas and the Texas Class)

25 124. Plaintiff alleges and incorporates herein by reference, each and every
26 allegation contained in paragraphs 1 through 51, inclusive, of this Complaint as if
27 set forth fully herein.

28 125. Defendant is a “person,” as defined by Tex. Bus. & Com. Code §

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

1 17.45(3).

2 126. Plaintiff and the Texas Class members are “consumers,” as defined by
3 Tex. Bus. & Com. Code § 17.45(4).

4 127. Defendant advertised, offered, or sold goods or services in Texas and
5 engaged in trade or commerce directly or indirectly affecting the people of Texas,
6 as defined by Tex. Bus. & Com. Code § 17.45(6).

7 128. Defendant engaged in false, misleading, or deceptive acts and
8 practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

- 9 i. Representing that goods or services have sponsorship, approval,
10 characteristics, ingredients, uses, benefits or quantities that they
11 do not have;
- 12 ii. Representing that goods or services are of a particular standard,
13 quality or grade, if they are of another; and
- 14 iii. Advertising goods or services with intent not to sell them as
15 advertised.

16 129. Defendant’s false, misleading, and deceptive acts and practices
17 include:

- 18 i. Failing to implement and maintain reasonable security and
19 privacy measures to protect Plaintiff and Texas Class members’
20 PII, which was a direct and proximate cause of the data breach;
- 21 ii. Failing to identify foreseeable security and privacy risks,
22 remediate identified security and privacy risks, and adequately
23 improve security and privacy measures following previous
24 cybersecurity incidents, which was a direct and proximate cause
25 of the data breach;
- 26 iii. Failing to comply with common law and statutory duties
27 pertaining to the security and privacy of Plaintiff and Texas
28 Class members’ PII;

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

- iv. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Texas Class members' PII, including by implementing and maintaining reasonable security measures;
- v. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' PII;
- vi. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Texas Class members' PII; and
- vii. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Class members' PII.

130. Defendant intended to mislead Plaintiff and Texas Class members and induce them to rely on its misrepresentations and omissions.

131. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

132. Defendant engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Defendant engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

133. Consumers, including Plaintiff and Texas Class members, lacked knowledge about deficiencies in Defendant's data security because this information was known exclusively by Defendant. Consumers also lacked the ability, experience, or capacity to secure the PII in Defendant's possession or to fully protect their interests with regard to their data. Plaintiff and Texas Class members

1 lack expertise in information security matters and do not have access to systems in
2 order to evaluate its security controls. Defendant took advantage of its special skill
3 and access to PII to hide its inability to protect the security and confidentiality of
4 Plaintiffs and Texas Class members' PII.

5 134. Defendant intended to take advantage of consumers' lack of
6 knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless
7 disregard of the unfairness that would result. The unfairness resulting from
8 Defendant's conduct is glaringly noticeable, flagrant, complete, and unmitigated.
9 The data breach, which resulted from Defendant's failure to secure its own systems
10 or those for which it provides customer PII to, exposed Plaintiff and Texas Class
11 members to a wholly unwarranted risk to the safety of their PII and the security of
12 their identity or credit, and worked a substantial hardship on a significant and
13 unprecedented number of consumers. Plaintiff and Texas Class members cannot
14 mitigate this unfairness because they cannot undo the data breach.

15 135. As a direct and proximate result of Defendant's unconscionable and
16 deceptive acts or practices, Plaintiff and Texas Class members have suffered and
17 will continue to suffer injury, ascertainable losses of money or property, and
18 monetary and non-monetary damages, including from fraud and identity theft; time
19 and expenses related to monitoring their financial accounts for fraudulent activity;
20 an increased, imminent risk of fraud and identity theft; and loss of value of their
21 PII. Defendant's unconscionable and deceptive acts or practices were a producing
22 cause of Plaintiff's and Texas Class members' injuries, ascertainable losses,
23 economic damages, and non-economic damages, including their mental anguish.

24 136. Defendant's violations present a continuing risk to Plaintiffs and Texas
25 Class members as well as to the general public.

26 137. Plaintiff and the Texas Class seek all monetary and non-monetary
27 relief allowed by law, including economic damages; damages for mental anguish;
28 treble damages for each act committed intentionally or knowingly; court costs;

1 reasonably and necessary attorneys’ fees; injunctive relief; and any other relief
2 which the court deems proper.

3 **PRAYER FOR RELIEF**

4 WHEREFORE, Plaintiffs, individually and on behalf of all of the Class
5 Members, respectfully requests that the Court enter judgment in his favor and
6 against Defendant as follows:

- 7 A. For an Order certifying the Classes as defined herein and appointing
8 Plaintiffs and his Counsel to represent the Classes;
- 9 B. For equitable relief enjoining Defendant from engaging in the
10 wrongful conduct complained of herein pertaining to the misuse and/or
11 disclosure of Plaintiff’s and Class Members’ PII, and from refusing to
12 issue prompt, complete, and accurate disclosures to Plaintiffs and
13 Class Members;
- 14 C. For equitable relief compelling Defendant to utilize appropriate
15 methods and policies with respect to consumer data collection, storage,
16 and safety and to disclose with specificity to Class Members the type
17 of PII compromised.
- 18 D. For restitution and disgorgement of the revenues wrongfully obtained
19 as a result of Defendant’s wrongful conduct;
- 20 E. For an award of actual damages, statutory damages and compensatory
21 damages, in an amount to be determined at trial;
- 22 F. For an award of costs of suit, litigation expenses and attorneys’ fees,
23 as allowable by law; and
- 24 G. For such other and further relief as this Court may deem just and
25 proper.

26 ///

27 ///

28 ///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd. 12th Floor
Los Angeles, CA 90010-1137

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of himself and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated: April 5, 2019

Respectfully Submitted,

/s/ Thiago M. Coelho
Thiago M. Coelho
Bobby Saadian
Robert J. Dart
Justin F. Marquez
Attorneys for Plaintiffs

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

EXHIBIT A

https://www.kimptonhotels.com/privacy SEP FEB MAY
 25 captures
 24 Dec 2013 - 21 Sep 2018
 2015 2016 2017
 About this capture

Privacy Policy

Legal Statement

The photographs and materials contained in this web site are copyrighted and certain names and logos are protected by federal and/or state trademark registrations. Kimpton Hotel & Restaurant Group, LLC ("Owner") maintains all ownership rights in these materials.

The Owner grants you a non-transferable non-exclusive right and license to use the information provided here for your own personal use or for use by your business, but strictly for purposes of gaining information about the property described and determining whether and how to book reservations at said property. You may not copy, reverse engineer, upload, modify or make derivative works from the materials on this web site, or publish, market, sublicense or market said materials. External links to any portion of this web site must be authorized in advance by Kimpton Hotel & Restaurant Group, LLC.

Privacy

Kimpton Hotel & Restaurant Group uses your personal information in order to fulfill our commitment to providing an unparalleled guest service experience. As part of that undertaking, we are committed to safeguarding the privacy of the personal information that we gather.

As one of our guests, you understand and agree that we collect, use and disclose your personal information in accordance with this Privacy Policy for Guests (this "**Policy**").

TYPES OF PERSONAL INFORMATION WE COLLECT

https://www.kimptonhotels.com/privacy SEP FEB MAY
◀ 16 ▶
2015 2016 2017

25 captures
24 Dec 2013 - 21 Sep 2018

ⓘ ? ✕
f t
▼ About this capture

- your name, gender, home and work contact details, business title, date and place of birth, nationality and passport and visa information;
- guest stay information, including the hotels where you have stayed, date of arrival and departure, goods and services purchased, special requests made, observations about your service preferences (including room and holiday preferences), telephone numbers dialed and faxes and telephone messages received;
- your credit card details, Kimpton Karma Rewards member information, online user account details, profile or password details and any frequent flyer or travel partner program affiliation;
- any information necessary to fulfill special requests (e.g., health conditions that require specific accommodation, purchase of goods and services);
- information you provide regarding your marketing preferences or in the course of participating in surveys, contests or promotional offers;
- information collected through the use of closed circuit television systems, card key and other security systems; and
- contact and other relevant details concerning the employees of corporate accounts and vendors and other individuals with whom we do business (e.g., travel agents or meeting and event planners).
- geolocation information for our mobile internet and iPhone app users, upon your consent

Most of the personal information we process is information that you or someone acting on your behalf knowingly provides to us. However, in some instances, we process personal information that we are able to infer about you based on other information you provide to us or on our interactions with you, or personal information about you that we receive from a third party.

HOW WE USE INFORMATION

Demographic and profile data is collected at our site, and we use this data in two main ways:

First, we analyze visitor information in aggregate, which means that we collect information about thousands of site visits and analyze it as a whole. This kind of study involves looking for trends among many visitors to our site, rather than analyzing information about any individual visitor.

https://www.kimptonhotels.com/privacy SEP FEB MAY
◀ 16 ▶
2015 2016 2017 About this capture

25 captures
24 Dec 2013 - 21 Sep 2018

Second, we may use specific information you provide to help us customize our communications with you and improve our service to you when you visit any Kimpton property, to conduct market research, customer satisfaction and quality assurance surveys and to direct marketing and sales promotions. For instance, if you inform us of a room or service preference, we will attempt to satisfy that request when you visit us in the future and may send you promotions relating to that preference.

We use third parties to build and manage these communication and preference systems, and our arrangements with these third parties prohibit them from disclosing your personal information. [REDACTED]

Specifically, subject to applicable laws, we may collect, use and disclose relevant portions of your personal information in order to:

- provide and charge for the hotel accommodation and other goods and services you purchase;
- provide you with a better, more personalized level of service;
- administer the Kimpton Karma rewards program;
- fulfill contractual obligations to you, anyone involved in the process of making your travel arrangements (e.g., travel agents, group travel organizers or your employer) and vendors (e.g., credit card companies, airline operators and other loyalty programs);
- conduct market research, customer satisfaction and quality assurance surveys, direct marketing and sales promotions;
- respond to requests for information and services;
- provide for the safety and security of staff, guests and other visitors;
- administer general record keeping; and
- meet legal and regulatory requirements

SHARING OF PERSONAL INFORMATION

We reveal Personally Identifiable Information about you to unaffiliated third parties if: [REDACTED]

- you request or authorize it;
- the information is provided to help complete a transaction for you;



or safety of the rights, property or safety of our users or others (e.g., to a consumer reporting agency for fraud protection etc.);

- the disclosure is done as part of a changeover in management of a hotel or restaurant from Kimpton to a third party;
- the information is provided to our agents, outside vendors or service providers to perform functions on our behalf (e.g., analyzing data, providing marketing assistance, providing customer service, processing orders, etc.);or
- to others as described in this Privacy Policy.

Online Preferences

UNSUBSCRIBING

Every e-mail communication from Kimpton or its authorized agents, excepting reservation confirmations and the like, will contain clear and obvious instructions for how you can remove yourself from that mailing list ("Opt-out"). You may also unsubscribe at any time by [updating your subscription preferences here](#).

THIRD PARTY INTERNET SITES^[1]_[SEP]

Third party Internet sites available through advertising and other links on our site have separate privacy and data collection practices. If you click on a link found on our websites or on any other website, you should always look at the location bar within your browser to determine whether you have been linked to a different website. This Policy, and our responsibility, is limited to our own information collection practices. We are not responsible for, and cannot always ensure, the information collection practices or privacy policies of other websites maintained by third parties or our service providers where you submit your personal information directly to such websites. In addition, we cannot ensure the content of the websites maintained by these third parties or our service providers, even if accessible using a link from our websites. We urge you to read the privacy and security policies of any external sites before providing any personal information while accessing those sites.^[1]_[SEP]

THE SECURITY OF YOUR INFORMATION

We work diligently to protect the security of your personal information, including credit card information, during transmission by using Secure Sockets Layer (SSL) software, which encrypts

https://www.kimptonhotels.com/privacy Go SEP FEB MAY
25 captures
24 Dec 2013 - 21 Sep 2018
16
2015 2016 2017 About this capture

our site.

COOKIES

Cookies are small pieces of information that are stored in a browser-related file on your computer's hard drive when you visit our site. We use cookies as necessary to enable certain aspects of our site to function properly, such as our hotel booking engine. We also use cookies to improve your experience, for instance, by allowing you to login without typing the registered email address or registration number and password, and to deliver information and fresh content relevant to your interests. Cookies are also used to collect anonymous information on the pages you visit so we can improve our overall guest services. Some cookies will expire as soon as you leave our site, and others will remain on your browser so we can recognize you when you return to our site. We may use third party advertising companies to serve ads on our behalf. These companies may employ cookies and action tags (also known as single pixel gifs or web beacons) to measure advertising effectiveness.

We use different kinds of cookies for various reasons. Examples of the kinds of cookies we use on our site are below:

- **Session cookies:** These temporary cookies expire and are automatically erased whenever you close your browser. We use session cookies to grant you access to our webpage content and to enable more efficient use of our hotel booking engine.
- **Persistent cookies:** These usually have an expiration date in the distant future and remain in your browser until they expire or you manually delete them. We use persistent cookies to better understand usage patterns so we can improve the site for our users.
- **Third-party cookies:** In keeping with our policies, these session or persistent cookies are set only by trusted partners of our site. For example, we currently use a web analytics service to help us understand usage patterns of our website. No personal data is stored and site usage is always analyzed on an aggregate (and anonymous) basis.

By entering and using our site, you agree that we can place these types of cookies on your device.

"DO NOT TRACK" BROWSER SETTINGS

https://www.kimptonhotels.com/privacy SEP FEB MAY
 25 captures
 24 Dec 2013 - 21 Sep 2018
 2015 2016 2017
 About this capture

USE OF REPORTING SERVICES^[L]_[SEP]

We may use independent reporting services to analyze traffic to our website. These reporting services do not create individual profiles for each visitor and do not maintain a database of individual profiles. These services only collect aggregate data, which is used solely for analytical purposes. This kind of study involves looking for trends among many visitors to our site, rather than analyzing information about any individual visitor.

BROWSER MONITOR

We may employ a browser monitor within web pages on our site in order to determine your browser status and the client-side metrics relating to page loading. We constantly seek ways to improve page load times for our visitors and may ultimately use these metrics for such purposes. Any such browser monitor will only be active while the user is active on our site. For your protection, any such browser monitor will not require an executable (*.exe) application.

IP ADDRESS^[L]_[SEP]

Like most Internet sites, we use your IP address to help diagnose problems with our server, and to administer our site. Your IP address is also used to gather broad demographic information.^[L]_[SEP]

CHILDREN

Our websites do not sell products or services for purchase by children. If you are under the age of 18, you may only use our websites with the involvement of a parent or guardian.

CHANGES TO THIS POLICY

Just as our business changes constantly, this Policy may also change. To assist you, this Policy has an effective date set out at the end of this document.

Your California Privacy Rights^[L]_[SEP]

For California residents only. We may disclose your personal information to our affiliates or other Kimpton-related third parties for their use in marketing to you. Pursuant to California's "Shine the Light Act," California residents are permitted to request information about the manner in which we

https://www.kimptonhotels.com/privacy SEP FEB MAY
 25 captures 24 Dec 2013 - 21 Sep 2018 2015 2016 2017 About this capture

We will provide the required information to your email address in response. Please be aware that not all information sharing is covered by the "Shine the Light" requirements and only information on covered sharing will be included in our response.

EMAIL ADDRESS *

Submit Contact Form

Contact Us

If you have any questions about our privacy policies or any other matter, please contact us at privacypolicy@kimptongroup.com.

Effective Date

November 5, 2015

QUICK LINKS 

ABOUT US 

GET IN TOUCH 

1-800-KIMPTON (546-7866)

KIMPTON BLOG LIFE IS SUITE

https://www.kimptonhotels.com/privacy

Go

SEP FEB MAY

16

2015 2016 2017



About this capture

25 captures

24 Dec 2013 - 21 Sep 2018

Kimpton Hotel & Restaurant Group, LLC © 2016


Privacy + Legal Your CA Privacy Rights Sitemap

EXHIBIT B

Advertisement

 [Subscribe to RSS](#)

 [Follow me on Twitter](#)

 [Join me on Facebook](#)



LIVE BROADCAST
SAY "HACK NO!" TO CYBER THREATS
NOC + SOC = Better Visibility and Security
THURSDAY APR. 18 | 10AM PDT 1PM EDT

HACK, NO!

Infoblox 

REGISTER NOW »

Krebs on Security

In-depth security news and investigation



[About the Author](#)
[Advertising/Speaking](#)

26
Apr 16

All About Fraud: How Crooks Get the CVV

A longtime reader recently asked: “How do online fraudsters get the 3-digit [card verification value](#) (CVV or CVV2) code printed on the back of customer cards if merchants are forbidden from storing this information? The answer: If not via phishing, probably by installing a Web-based keylogger at an online merchant so that all data that customers submit to the site is copied and sent to the attacker’s server.

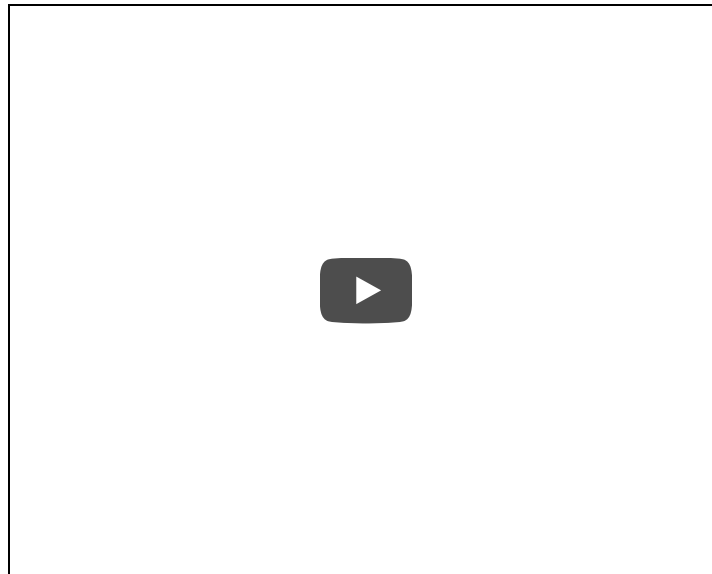
Kenneth Labelle, a regional director at insurer **Burns-Wilcox.com**, wrote:

“So, I am trying to figure out how card not present transactions are possible after a breach due to the CVV. If the card information was stolen via the point-of-sale system then the hacker should not have access to the CVV because its not on the magnetic strip. So how in the world are they committing card not present fraud when they don’t have the CVV number? I don’t understand how that is possible with the CVV code being used in online transactions.”

First off, “dumps” — or credit and debit card accounts that are stolen from hacked point of sale systems via skimmers or malware on cash register systems — retail for about \$20 apiece on average in the cybercrime underground. Each dump can be used to fabricate a new physical clone of the original card, and thieves typically use these counterfeits to buy goods from big box retailers that they can easily resell, or to extract cash at ATMs.

However, when cyber crooks wish to defraud online stores, they don’t use dumps. That’s mainly because online merchants typically require the CVV, criminal dumps sellers don’t bundle CVVs with their dumps.

Instead, online fraudsters turn to “CVV shops,” shadowy cybercrime stores that sell packages of cardholder data, including customer name, full card number, expiration, CVV2 and ZIP code. These CVV bundles are far cheaper than dumps — typically between \$2-\$5 apiece — in part because they are useful mainly just for online transactions, but probably also because overall they more complicated to “cash out” or make money from them.



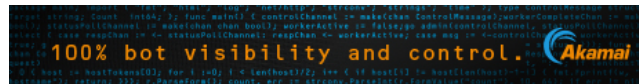
The vast majority of the time, this CVV data has been stolen by Web-based keyloggers. This is a relatively uncomplicated program that behaves much like a banking Trojan does on an infected PC, except it's designed to steal data from Web server applications.

PC Trojans like ZeuS, for example, siphon information using two major techniques: snarfing passwords stored in the browser, and conducting “form grabbing” — capturing any data entered into a form field in the browser before it can be encrypted in the Web session and sent to whatever site the victim is visiting.

Web-based keyloggers also can do form grabbing, ripping out form data submitted by visitors — including names, addresses, phone numbers, credit card numbers and card verification code — as customers are submitting the data during the online checkout process.

These attacks drive home one immutable point about malware's role in subverting secure connections: Whether resident on a Web server or on an end-user computer, if either endpoint is compromised, it's ‘game over’ for the security of that Web session. With PC banking trojans, it's all about surveillance on the client side pre-encryption, whereas what the bad guys are doing with these Web site attacks involves sucking down customer data post- or pre-encryption (depending on whether the data was incoming or outgoing).


If you're responsible for maintaining or securing Web sites, it might be a good idea to get involved in one or more local groups that seek to help administrators. Professional and semi-professionals are welcome at local chapter meetings of [OWASP](#), [CitySec](#), [ISSA](#) or [Security Bsides](#) meetups.




Tags: [bsides](#), [Burns-Wilcox](#), [citysec](#), [cvv](#), [cvv2](#), [dumps](#), [issa](#), [Kenneth Labelle](#), [owaps](#), [web-based keyloggers](#), [zeus](#)

This entry was posted on Tuesday, April 26th, 2016 at 2:56 pm and is filed under [A Little Sunshine](#), [Web Fraud 2.0](#). You can follow any comments to this entry through the [RSS 2.0](#) feed. Both comments and pings are currently closed.

53 comments


- 
[Bruce Hobbs](#)
[April 26, 2016 at 5:33 pm](#)

I use IBM's Trusteer Endpoint Protection (Rapport) which is supposed to block these key loggers either on my computer or on the server I'm connecting to. My understanding is that they encrypt the keystrokes before the SSL encryption and the encryption continues on the server after the SSL encryption has been removed. I have no idea if it works except I have no problems with online transaction fraud (which really doesn't prove that it works).

- 
[Bruce Hobbs](#)
[April 26, 2016 at 5:36 pm](#)

Brian, you wrote about Rapport back on April 29, 2010. Since then, IBM has bought them.

<http://krebsonsecurity.com/2010/04/a-closer-look-at-rapport-from-trusteer/>

- 
[zboot](#)
[April 26, 2016 at 5:38 pm](#)

Brian, I'm not sure I understand how the CVV dumps are not worth as much as the normal card shops. It seems the CVV dumps has everything you'd get from a card shop plus the CVV2 and zipcode. Why wouldn't you be able to fabricate a physical card from that data just as well as you could from card shop data?



Gavin

[April 26, 2016 at 6:22 pm](#)

The CVV Dumps are worth less because they have not been compromised physically, only digitally. Carders using the cloning method wouldn't be comfortable trying to clone a card they weren't sure had been physically compromised because there is not proof that the card will be active still. Who's to say the cards caught I'm the CVV dumps haven't been used in other ways by other crooks where they tend to keep physical dumps much more private, selling once, maybe twice.



Jim

[April 27, 2016 at 6:50 am](#)

Actually, a CNP dump doesn't have all of the information necessary to create a physical card. A common point of confusion is that there are actually two CVVs per card – one is encoded only on the mag stripe (the "CVV" or "CVV1") and the other is printed physically on the back of the card (the "CVV2", which is what most people refer to as the "CVV"). Consumers cannot enter the CVV1 to complete an ecommerce transaction as they have no idea what it is. Likewise, no brick-n-mortar merchant I know requests consumers enter the CVV2 during checkout. So, a dump obtained from an ecommerce merchant cannot be used at brick-n-mortar retailers and vice versa. And since ecommerce fraud is, all things being equal, trickier to monetize those dumps are worth less.



Joe

[April 27, 2016 at 8:00 pm](#)

I actually have seen stores enter the CVV2 code into their POS system. These stores usually have a sign "show the card to the cashier" or the like.



Ross

[April 28, 2016 at 9:04 am](#)

Can't speak for the stores you visited, but when I worked retail and had to ask for the card, it was basically a minor security measure (checking that the signature on the card matched the signature on the pin pad). To prove that we had taken the card from the customer (and I suppose as another level of security against a badly made counterfeit), we had to punch in the last four digits of the card number. However, we never touched the CVV.



Greybeard

[April 29, 2016 at 9:21 am](#)

And most cashiers have no idea why they're asking for that "last 4" (beyond "because I'm supposed to"), so most buyers just say the last four digits—thus totally voiding any theoretical security value to the process, alas!



Thomas

[April 28, 2016 at 11:23 am](#)

Entering the CVV2 at point of sale is now supported as a form of additional verification that a card is genuine.



Hav0c

[April 28, 2016 at 11:28 am](#)

Joe – most stores that require you to hand over the card are entering the last 4 digits printed on the card and the POS is validating they match the last 4 digits from the track data. This makes is a bit more difficult to cash out dumps as you need to have a card that the last 4 digits match track data or it fails this transaction. Simple effective process. Now if we only start using the PIN portion for EMV...probably at the same time we adopt the metric system.




DesertIT


[May 3, 2016 at 2:53 pm](#)

LOL

I agree, and although America should be using strictly PIN and no signature, Americans should at least currently have a choice between signature or PIN rather than just forcing the insecure use of signature with the new chip cards.

 [MadAnthony](#)
[April 26, 2016 at 8:24 pm](#)


Using a card online usually means buying something and having it physically shipped somewhere other than the billing address. Merchants tend to flag those to begin with, and the criminal needs to have it shipped somewhere that can't be connected to them. That's spawned the whole mail-drop schemes that have been written about on this site, and means the scammer needs to convince someone to have stuff shipped to them and then ship it to the scammer.

▪  [darrell](#)
[May 3, 2016 at 1:36 am](#)


Sounds like a good idea. But even a small online business can process hundreds of credit card transactions per day. To limit buyers to ship only to their billing address limits fraud but also keep legit buyers from sending gifts, shipping to their job, girlfriend, boyfriends, parents house ect. Software flags some fraud transactions but the rest have to be manually reviewed.

◦  [zboot](#)
[April 28, 2016 at 11:24 am](#)


Wow, thanks everyone for the responses. You've taught me a lot which will help keep me more secure!

3.  [Sven](#)
[April 26, 2016 at 6:01 pm](#)


Another way of obtaining CVV info (although keyloggers and other malware is the lion's share) is via skimmers that integrate cameras to take pictures of the cards as they're being swiped.

4.  [Y](#)
[April 26, 2016 at 7:49 pm](#)


Brian writes "PC Trojans like Zeus, for example, siphon information using two major techniques: snarfing passwords stored in the browser." Does that mean if someone chooses to store passwords on their personal pc, a Trojan like Zeus can grab that information?

◦  [BrianKrebs](#)
[April 27, 2016 at 12:41 pm](#)

yes that's correct.

5.  [Mike](#)
[April 26, 2016 at 9:50 pm](#)

There is nothing to worry about...
Just update you OS and your browser and you will be fine.

◦  [simguy](#)
[April 27, 2016 at 11:48 am](#)

Updating your OS and browser and keeping it 100% up to date will not do ANYTHING to stop a phishing attempt in your email that you click on because you think it's from your bank. It won't do ANYTHING to protect you against a zero day exploit on a malicious ad from a well known site that installed a keylogger.


For instance just a few weeks ago:

<http://arstechnica.com/security/2016/03/big-name-sites-hit-by-rash-of-malicious-ads-spreading-crypto-ransomware/>

"It hit some of the biggest publishers in the business, including msn.com, nytimes.com, bbc.com, aol.com, my.xfinity.com, nfl.com, realtor.com, theweathernetwork.com, thehill.com, and newsweek.com."

You ever visit msn.com the default homepage set by IE?
You ever visit BBC or newsweek or new york times websites?


You can get hit with malicious ads from anywhere. You need to have more defenses than just "Oh I keep my OS and browser updated so I'm perfectly safe" or else you will get infected someday.

▪  [Mike](#)
[April 27, 2016 at 1:45 pm](#)

Exactly!

6.  [Christoph](#)
[April 27, 2016 at 4:05 am](#)

And another source of compromise of course are the retailers that DO store CVV2, contrary to the rules, and have their database hacked.


-  [Jim](#)
[April 27, 2016 at 6:55 am](#)

To be precise: merchants are allowed to retain the CVV1 or CVV2 until the transaction has been authorized. If the merchant is operating in “fallback” for a period of time (meaning, they are not able to connect to their acquirer to authorize the transaction – typically due to connectivity or network issues), they can retain this information (although it must per PCI DSS be encrypted while at rest) until the transaction is completed. The merchant is, of course, taking on a risk that the transaction is not authorized when connectivity to the acquirer is restored – but for business reasons many merchants accept this risk in the name of customer satisfaction.


-  [Mike](#)
[May 2, 2016 at 11:36 am](#)

Apparently, some merchants are allowed more, eg Steam keeps CVV2 for as long as they like for one-click orders.


Amazon, on the other hand, doesn't even ask for it at all. My friend with banking background (and good knowledge of PCI DSS) was shocked.

7.  [Jerry](#)
[April 27, 2016 at 4:27 am](#)

I always wondered if CVVs couldn't be extracted more easily at brick and mortar point of sale – where I live it's common for salespeople to physically handle customer cards, so how hard could it be for them to either memorize the number or show it to a camera (either one put in specifically for this reason, or one of store's surveillance ones)? This not only does not require advanced IT skills, but also makes detecting source of the leak harder.

8.  [George Dragojevic](#)
[April 27, 2016 at 6:22 am](#)

Hey Brian, I definitely agree with you that everybody who are responsible for maintaining any website security should be seeking for help from other professional administrators.

-  [Mike](#)
[April 27, 2016 at 6:30 am](#)

No one is responsible for anything. Security will automatically come to you in the form of an update from Apple and Microsoft. Those who maintain websites only need to make sure they maintain their connections to their cloud based advertisers.


9.  [Gillespie](#)
[April 27, 2016 at 6:40 am](#)

re: Jerry's remarks about the physical handling of cards

My wife noticed recently that in contrast to the US, where the card disappears for various lengths of time, here in Germany card transactions are carried out at the table, counter or POS via wireless readers. The only time the card “leaves” your possession is when it's inserted in the reader. You're then given the reader to enter your pin number on a screened keyboard, whereupon a receipt is printed out by the gadget. I suppose it would be possible to note the CVV number with some skillful manipulation, but it surely wouldn't be so easy or ubiquitous.

10.  [paul](#)
[April 27, 2016 at 6:52 am](#)

If CVV is only needed for online purchases, can cardholders write down the CVV, keep it at home, and then scrape the CVV off the back of the card?

-  [Jim](#)
[April 27, 2016 at 6:59 am](#)

For the CVV2, yes – one could do that. If you can see it on your card, anyone who handles your card and has a good memory has access to the same information necessary to perform an ecommerce transaction. Well, except for your ZIP code and address, assuming the ecommerce merchant is performing address verification (which most now do).



Jay

[April 27, 2016 at 7:23 pm](#)

why not just cover the CVV2 with black electrician's tape? Easy to remove if you really need to use it, but covered otherwise.



somguy

[April 27, 2016 at 11:50 am](#)

Scraping off the number will protect you from a single source:
Camera's that capture this info at physically compromised sites like ATMs.

It will NOT protect you if you have keylogger on your computer. It will NOT protect you if the retailer's website is compromised and sending captured information to the thieves.



somguy

[April 27, 2016 at 11:52 am](#)

Unless of course you never ever type in or use the cvv2 for any purposes whatsoever.
But then you are still vulnerable from identity theft, and skimmers, and many other sources, even if you never ever made any credit card purchase online.

11.



Hon

[April 27, 2016 at 7:34 am](#)

Many of card managements systems around the world suffered from fraudulent attack coming from Brazil. They using Bin attack technique and generate cards through card generation tools and send deferent authorization message one time as e commerce transaction, magnetic transactions and chip transactions looking for any bugs in authorization system. When they successful with any attempts they send thousands of trails with the same pattern when they got approval for any card they decode this data on card and send physical card to the market to make a lot of transaction though their gang members. They depend on authorizations system fail or security problem to do such of this transactions

12.



Rick Romero

[April 27, 2016 at 8:46 am](#)

It makes me giggle how everyone likes to over complicate things. Keep in mind that just because a merchant has a field for CVV, it's doesn't mean they're requiring a valid CVV that at their processor to accept the payment.

There are multiple levels of card holder verification (including address verification) that may be used by the merchant when the transaction is authorized. If too many of their customers are having issues making payments, some of these may be disabled. It's worth it to them to pay a higher price for processing within a higher fraud category, because they'll make up for it in increased revenue. Especially online-only merchants who have customers in multiple countries.

13.



R Mccoy

[April 27, 2016 at 9:17 am](#)

Some merchants are not honest about storing the CVC2 information. When the CVC2 information is sent to the issuer and/or processor for recurring merchants it can come across in two different ways. For your Netflix, and other subscription service you will see a straight up CVC2/CVV2 validation on the first transaction (sign up) and any other monthly transactions will display a different code which denotes that the CVC2/CVV2 was not passed. However, there are other subscription services we will see the validation of the CVC2 every single transaction meaning that the CVC2 is stored. Happens clockwork on the specific billing day that was set by merchant of that month.

Now there is an exception to merchants selling tangible/intangible goods. Everyone who frequents some off brand website notices the button "save your card info". Ok....., what I noticed while doing a test with one of my frequent personal merchants is that even though they saved it they still require the CVC2/CVV2 every time. I can't speak for all. I do not know much about the keylogger situation, but when there is something of value...there is a means & method to steal it.




Greybeard


[April 29, 2016 at 9:25 am](#)

Indeed. And if you notice such a case, call 1-800-VISA-911 or 1-800-MC-ASSIST or 1-800-333-AMEX and report it. That's a PCI violation.

Of course, as others have noted, that doesn't exactly call in an airstrike, or indeed guarantee *any* action. But it's worth a try.

-  *R Mccoy*
[April 29, 2016 at 3:02 pm](#)

I normally send more severe issues, but they are quite lient on the merchants. They see the outcome codes the same as I do so no doubt they are aware. I can't be a hypocrite here since I brought it up, so I will compile a list and send them my merchant list. Lets see where it goes. Thx.

14.  *Paul Goble*
[April 27, 2016 at 10:33 am](#)

Keyloggers may be the easiest way to gather large quantities of CVV2 codes, but fraudsters have many options. Certain industries routinely collect CVV2 on paper forms, which are then either scanned or placed in long-term storage. When I've talked to merchants about it, it's clear that they are conflating card-not-present transactions with *real-time* card-not-present transactions, then relying on some kind of warped folklore about what PCI says about CVV2 storage. Storage locker rentals and medical providers are the worst violators, in my experience. I imagine those businesses would be especially lucrative targets. Brick-and-mortar merchants don't usually collect CVV2, but merchants under canvas sure do—I've also noticed that quite a few small merchants at various festivals and fairs will scribble down the CVV2 when processing a credit card transaction. I bet a fair number shady businesses just aim a camera at their counter and transcribe card information at their leisure. I'd love to see a hotline where consumers could report blatant PCI violations like these.

15.  *BillP*
[April 27, 2016 at 1:13 pm](#)

Jim has it 100% right (who do you work for?). The article is pretty much ancient data and card security / card transaction risk mitigation professionals have known this for almost 20 years.

PC attacks and communication compromises have been around since the beginning. It's one of the reasons SET was written in 1996 (RIP). It's also the reason why CVC / CVV is different from CVC2 / CVV2. It was designed to be different (except for wild chance).

Chip card does NOTHING to prevent ecommerce fraud. It has been sold to the great unwashed masses as the final word in card security, but that 1993 EMV concept fails in today's huge CNP environment.

16.  *Keith appleyard*
[April 27, 2016 at 1:51 pm](#)

A colleague here in the UK once showed me an Excel-based Invoice he had received from a small Retailer which contained all of his Card details, including the CVV. He didn't know who the Merchant Acquirer was, so as a public-minded citizen I wrote to all of the major players in the UK on the off-chance they'd react. Only 1 responded to me (HSBC), and suggested I take it up with the Merchant myself. Barclays, Lloyds, Natwest & RBS never even replied to me – that's how seriously they took it.

17.  *JTL*
[April 27, 2016 at 2:29 pm](#)

I guess "keylogger" for server-side malware would be the wrong terminology but I understand the concept.

Server-side formgrabber?

18.  *Andrew C.*
[April 27, 2016 at 3:34 pm](#)

"if merchants are forbidden from storing this information?" – Yes. Merchants are forbidden from storing this info... but most of them still do. I have had a lot of companies try to write the CVV on the invoice for sake of convenience.

19.  *MikeK*
[April 27, 2016 at 10:11 pm](#)

It's pretty easy to get the CVC2/CVV2. There are only 999 possibilities. Card numbers have only so many possibilities if the first 6-8 are fixed and the last one is a check digit. With a card number, all you need is a bunch of websites that check the cvc2/cvv2 (every ecommerce site in existence) and check the 1000 possibilities, brute force. You don't check the same site twice from the same attacker and you don't check the same card twice at the same site. You use a bot net that can work on this 24x7 until you've cracked the cvv/cves for the lot.

However, it's often easier to just crack the users password at a retailer's site and add a new address, change the email, change the password, order stuff, send to new address, and then clean up, and put things back. Or not, and resell the account.

You'd be amazed at what mortgage refinance companies leave unprotected in the cloud and on their systems.



John

[April 28, 2016 at 8:58 am](#)

Wouldn't work, would kill the card making it useless for faudsters.



Patrick Star

[April 30, 2016 at 12:24 pm](#)

Works just fine if you have a lot of cards. Think big DB dump(s). That way you can limit the number of guesses per card – even with just a single guess per card, you'd get 1000 valid CVV2s from a dump of a million.



surik

[April 28, 2016 at 8:36 am](#)

its end of the card chips anyways, in near future we all will have micro chips under our skin, thats so simple this is nothing jet



Hav0c

[April 28, 2016 at 11:47 am](#)

It would be interesting to shift the burden to the acquirer by forcing websites to inject iframes to the acquirers portal (Chase / Paymentech – Orbital). Then the only point of compromise is the acquirer or the users PC. I only use online ordering from about 5 large vendors. After that I use Paypal or generate a 1 time use (or 1 month use) virtual card. I believe all major banks have that ability. That way compromise of a card is does not impact my physical card and is time, transaction or dollar bound so minimal impact. It would be really nice for the banks to create the one time payment via the injected iframe and only send trx and auth data to merchant so no chance for them to lose the data.



Bill

[April 28, 2016 at 4:41 pm](#)

I use a program called KeyScrambler, which according to their website: Encrypts in real time your keystrokes on all websites and keeps them safe through the operating system to protect your privacy/identity, even on infected computers. I use the free personal version. It gets good reviews. I hope it works as advertised. Link: <http://www.qfxsoftware.com/download.htm>



Ed F Dev Prog

[April 28, 2016 at 9:08 pm](#)

I don't know if BK himself keeps up with all comments, but I'd like to thank him for mentioning local memberships of OWASP. I've looked at their sites before but had no idea they were an organization you could join like a professional association.

I work with some PCI-compliant-ish code and I'm setting up new web-facing stuff with MVC, and between this site and Ars Technica, I've come to take security about 10,000% more seriously than the others at work, including our "PCI compliance officer."

Joining OWASP and using their security-101 site seem like really good ideas to help make sure my work doesn't suck. I'm mentioning OWASP here but I don't exclude the others BK mentioned.

This is why we visit KOS. All hail BK and I'll be sure to donate again this year.



Charles Spong

[April 29, 2016 at 5:42 pm](#)

I believe if the processor offers P2PE (Point to Point Encryption) with Tokenization, everything is encryption, including keyed transactions.



DesertIT

[May 3, 2016 at 2:44 pm](#)

Don't forget local ISC2 Chapters!




William Hugh Murray, CISSP

[May 5, 2016 at 12:08 am](#)

Consumers should prefer online merchants that support checkout proxies like PayPal, Amazon, MasterCard MasterPass, and Visa Checkout. If they enter their CVV at enough on line merchants, they will hit one that is compromised.

Merchants should support these proxies rather than accept credit cards themselves. The proxies will provide the merchant with all the advantages of accepting credit cards, improve customer convenience, speed checkout, and provide both merchants and consumers with improved security.

◦  *Estoppel*
[May 15, 2016 at 3:13 pm](#)

Not until there's adequate legal and regulatory frameworks in place to keep these processors in line. Paypal is well known for being a target of fraud both in the theft of its accounts and ridiculously one-sided chargebacks (although as someone who isn't too long out of law school, the word between my friends is that their PLLCs tend not to lose chargebacks like when they were selling things on eBay that they sent without tracking numbers). Ultimately everyone is trying to cover their own ass but the end user is the one least able to. Going through Paypal or Amazon or a bank just can screw the end user, business or customer, just as easily merely in different ways.

Advertisement



Independently conducted by Ponemon Institute LLC

Assessing the DNS SECURITY RISK

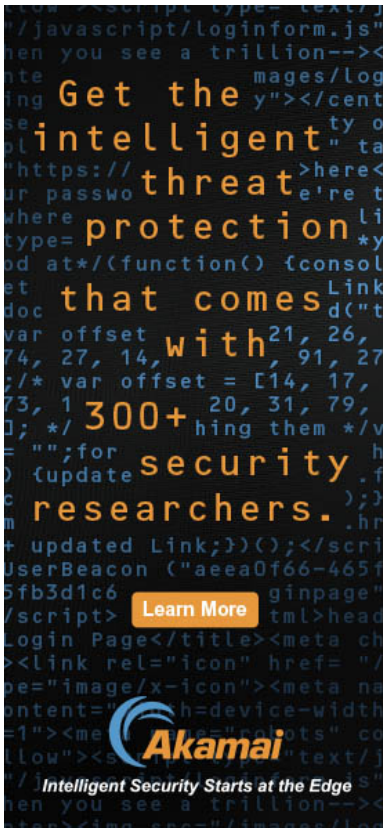
Ponemon INSTITUTE

Infoblox  [READ THE SURVEY REPORT >>](#)

• 


• **Mailing List**

• [Subscribe here](#)



Get the intelligent threat protection that comes with 300+ security researchers.

[Learn More](#)

 **Akamai**

Intelligent Security Starts at the Edge

• **Recent Posts**

- [Annual Protest Raises \\$250K to Cure Krebs](#)
- [Man Behind Fatal 'Swatting' Gets 20 Years](#)
- [A Month After 2 Million Customer Cards Sold Online, Buca di Beppo Parent Admits Breach](#)
- [Alleged Child Porn Lord Faces US Extradition](#)
- [Facebook Stored Hundreds of Millions of User Passwords in Plain Text for Years](#)

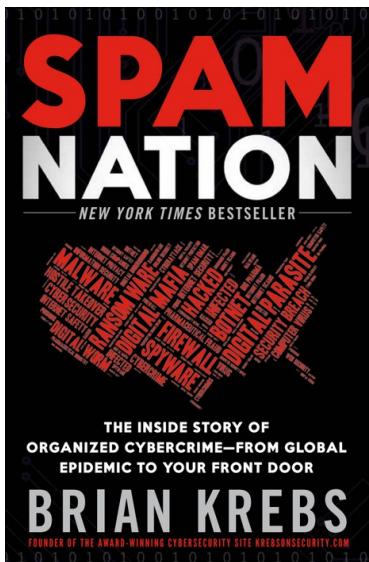
• **All About Skimmers**



Click image for my skimmer series.



• **Spam Nation**



A New York Times Bestseller!



• **The Value of a Hacked PC**



Badguy uses for your PC

• **Tools for a Safer PC**



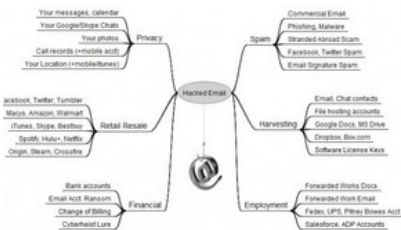
Tools for a Safer PC

• **The Pharma Wars**



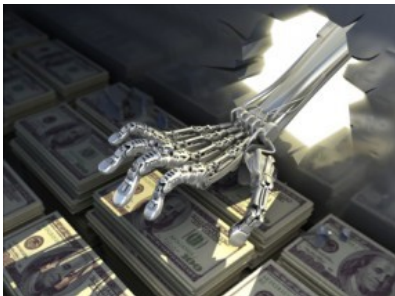
Spammers Duke it Out

• **Badguy Uses for Your Email**



Your email account may be worth far more than you imagine.

• **eBanking Best Practices**



eBanking Best Practices for Businesses

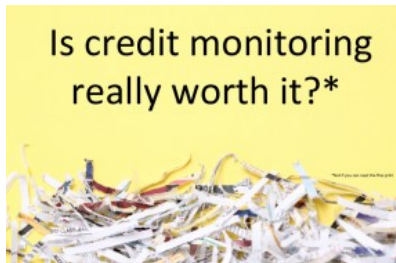
• **Most Popular Posts**

- [Sextortion Scam Uses Recipient's Hacked Passwords](#) (1076)
- [Online Cheating Site AshleyMadison Hacked](#) (798)
- [Sources: Target Investigating Data Breach](#) (620)
- [Cards Stolen in Target Breach Flood Underground Markets](#) (445)
- [Reports: Liberty Reserve Founder Arrested, Site Shuttered](#) (416)
- [Was the Ashley Madison Database Leaked?](#) (376)
- [True Goodbye: 'Using TrueCrypt Is Not Secure'](#) (363)
- [Who Hacked Ashley Madison?](#) (361)
- [Following the Money, ePassporte Edition](#) (353)
- [U.S. Government Seizes LibertyReserve.com](#) (315)

• **Category: Web Fraud 2.0**



Innovations from the Underground



ID Protection Services Examined

• **Is Antivirus Dead?**



The reasons for its decline

• **The Growing Tax Fraud Menace**



File 'em Before the Bad Guys Can

• **Inside a Carding Shop**



A crash course in carding.

• Beware Social Security Fraud



At each stage of your life, my Social Security is for you. Your personal online my Social Security account is a valuable source of information beginning in your working years and continuing throughout the time you receive Social Security benefits.

If you receive benefits or have Medicare, you can:

Use a my Social Security online account to:

- Get your benefit verification letter;
- Check your benefit and payment information and your earnings record;
- Change your address and phone number; and
- Start or change direct deposit of your benefit payment.

Sign up, or Be Signed Up!

• How Was Your Card Stolen?



Finding out is not so easy.

• Krebs's 3 Rules...



...For Online Safety.

EXHIBIT C

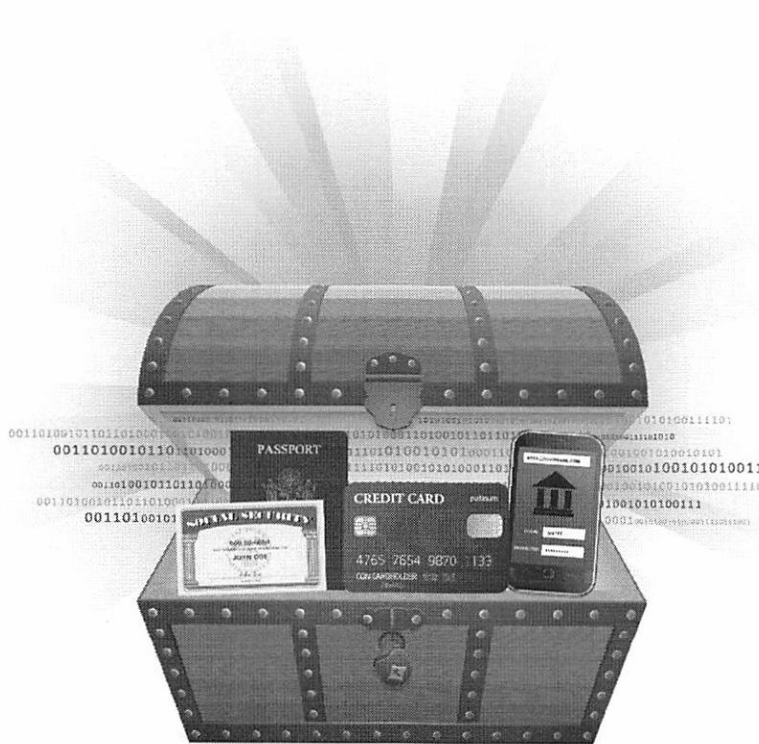


STRATEGIC INSIGHTS INTO
CUSTOMER TRANSACTIONS

2013 IDENTITY FRAUD REPORT:

Data Breaches Becoming a Treasure Trove for Fraudsters

February 2013





2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a Treasure Trove for Fraudsters

ABOUT JAVELIN:

Javelin Strategy & Research, a division of Greenwich Associates, provides strategic insights into customer transactions, increasing sustainable profits for financial institutions, government, payments companies, merchants and other technology providers.

AUTHORS:

Alphonse Pascual, Senior Analyst, Security, Risk and Fraud
Sarah Miller, Analyst, Security, Risk and Fraud

RESEARCH:

Lorie Curtis, Research Associate
James Jarzab, Research Specialist
Aleia Van Dyke, Analyst
Daniel Van Dyke, Research Associate
Paul Wangsvick, Research Specialist

CONTRIBUTORS:

Jim Van Dyke, CEO
Mary Monahan, Executive Vice President and Research Director

PUBLICATION DATE: February 2013

PRICE: \$3,000 - Department license
\$5,500 - Enterprise license

LENGTH: 82 pages
56 charts/graphs

OVERVIEW

Identity fraud incidence increased in 2012 for the second consecutive year, affecting 5.26% of U.S. adults. This increase was driven by dramatic jumps in the two most severe fraud types, new account fraud (NAF) and account takeover fraud (ATF). Javelin's "2013 Identity Fraud Report" provides a comprehensive analysis of fraud trends in the context of a changing technological and regulatory environment in order to inform consumers, financial institutions, and businesses on the most effective means of fraud prevention, detection, and resolution. This year, Javelin conducted a thorough exploration of the relationship between the compromise of personal information in a data breach and fraud incidence. This report also expounds current trends in online retail fraud and familiar fraud, and implicates key factors in victims' susceptibility and responses to fraud. "2013 Identify Fraud Report" data was gathered by a survey of a representative sample of 5,249 U.S. adults, including 857 consumers who were fraud victims in the past six years. This report has been issued as a longitudinal update to the Javelin 2005, 2006, 2007, 2008, 2009, 2010, 2011 and 2012 identity fraud reports, and the Federal Trade Commission's "2003 Identity Theft Survey" report.

The survey was made possible in part by CitiGroup Inc., Intersections LLC, and Visa Inc. To preserve the project's independence and objectivity, the sponsors of this project were not involved in the tabulation, analysis, or reporting of final results.



2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a Treasure Trove for Fraudsters

METHODOLOGY

The 2013 Javelin “Identity Fraud Survey Report” provides consumers and businesses an in-depth and comprehensive examination of identity fraud in the United States. Its purpose is to help readers understand the causes and incidence rates of identity fraud and the success rates of methods used for its prevention, detection, and resolution.

This report builds on Javelin’s annually published “Identity Fraud Survey Report” and the Federal Trade Commission’s “2003 Identity Theft Survey Report.”

2012 SURVEY DATA COLLECTION

Javelin’s ID fraud survey was historically fielded as a landline survey using computer-assisted telephone interviewing (CATI). At the time of the survey’s inception in 2003, landlines provided a relatively comprehensive coverage of the U.S. population. However, with advent of time and technology, landline coverage has been shrinking — thus the ID fraud survey has had increasingly less penetration into the younger, more-mobile population. Cognizant of this shift, in 2011 Javelin fielded the ID fraud survey through the KnowledgePanel®. Javelin continued to use KnowledgePanel for its 2012 and 2013 ID fraud surveys in order to obtain the most representative sample of U.S. adults.

KnowledgePanel is the only probability-based online panel in the U.S. The panel recruits households with no access to Internet (at the time of recruitment) as well as cell-phone-only households, through mail recruitment. The panel offers a mix of RDD-based recruitment (1999–present) and address-based sampling (introduced in 2008 with a full rollout in 2009).

The 2013 ID fraud survey was conducted among 5,249 U.S. adults over age 18 on KnowledgePanel; this sample is representative of the U.S. census demographics distribution, recruited from the Knowledge Networks panel. Data collection took place between September 20 and October 12, 2012. Final data was weighted by Knowledge Networks, while Javelin was responsible for data cleaning, processing, and reporting. Data is weighted using 18+ U.S. Population Benchmarks age, gender, race/ethnicity, education, census region, and metropolitan status from the most current CPS targets.

LONGITUDINAL TRENDING

Given the departure from the previous computer-assisted telephone interviewing (CATI) through random digit dialing (RDD), Javelin also fielded a parallel CATI survey among 1,000 18+ adults in 2011 through Opinion Access in order to derive calibration estimates to trend and update longitudinal data. For all questions asked of the entire population, 2003–2010 data has been calibrated using ratios derived from comparing 2011 CATI vs. web-based survey. For other questions affecting only a subset of the population, a three-year rolling average has been applied to smooth year-over-year trending data.



2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a Treasure Trove for Fraudsters

In adherence with best practices, in 2011 Javelin also moved from bracketed dollar amount calculations to true open-end numerical dollar calculations. On continuous variables captured from numerical open-ended items, extreme outliers were identified using a standard rule of approximately two standard deviations above the mean to retain consistency year over year. These extreme outliers were replaced with mean values to minimize their disproportionate impact on final weighted estimates. Where responses pertained to a range in value (e.g., "one day to less than one week"), the midpoint of the range, rounded up to the nearest whole unit, was used to calculate the median or mean value. For example: If the response selected for number of days to detection was one day to less than one week, the assigned value would be the median of one day and seven days, inclusive, or four days. To ensure consistency in comparing year-to-year changes, historical figures for average fraud amounts have been adjusted for inflation using the Consumer Price Index.

Due to rounding errors, the percentages on graphs may add up to 100% plus or minus 1%.

CATEGORIZING FRAUD BY FTC METHODOLOGY

With one exception, this report continues to classify fraud within the three categories originally defined by the FTC in 2003. For 2005 and beyond, debit card fraud has been recategorized as existing card account fraud⁵⁰ instead of existing non-card account fraud.⁵¹ Javelin believes this change reflects a more accurate representation of debit card fraud, because much of its means of compromise, fraudulent use, and detection methods parallel those of credit cards.

The categories of fraud are listed below from least to most serious:

- Existing card account: This category includes both the account numbers and/or the actual card for existing credit and card-linked debit accounts. Prepaid cards were added for 2007 and subsequently removed due to extremely low incidence.
- Existing non-card account: This category includes existing checking and savings accounts, and existing loans, insurance, telephone, and utilities accounts.
- New account and other fraud: This category includes new accounts or loans for committing theft, fraud, or other crimes using the victim's personal information.

Many victims experience identity fraud within more than one of these categories. In reporting the overall incidence rates of the three categories or types of accounts, the victims of crimes to more than one type of account are categorized based on the most serious (as designated by the FTC) problem reported. Thus, victims who reported that new accounts had been opened using their information and also that their existing credit cards had been misused would be placed in the new account and other fraud classification, not in the existing card account classification. This categorization is applicable only for reporting the rates of the three types of fraud.

2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a Treasure Trove for Fraudsters



DEVIATION FROM FTC AND 2003 METHODOLOGY AND REPORTING

When the report cites victims' average financial damages or resolution times in dollars or hours, the entire amount of damages or losses is placed into every type of fraud the victims suffered. For example, for a victim who reports that a total of \$100 is obtained for both new account and other fraud category and existing card account, the \$100 is counted in both categories. This method of reporting costs by types of fraud will not change the overall total costs of fraud across all three categories, but the average in dollars or time associated in the three types of fraud should not be summed because the result will be overlapping amounts.

SURVEY QUESTIONNAIRE

The set of questions and underlying methodology used for this report were identical to or highly similar to those in the 2011, 2010, 2009, 2008, 2007, 2006, 2005, 2004, and 2003 surveys. Some structural adjustments were made in 2011 to adapt CATI-based questions to web-based questions. All changes were made under the purview of experienced methodologists. Therefore, Javelin continues to provide longitudinal trends on various subjects, such as incidence rates and detection methods.

In addition, Javelin added a number of discreet new questions in 2012 to further explore the significance of past responses as well as to identify new trends around emerging technologies. In particular, Javelin sought to gain a better understanding of consumer behaviors regarding organizations contacted after fraud incidence.

MARGIN OF ERROR

The ID fraud report estimates key fraud metrics for the current year using a base of consumers experiencing identity fraud in the past six years.⁵² Other behaviors are reported based on data from all identity fraud victims in the survey (i.e., based on fraud victims experiencing fraud up to six years ago) as well as total respondents, where applicable.

For questions answered by all 5,249 respondents, the maximum margin of sampling error is +/- 1.35 percentage points at the 95% confidence level. For questions answered by all 857 identity fraud victims, the maximum margin of sampling error is +/- 3.35 percentage points at the 95% confidence level.

SPONSORING ORGANIZATIONS

The project was made possible in part by CitiGroup Inc., Intersections LLC and Visa Inc. To preserve the project's independence and objectivity, the sponsors of this project were not involved in the tabulation, analysis, or reporting of final results.



2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a Treasure Trove for Fraudsters

Table of Contents

| | |
|---|----|
| OVERVIEW | 6 |
| INTRODUCTION..... | 7 |
| Executive Summary | 7 |
| Major Findings..... | 7 |
| Recommendations..... | 11 |
| Consumer Recommendations for Prevention, Detection and Resolution™ of Identity Fraud..... | 11 |
| Recommendations for Financial Institutions..... | 13 |
| Recommendations for Merchants | 15 |
| QUICK REFERENCE GUIDE | 17 |
| FRAUD TYPES | 21 |
| New Account Fraud | 21 |
| Compromising Identities | 22 |
| Fraudsters Prefer New Card Accounts | 23 |
| Existing Account Fraud | 24 |
| Existing Card Fraud | 25 |
| Payment Card Data Targeted Through Multiple Vectors | 26 |
| Addressing Fraud Attempts..... | 28 |
| The Effect of EMV..... | 28 |
| Existing Non-Card Fraud | 30 |
| Account Takeover | 32 |
| Accessing Existing Accounts | 33 |
| Accounts Targeted and the Effect on Consumers | 35 |
| Familiar Fraud..... | 37 |
| Despite Changes in Fraud Trends, Familiar Fraud Patterns Remain Constant | 37 |
| Motivation and Opportunity | 38 |
| One-Stop Shopping: Access to PII and the Severity of Familiar Fraud | 39 |
| PREVENTION | 42 |
| Data Breaches: Precursors to Fraud | 42 |
| Online Retail Fraud | 44 |
| Mobile Consumers Are Vulnerable Targets..... | 47 |
| Social Media | 50 |
| Risky Practices on Social Networking | 50 |
| DETECTION..... | 52 |
| Methods of Detection | 52 |
| Means of Detection by Fraud Type | 52 |



2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a Treasure Trove for Fraudsters

Table of Contents

| | |
|--|----|
| Means of Detection Among Existing Debit and Credit Card Fraud Victims..... | 54 |
| Effect of Common Fraud Detection Types on FI Fraud Victim Retention | 55 |
| Length of Fraudulent Activity Before Detection by Detection Methods..... | 56 |
| Detecting Familiar Fraud: Perpetrators Represent Camouflaged Threat..... | 56 |
| RESOLUTION | 58 |
| Fraud Resolution Rates Reach All-Time High..... | 58 |
| Resolution by Fraud Type | 59 |
| Existing Card Fraud Resolution Is Quicker Because the Process Is Streamlined | 60 |
| Existing Non-Card Fraud Resolution..... | 61 |
| New Account Fraud Resolution..... | 62 |
| Account Takeover Fraud Resolution | 63 |
| Severity of Fraud and Resolution Actions..... | 64 |
| Lower-Income Consumers Are More Severely Affected by Fraud | 64 |
| Low-Income Consumers Know the Perpetrators and Take Legal Action | 66 |
| Fraud Severity and Responses to Fraud | 68 |
| Demographic Determinants of Resolution Action..... | 69 |
| Consumer Responses to Fraud Depend on Age | 69 |
| APPENDIX..... | 72 |
| METHODOLOGY | 74 |
| 2012 Survey Data Collection..... | 74 |
| Longitudinal Trending..... | 74 |
| Categorizing Fraud by FTC methodology..... | 75 |
| Deviation From FTC and 2003 Methodology and Reporting | 75 |
| Survey Questionnaire | 76 |
| Margin of Error | 76 |
| Contributing Organizations | 76 |
| GLOSSARY | 77 |
| RELATED RESEARCH | 80 |
| COMPANIES MENTIONED | 82 |



2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a Treasure Trove for Fraudsters

Table of Figures

| | |
|--|----|
| Figure 1: Overall Identity Fraud Incidence Rate and Total Fraud Amount by Year | 7 |
| Figure 2: Breakdown of Identity Crime Types | 17 |
| Figure 3: Overall Measures of the Impact of Identity Fraud, 2004–2012..... | 18 |
| Figure 4: Identity Fraud Overview: Existing Account Fraud..... | 18 |
| Figure 5: Identity Fraud Overview: Existing Card Fraud | 19 |
| Figure 6: Identity Fraud Overview: Existing Non-Card Fraud | 19 |
| Figure 7: Identity Fraud Overview: New Account Fraud | 20 |
| Figure 8: Identity Fraud Overview: Account Takeover Fraud | 20 |
| Figure 9: New Account Fraud Incidence and Total Fraud Amount by Year..... | 21 |
| Figure 10: Types of New Fraudulent Accounts Opened | 23 |
| Figure 11: Existing Account Fraud Incidence and Total Fraud Amount by Year | 24 |
| Figure 12: Existing Card Fraud Incidence and Total Fraud Amount by Year | 25 |
| Figure 13: Type of Existing Card Misused by Age | 26 |
| Figure 14: Type of Personal Information Compromised in a Data Breach | 27 |
| Figure 15: Road Map for EMV Migration And Shifting Liability | 29 |
| Figure 16: Existing Non-Card Fraud Incidence and Total Fraud Amount by Year..... | 30 |
| Figure 17: Consumer Out-of-Pocket Costs As a Percent of Fraud Losses..... | 31 |
| Figure 18: Account Takeover Fraud Incidence and Total Fraud Amount by Year | 32 |
| Figure 19: Information Changed on Accounts Taken Over..... | 33 |
| Figure 20: Recent Use of Security Software | 34 |
| Figure 21: Types of Accounts Taken Over | 35 |
| Figure 22: Type of Card Account Misused Among Account Takeover Victims and All Fraud Victims | 36 |
| Figure 23: Key Fraud Metrics among Familiar Fraud and Non Familiar Fraud Victims..... | 37 |
| Figure 24: Personal Acquaintance With the Perpetrator by Annual Household Income | 38 |
| Figure 25: Severity of Effective Fraud by Familiar Fraud Victims, All Fraud Victims..... | 39 |
| Figure 26: Type of PII Compromised Among Familiar Fraud Victims, All Fraud Victims..... | 40 |
| Figure 27: Fraud Incidence by Data Breach Victims, Non-Data-Breach Victims and All Fraud Victims | 42 |
| Figure 28: Incidence of Fraud Types by Type of Information Breached | 43 |
| Figure 29: Means of Misuse of Fraud Victims' Information 2010–2012 | 44 |
| Figure 30: Online Retail Fraud Incidence vs. POS Fraud Incidence 2005–2012..... | 45 |
| Figure 31: Type of Existing Card Misused for Fraudulent Online vs. In-Person Purchases..... | 46 |
| Figure 32: Mobile Consumers' Perceptions of the Riskiness of Behaviors | 47 |
| Figure 33: How Recently Mobile Consumers Have Downloaded Apps to their Mobile Device | 48 |
| Figure 34: Fraud Incidence by Ownership of Tech Products | 49 |
| Figure 35: Incidence Rate by Social Networking Activity, 2012..... | 51 |



2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a Treasure Trove for Fraudsters

Table of Figures

| | |
|---|----|
| Figure 36: Means of Fraud Detection by Fraud Type | 52 |
| Figure 37: Means of Fraud Detection by Credit and Debit Card Victims | 53 |
| Figure 38: Fraud Victims Who Switched Their FI or Credit Card Provider by Detection Method..... | 54 |
| Figure 39: Mean Detection Time by Fraud Detection Method..... | 55 |
| Figure 40: Detection Times for All Fraud Victims vs. Familiar Fraud Victims | 56 |
| Figure 41: Means of Discovery of Fraud by All Fraud Victims vs. Familiar Fraud Victims | 57 |
| Figure 42: Percent of Fraud Victims Who Have Completely Resolved Their Fraud | 58 |
| Figure 43: Percent of Victims Who Have Resolved Their Fraud by Fraud Type, 2011 and 2012..... | 59 |
| Figure 44: Number of Organizations Contacted for Assistance by Fraud Type | 60 |
| Figure 45: Resolution Time by Fraud Type | 61 |
| Figure 46: Organizations Contacted by Fraud Type..... | 62 |
| Figure 47: Severity of Effect of Fraud by Fraud Type..... | 63 |
| Figure 48: Fraud Amounts and Consumer Costs As a Percent of Annual Household Income | 64 |
| Figure 49: Severity of Effect of Fraud by Annual Household Income | 65 |
| Figure 50: Agencies Contacted by Familiar Fraud Victims and All Fraud Victims | 66 |
| Figure 51: Legal Actions Taken by Familiar Fraud Victims and All Fraud Victims | 67 |
| Figure 52: Responses to Fraud by Fraud Amount and Resolution Hours | 68 |
| Figure 53: Organizations Contacted by Severity of Fraud | 69 |
| Figure 54: Fraud Victims' Responses to Fraud by Age..... | 70 |
| Figure 55: Victims' Actions as a Result of Fraud by Year | 72 |
| Figure 56: Types of Merchants Fraud Victims Avoid | 73 |



**2013 IDENTITY FRAUD REPORT:
Data Breaches Becoming a Treasure Trove for Fraudsters**

EXECUTIVE SUMMARY

The incidence of identity fraud in the U.S. continues to rise, rebounding from a sharp decline between 2009 (6.0%) and 2010 (4.35%), and increasing further from 4.9% in 2011 to 5.26% in 2012. Identity fraud affected 12.6 million consumers in 2012, and at least half did not suffer any out-of-pocket costs (median cost to consumers of \$0) nor did they spend much time resolving these cases (median resolution time of three hours). That is not to say that all cases of fraud have equally limited negative effects — the mean cost to consumers as a result of fraud actually increased from \$354 in 2011 to \$365 in 2012, with the bulk of the fraud costs being borne by financial institutions, merchants, and other businesses. The mean resolution time remains unchanged at 12 hours. On a positive note, consumer information is being misused

for the shortest period of time (48 days), and more of these cases are being resolved (92% resolution rate) than at any time in the past seven years.

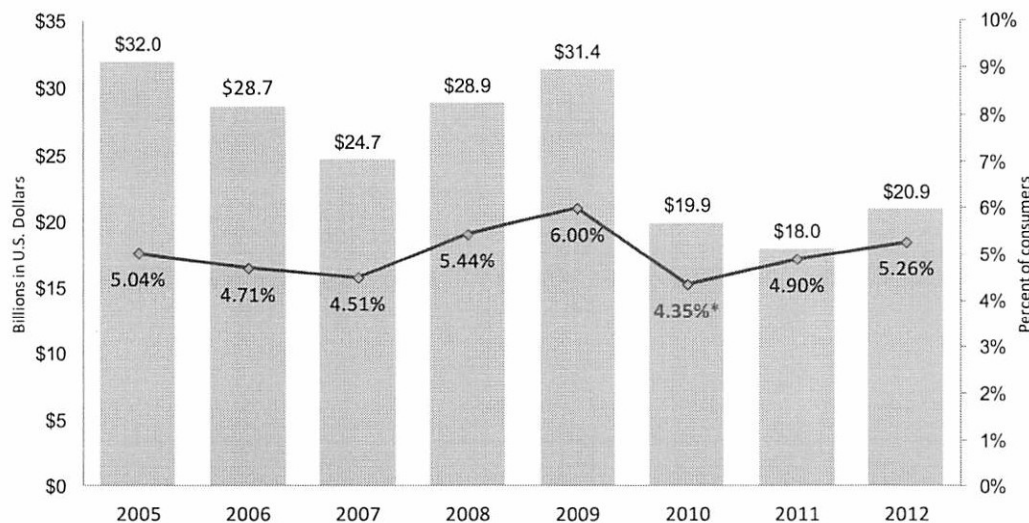
Major Findings

New Account Fraud Increasingly Threatens Consumers and Businesses

Having increased by 50%, from 0.82% of all adults in 2011 to 1.22% in 2012, NAF poses a growing threat to consumer identities and private industry's bottom line — especially as the total fraud loss has doubled from 2011, to \$9.8 billion. Monitoring of credit reports can help detect many of these cases, as 57% of NAF cases involved the establishment of new general-use and store-branded credit cards.

Identity Fraud Rises for Second Consecutive Year, Affecting 5.26% of Consumers and Costing \$20.9 Billion

Figure 1: Overall Identity Fraud Incidence Rate and Total Fraud Amount by Year



*Significance tested against 2012; Blue significantly lower, Red significantly higher.

October 2005 through 2012, n= varies 4,784 - 5,249. Base: All Consumers. © 2013 Javelin Strategy & Research

Strategy & Research, a Associates. All rights by copyright and other

PREVENTION

DATA BREACHES: PRECURSORS TO FRAUD

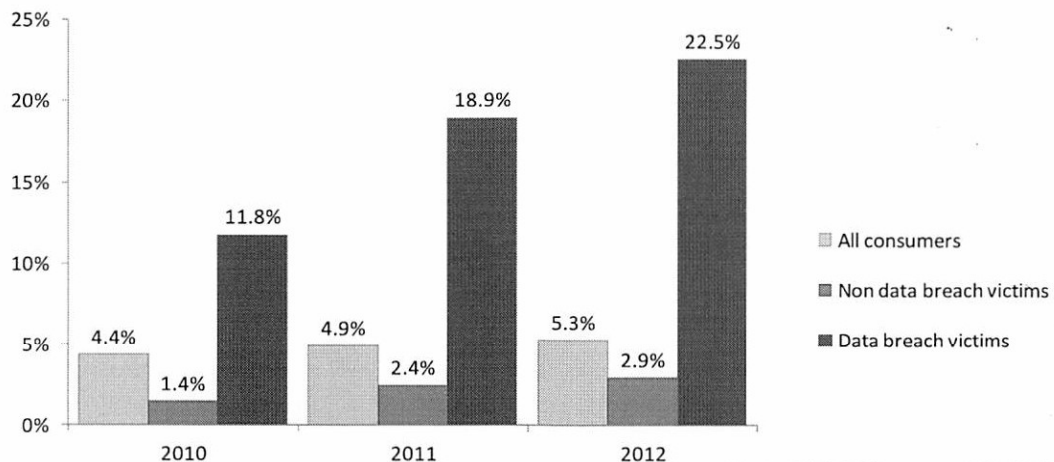
The most essential of tools required to commit identity fraud is the identity itself. In the past, this information was obtained a variety of ways that have included rooting through victims' trash, stealing records from their health care provider's office, or manipulating victims through social engineering. Advancement comes to crime, as it does to most things in which a profit can be made, and data breaches have become the means de rigueur for pilfering voluminous amounts of consumer information with far less risk than previous methods. The type of PII secured during these breaches lend themselves to committing particular types of fraud, and criminals are using the breached information to do just that — breaches beget fraud. Protecting against a breach and responding

properly in its wake are necessary steps in the battle against this insidious criminal practice.

Notifying consumers of a breach has become common practice in an effort to keep consumers informed, and in some instances as necessitated by law. These notifications are generated by the organization that suffered the data breach or by the FI associated with the account information that was breached. In keeping with the trend of the past few years, consumers who were notified that they were victims of a data breach in 2012 were significantly more likely to be victims of fraud than they were in 2011, with a fraud incidence rate of 22.5% (see Figure 27) compared with 5.3% of all consumers.

Increase in Fraud Rate Among Data Breach Victims Outpaces Increase in Overall Fraud Rate

Figure 27: Fraud Incidence by Data Breach Victims, Non-Data-Breach Victims and All Fraud Victims



Q2. In the last 12 months, have you been notified by a business or other institution that your personal or financial information has been lost, stolen or compromised in a data breach?

October 2010 - 2012, n = varies 337 - 5,249
Base: All consumers, data breach victims, non data breach victims.
© 2013 Javelin Strategy & Research

Insights Report Brochure



2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a Treasure Trove for Fraudsters

The number of mobile malware programs is growing at a rapid pace (see Account Takeover section, pg. 32, but consumers have the means to mitigate these threats. The successful malware that takes advantage of weaknesses in mobile device operating systems or other apps can be mitigated by installing the latest software patches and keeping operating systems up to date. Security software, which 64% of smartphone owners have displayed a willingness to use,⁴³ can proactively stop malware from being installed and eliminate any malware already on the device.

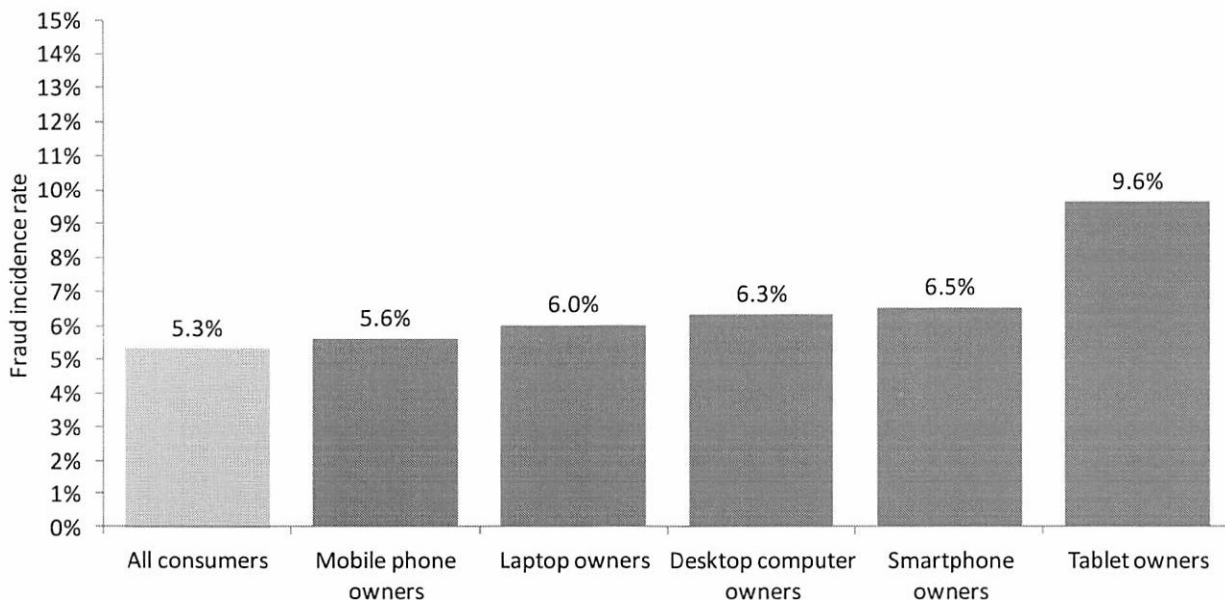
When a mobile network data connection is either unavailable or inconvenient, consumers may choose to use public Wi-Fi hotspots as an alternative, but not all hotspots are created equal in terms of security. While only 40% of mobile consumers consider such activity risky (see Figure 32) public Wi-Fi hotspots can provide

fraudsters with a backdoor to transmissions carrying sensitive consumer data. Airports, hotels, and coffee shops are locations that frequently offer Wi-Fi hotspots as a convenience. Consumers could mistakenly connect to hotspots that appear to be legitimate as they bear names similar to other business in the same location or they have names such as "Free Wi-Fi" but are in fact controlled by fraudsters. Once the consumer's device is connected, any transmitted data is intercepted and may later be misused to commit identity fraud. Such a scenario could be responsible for a fraud incidence rate among public Wi-Fi users that is 45% higher than for those who have not used public hotspots.

Among technology product owners, tablet owners are most likely to suffer from identity fraud compared with all other consumers (see Figure 34), though this is likely a function of multiple factors.

Tablet Owners More Than 80% More Likely Than All Other Consumers to Become Fraud Victims

Figure 34: Fraud Incidence by Ownership of Tech Products



Q39A: Please indicate which of the following products do you personally own and use. Q5: How long ago did you DISCOVER that your personal or financial information had been misused?

October 2012, n = varies 1,062 to 5,249.
Base: All consumers, owners of various products.
© 2013 Javelin Strategy & Research

**2013 IDENTITY FRAUD REPORT:
Data Breaches Becoming a Treasure Trove for Fraudsters**



| Companies Mentioned | |
|---------------------|-------------|
| Amazon | MasterCard |
| American Express | McAfee |
| Apple | Microsoft |
| Discover | PayPal |
| EBay | Target |
| Europay | Trend Micro |
| Facebook | Visa |
| Global Payments | Wal-Mart |
| Google | Zappo's |
| Macy's | |

Insights Report Brochure

**2013 IDENTITY FRAUD REPORT:
Data Breaches Becoming a Treasure Trove for Fraudsters**



Place Your Order as Follows:

- 1) Call us at (925) 219-0116
- 2) Email us at marketing@javelinstrategy.com
- 3) Fax or Mail using the form below:

| Report Title | Publication Date | Price |
|--------------|------------------|-------|
| | | |
| | | |
| | | |
| | | |
| | | |

Name: _____ Title: _____

Organization: _____ Division or group: _____

Email: _____ Phone: _____ Fax: _____

Address: _____

Signature to confirm your order: _____

Payment Method: Payment card Check Enclosed Invoice me

Visa, MC, AE or Disc. card #: _____ Exp date: ___/___

Name on Card: _____ Signature: _____

Note: Reports are provided in electronic PDF form only. Javelin reports are subject to standard terms and conditions, as described on our web site. Javelin will contact you in the future to provide our free research newsletter or other mailings. If you do not wish to receive our newsletter or other mailings, you may advise us of this. Your contact information will not be sold to other organizations.

EXHIBIT D

FOX BUSINESS

Someone Became an Identity Theft Victim Every 2 Seconds Last Year

By [Kate Rogers](#) | Published February 05, 2014 | [FOXBusiness](#)

Data breaches have been dominating headlines recently--and with good reason.

A new identity fraud victim was hit every two seconds in America in 2013, with the number of victims climbing to 13.1 million over the year, according to Javelin Strategy & Research's 2014 Identity Fraud Study. This is an uptick of more than 500,000 victims in 2012.

Just this week, the fallout of the breaches at both Target (NYSE:TGT) and Neiman Marcus continued to unravel with corporate officials testifying on Capitol Hill and how many stores were hit.

Javelin's report has been conducted for the past 11 years, and this report draws on responses from 5,634 consumers to identify the impacts of fraud nationwide.



Sponsored By [Spectrumreach.com](#)

Sponsored Video

Watch to learn more

While the number of victims increased year over year, the amount of defrauded money decreased by \$3 billion to \$18 billion compared to 2012. Al Pascual of Javelin Strategy & Research, points to advancements in the financial industry that has made it better at detecting new instances of fraud is behind the drop in compromised funds as criminals have a harder time creating new fraudulent accounts.

“In 2012, we had a big spike in new fraud with a high average fraud amount,” he says. “But in 2013, that was pushed down with criminals shifting into existing card fraud.”

This shift means we will see more breaches like those that hit Target and Neiman, he adds. And as individuals continue migrating their financial lives online, identity thieves and scammers will focus more attention targeting online banks and payment sites like Paypal.

“They will go where the money is. The behavior we exhibit using passwords is exacerbating the issue as well.”

The more passwords a consumer has for different online accounts, the less likely they are to change them, he says, which is good news for scammers. Consumers with less than 10 online accounts usually use different passwords for each account. But when the amount of online accounts climbs higher to 20, the survey shows people are more likely to use the same password for multiple accounts.

“This is driving a lot of fraud diversification,” he says. The study finds fraudsters are increasingly turning to eBay (NASDAQ:EBAY), Amazon (NASDAQ:AMZN) and Paypal with stolen information to make purchases.

One in every three people who is notified of being a potential fraud victim becomes one, Javelin reports, with 46% of consumers who had cards breached becoming fraud victims that same year. This is up from one in four in 2012.

Account takeovers to commit fraud have hit a record in incidence, with 28% of fraud losses.

While it's clear identity scams and data breaches are on the rise, the financial industry is scrambling to figure out how to better protect consumers.

There's been much talk of bringing chip-based, or EMV cards to the U.S., but little action from major banks and retailers, likely because of the cost associated with installing terminals to read the cards.

Pascual says change is clearly necessary, and expects a major shift over the next five years.

“Consumers pay the bill—we suffer the fraud, pay increased costs. But we still need to depend on businesses to make the changes for us,” he says. “The checkout counter is really a crap shoot, it's become Russian roulette. You have no idea if that retailer has been breached.”

More cooperation between the financial industry and retailers will be necessary to spark change.

“They are really antagonistic toward one another and I don’t expect them to be holding hands and singing ‘Kumbaya’ anytime soon,” Pascual says. “We need time. And pressure from Capitol Hill.”

URL

<https://www.foxbusiness.com/features/someone-became-an-identity-theft-victim-every-2-seconds-last-year>

Quotes delayed at least 15 minutes. Real-time quotes provided by [BATS BZX Real-Time Price](#). Market Data provided by Interactive Data ([Terms & Conditions](#)). Powered and Implemented by [Interactive Data Managed Solutions](#). Company fundamental data provided by [Morningstar](#). Earnings estimates data provided by Zacks. Mutual fund and ETF data provided by [Lipper](#). Economic data provided by Econoday. Dow Jones & Company Terms & Conditions.
This material may not be published, broadcast, rewritten, or redistributed. ©2019 FOX News Network, LLC. All rights reserved. [FAQ](#) - [Updated Privacy Policy](#)

EXHIBIT E



December 2013, NCJ 243779

Victims of Identity Theft, 2012

Erika Harrell, Ph.D. and Lynn Langton, Ph.D., *BJS Statisticians*

Approximately 16.6 million persons or 7% of all U.S. residents age 16 or older, were victims of one or more incidents of identity theft on 2012 (**figure 1**). Among identity theft victims, existing bank (37%) or credit card accounts (40%) were the most common types of misused information.

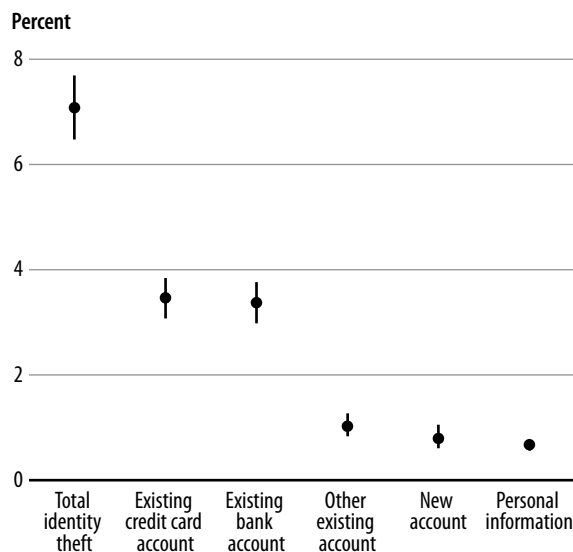
This report uses data from the 2012 Identity Theft Supplement (ITS) to the National Crime Victimization Survey (NCVS). From January to June 2012, the ITS collected data from persons who experienced one or more attempted or successful incidents of identity theft during the 12 months preceding their interview.

Identity theft victims are defined as persons age 16 or older who experienced one or more of the following incidents:

- unauthorized use or attempted use of an existing account, such as a credit or debit card, checking, savings, telephone, online, or insurance account (referred to as fraud or misuse of an existing account).

FIGURE 1

Persons age 16 or older who experienced at least one identity theft incident during the past 12 months, by type of theft, 2012



Note: See table 1 for estimates and appendix table 1 for standard errors. Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

Bulletin

Highlights

The purpose of this report is to describe the prevalence of identity theft, its victims, and the characteristics and effects of this crime. The 2012 Identity Theft Supplement (ITS) of the National Crime Victimization Survey (NCVS) provided the data for this report.

- About 7% of persons age 16 or older were victims of identity theft in 2012.
- The majority of identity theft incidents (85%) involved the fraudulent use of existing account information, such as credit card or bank account information.
- Victims who had personal information used to open a new account or for other fraudulent purposes were more likely than victims of existing account fraud to experience financial, credit, and relationship problems and severe emotional distress.
- About 14% of identity theft victims experienced out-of-pocket losses of \$1 or more. Of these victims, about half suffered losses of less than \$100.
- Over half of identity theft victims who were able to resolve any associated problems did so in a day or less; among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems.
- About 36% of identity theft victims reported moderate or severe emotional distress as a result of the incident.
- Direct and indirect losses from identity theft totaled \$24.7 billion in 2012.

BJS

- unauthorized use or attempted use of personal information to open a new account, such as a credit or debit card, telephone, checking, savings, loan, or mortgage account (referred to as fraud or misuse of a new account).
- misuse of personal information for a fraudulent purpose, such as getting medical care, a job, or government benefits; renting an apartment or house; or providing false information to law enforcement when charged with a crime or traffic violation (referred to as fraud or misuse of personal information).

This report details the number, percentage, and demographic characteristics of victims who reported one or more incidents of identity theft during a 12-month period. It focuses on the most recent incident experienced to describe victim characteristics and victim responses to identity theft. It describes how the victim discovered the crime; financial losses and other consequences of identity theft, including the amount of time victims spent resolving associated problems; reporting of the incident to credit card companies, credit bureaus, and law enforcement agencies; and the level of distress identity theft victims experienced.

For 85% of identity theft victims, the most recent incident involved the unauthorized use of an existing account

In 2012, the unauthorized misuse or attempted misuse of an existing account was the most common type of identity theft, experienced by 15.3 million persons age 16 or older (6% of

all persons) (table 1). The majority of victims experienced the fraudulent use of their credit cards (7.7 million or 3% of all persons) or bank accounts (7.5 million or 3% of all persons). Another 1.7 million victims (0.7% of all persons) experienced other types of existing account theft, such as misuse or attempted misuse of an existing telephone, online, or insurance account.

An estimated 1.1 million victims (less than 1% of all persons) reported the fraudulent misuse of their information to open a new account, such as a credit card. Another 833,600 victims reported the misuse of their personal information for other fraudulent purposes.

In 2012, 22% of victims experienced multiple incidents of identity theft, while 77% experienced a single incident (not shown).¹ During the single or most recent identity theft incident experienced in 2012, 8% or 1.2 million victims experienced multiple types of identity theft during a single incident. For 66% of victims of multiple types of identity theft, the incident involved the unauthorized use of a combination of existing accounts, such as credit card, checking, savings, telephone, or online accounts. The remaining 34% who experienced multiple types of identity theft during a single incident (less than 3% of all victims) reported some combination of misuse of an existing account, misuse of personal information to open a new account, and personal information used for other fraudulent purposes.

¹About 1% of victims did not know whether they experienced one or more than one incident.

TABLE 1

Persons age 16 or older who experienced at least one identity theft incident in the past 12 months, by type of theft, 2012

| Type of identity theft | Anytime during the past 12 months ^a | | Most recent incident ^b | | |
|-------------------------------|--|------------------------|-----------------------------------|------------------------|------------------------|
| | Number of victims | Percent of all persons | Number of victims | Percent of all persons | Percent of all victims |
| Total | 16,580,500 | 6.7% | 16,580,500 | 6.7% | 100% |
| Existing account | 15,323,500 | 6.2% | 14,022,100 | 5.7% | 84.6% |
| Credit card | 7,698,500 | 3.1 | 6,676,300 | 2.7 | 40.3 |
| Bank | 7,470,700 | 3.0 | 6,191,500 | 2.5 | 37.3 |
| Other | 1,696,400 | 0.7 | 1,154,300 | 0.5 | 7.0 |
| New account | 1,125,100 | 0.5% | 683,400 | 0.3% | 4.1% |
| Personal information | 833,600 | 0.3% | 622,900 | 0.3% | 3.8% |
| Multiple types | ~ | ~ | 1,252,000 | 0.5% | 7.6% |
| Existing account ^b | ~ | ~ | 824,700 | 0.3 | 5.0 |
| Other ^c | ~ | ~ | 427,400 | 0.2 | 2.6 |

Note: Detail may not sum to total due to victims who reported multiple incidents of identity theft and rounding. See appendix table 1 for standard errors.

~Not applicable.

^aIdentity theft classified as a single type.

^bIncludes victims who experienced two or more of the following: unauthorized use of a credit card, bank account, or other existing account.

^cIncludes victims who experienced two or more of the following: unauthorized use of an existing account, misuse of personal information to open a new account, or misuse of personal information for other fraudulent purposes.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

Persons in households with higher annual incomes were more likely to experience identity theft than persons in lower-income households

A similar percentage of males and females (7%) experienced identity theft in 2012 (table 2). Across all types of identity theft, prevalence rates did not vary significantly by sex. After accounting for whether a person owned a credit card and bank account, prevalence rates for existing credit card and existing banking account misuse did not vary by sex.

Persons ages 16 to 17 (less than 1%) were the least likely to experience identity theft, followed by persons ages 18 to 24 (5%) and 65 or older (5%). After accounting for credit card ownership, persons ages 16 to 24 were the least likely to experience the misuse of an existing account, while persons age 65 or older had a similar prevalence rate as persons ages 25 to 34. Among those who had a bank account, persons ages 16 to 17 and 65 or older were the least likely to experience banking account fraud.

A greater percentage of white non-Hispanics (7%) experienced identity theft in 2012 than black non-Hispanics (5%) and Hispanics (5%). This relationship also held true for the misuse of an existing credit card account among persons who had a credit card. However, among persons who had a bank account, there were no significant differences in the prevalence of bank account misuse among whites, blacks, and Hispanics.

Overall, persons in the highest income category (those with an annual household income of \$75,000 or more) had a higher prevalence of identity theft than persons in other income brackets. After accounting for credit card ownership, persons in the highest income bracket had the highest rate of existing credit card account misuse. Among persons who had a bank account, there were no significant differences in the prevalence of identity theft across income categories, with the exception of the unknown category.

TABLE 2
Persons age 16 or older who experienced at least one identity theft incident during the past 12 months, by victim characteristics, 2012

| Characteristic | Any identity theft | | Misuse of existing credit card | | | Misuse of existing bank account | | | New account or personal information ^a | |
|--------------------------------|--------------------|------------------------|--------------------------------|------------------------|-------------------------------------|---------------------------------|------------------------|--------------------------------------|--|------------------------|
| | Number of victims | Percent of all persons | Number of victims | Percent of all persons | Percent of persons with credit card | Number of victims | Percent of all persons | Percent of persons with bank account | Number of victims | Percent of all persons |
| Total | 16,580,500 | 6.7% | 7,698,500 | 3.1% | 4.5% | 7,470,700 | 3.0% | 3.5% | 1,864,100 | 0.8% |
| Sex | | | | | | | | | | |
| Male | 7,902,800 | 6.6% | 3,932,000 | 3.3% | 4.8% | 3,320,100 | 2.8% | 3.3% | 851,200 | 0.7% |
| Female | 8,677,700 | 6.9 | 3,766,400 | 3.0 | 4.3 | 4,150,600 | 3.3 | 3.8 | 1,012,900 | 0.8 |
| Age | | | | | | | | | | |
| 16-17 | 35,200! | 0.4%! | 4,300! | 0.1%! | 0.7%! | 16,300! | 0.2%! | 0.6%! | 5,800! | 0.1%! |
| 18-24 | 1,466,400 | 4.8 | 331,400 | 1.1 | 2.6 | 937,400 | 3.1 | 4.1 | 182,400 | 0.6 |
| 25-34 | 3,293,500 | 7.8 | 1,177,500 | 2.8 | 4.1 | 1,718,100 | 4.1 | 4.7 | 406,700 | 1.0 |
| 35-49 | 4,914,800 | 8.0 | 2,222,100 | 3.6 | 4.8 | 2,344,600 | 3.8 | 4.3 | 531,900 | 0.9 |
| 50-64 | 4,739,400 | 7.8 | 2,590,400 | 4.2 | 5.4 | 1,853,300 | 3.0 | 3.3 | 501,500 | 0.8 |
| 65 or older | 2,131,100 | 5.0 | 1,372,800 | 3.2 | 4.1 | 601,100 | 1.4 | 1.6 | 235,800 | 0.6 |
| Race/Hispanic origin | | | | | | | | | | |
| White ^b | 12,417,600 | 7.3% | 6,258,500 | 3.7% | 4.9% | 5,295,000 | 3.1% | 3.4% | 1,146,400 | 0.7% |
| Black ^b | 1,494,100 | 5.0 | 301,400 | 1.0 | 2.1 | 896,300 | 3.0 | 4.2 | 361,500 | 1.2 |
| Hispanic/Latino | 1,544,100 | 5.2 | 509,100 | 1.7 | 3.1 | 834,300 | 2.8 | 3.8 | 254,000 | 0.8 |
| Other race ^{b,c} | 841,400 | 6.4 | 523,900 | 4.0 | 5.4 | 302,700 | 2.3 | 2.7 | 54,000 | 0.4 |
| Two or more races ^b | 270,700 | 9.0 | 102,000 | 3.4 | 5.9 | 133,400 | 4.4 | 5.3 | 48,200 | 1.6 |
| Household income | | | | | | | | | | |
| \$24,999 or less | 1,888,000 | 4.9% | 413,200 | 1.1% | 2.6% | 1,068,800 | 2.8% | 3.9% | 419,400 | 1.1% |
| \$25,000-\$49,999 | 2,809,100 | 5.4 | 1,026,100 | 2.0 | 3.0 | 1,490,200 | 2.9 | 3.4 | 443,500 | 0.9 |
| \$50,000-\$74,999 | 2,598,500 | 7.7 | 1,084,600 | 3.2 | 4.1 | 1,305,800 | 3.8 | 4.2 | 259,000 | 0.8 |
| \$75,000 or more | 6,274,800 | 10.0 | 3,668,900 | 5.9 | 6.8 | 2,389,800 | 3.8 | 4.0 | 426,100 | 0.7 |
| Unknown | 3,010,100 | 5.1 | 1,505,700 | 2.6 | 3.7 | 1,216,200 | 2.1 | 2.4 | 316,100 | 0.5 |

Note: Estimates are based on the most recent identity theft incident. Includes successful and attempted identity theft in which the victim experienced no loss. See appendix table 2 for standard errors.

! Interpret with caution; estimate is based on 10 or fewer sample cases or coefficient of variation is greater than 50%.

^aIncludes the misuse of personal information to open a new account or to commit other fraud.

^bExcludes persons of Hispanic or Latino origin.

^cIncludes persons identifying as American Indian, Alaska Native, Asian, Hawaiian, or other Pacific Islander.

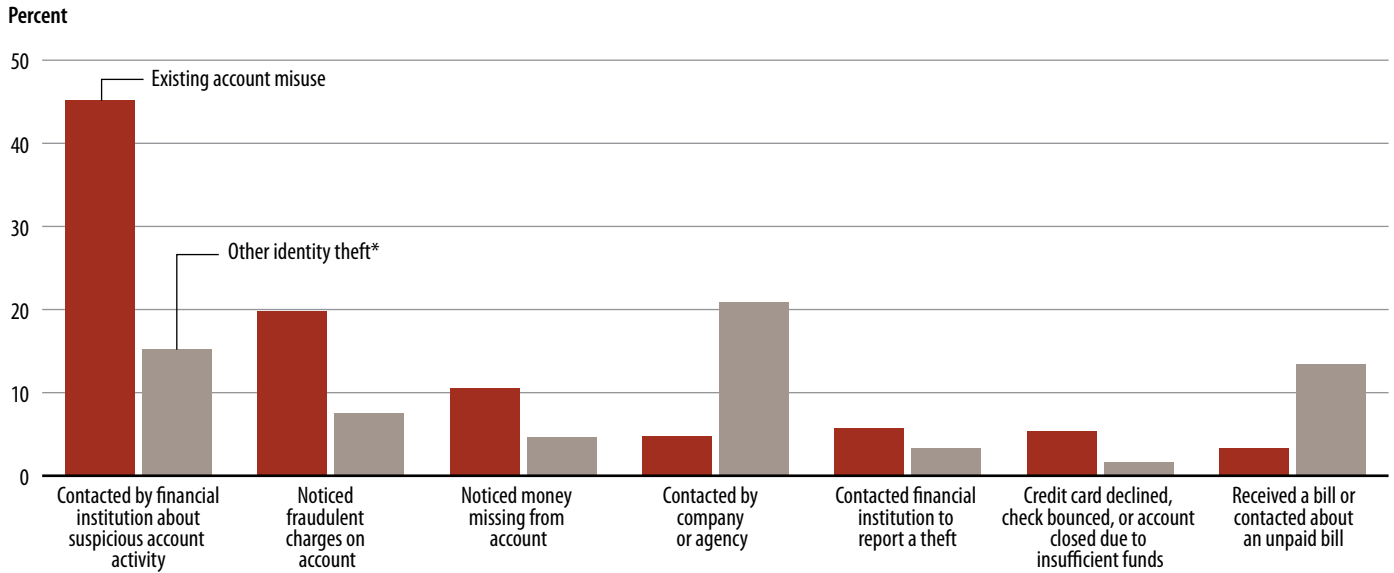
Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

The most common way victims discovered the identity theft was from contact by a financial institution about a problem

The way victims discovered that their identifying information was misused varied by the type of identity theft. Among victims who experienced the unauthorized use of an existing account, 45% discovered the identity theft when a financial institution contacted them about suspicious activity on their account (figure 2). In comparison, 15% of victims who

experienced the misuse of personal information to open a new account or for other fraudulent purposes discovered the incident when a financial institution contacted them. Victims of these other types of identity theft were more likely than victims of existing account misuse to discover the incident when another type of company or agency contacted them (21%) or after they received an unpaid bill (13%). Twenty percent of victims of existing account misuse discovered the incident because of fraudulent charges on their account, compared to 8% of victims of other types of identity theft.

FIGURE 2
Most common ways victims discovered identity theft, by type of theft, 2012



Note: Estimates are based on the most recent incident of identity theft. See appendix table 3 for estimates and standard errors for all ways that victims discovered the identity theft.

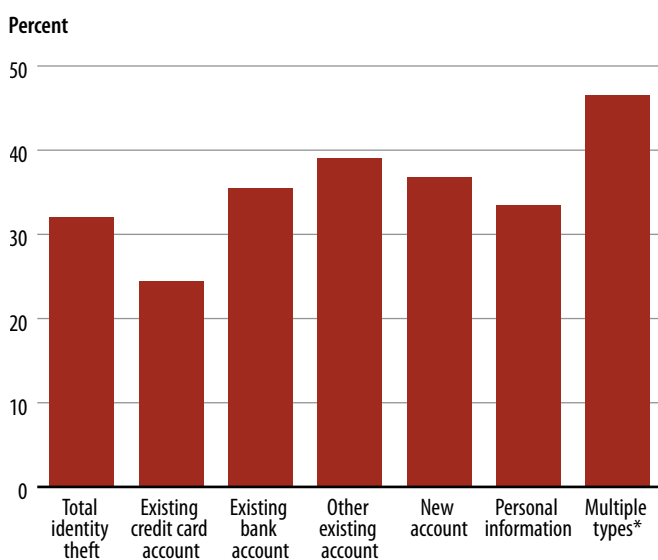
*Includes identity theft incidents involving the misuse of personal information to open a new account or for other fraudulent purposes.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

The majority of identity theft victims did not know how the offender obtained their information

About 32% of identity theft victims knew how the offender obtained their information (figure 3). Victims who experienced multiple types of identity theft during a single incident (47%) were among the most likely victims to know how the offender obtained the information. Victims who had an existing credit card account misused (24%) were among the least likely to know how the offender obtained the account information. Of the 5.3 million victims who knew how the identity theft occurred, the most common way offenders obtained information (43%) was to steal it during a purchase or other transaction (not shown).

FIGURE 3
Identity theft victims who knew how their personal information was obtained, by type of theft, 2012



Note: Estimates are based on the most recent incident of identity theft. See appendix table 4 for estimates and standard errors.

*Includes victims who experienced more than one type of identity theft in a single incident.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

9 in 10 identity theft victims did not know anything about the offender

Overall, most identity theft victims (91%) in 2012 did not know anything about the identity of the offender (table 3). However, the percentage of victims who knew something about offender varied depending on the type of identity theft. Victims who had personal information used to open a new account (25%) or for other fraudulent purposes (23%) were more likely than victims of existing account misuse (7%) to know something about the offender. Across all types of identity theft, victims who experienced the misuse of an existing credit card (3%) were the least likely to know something about the offender.

TABLE 3
Identity theft victims who knew something about the offender, by type of theft, 2012

| Type of identity theft | Victim knew something about the offender |
|-------------------------------|--|
| Total | 8.6% |
| Existing account | 6.6 |
| Credit card | 2.7 |
| Bank | 9.2 |
| Other | 15.9 |
| New account | 24.6 |
| Personal information | 22.9 |
| Multiple types | 15.1 |
| Existing account ^a | 11.0 |
| Other ^b | 23.1 |

Note: Estimates are based on the most recent incident of identity theft. See appendix table 5 for standard errors.

^aIncludes victims who experienced two or more of the following: unauthorized use of a credit card, bank account, or other existing account.

^bIncludes victims who experienced two or more of the following: unauthorized use of an existing account, misuse of personal information to open a new account, or misuse of personal information for other fraudulent purposes.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

Two-thirds of identity theft victims reported a direct financial loss

The economic impact of identity theft is comprised of direct and indirect financial loss. Direct financial loss, the majority of the total loss associated with identity theft, refers to the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. Indirect loss includes any other costs caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses (e.g., postage, phone calls, or notary fees). Direct and indirect losses do not necessarily reflect personal losses to victims, as victims may be reimbursed for some or all of the direct and indirect losses.

In 2012, 68% of identity theft victims reported a combined direct and indirect financial loss associated with the most recent incident (appendix table 8). Overall, victims who experienced a direct and indirect financial loss of at least \$1 lost an average of \$1,769 with a median loss of \$300.

The amount of financial loss varied by the type of identity theft. Approximately 69% of credit card fraud, 74% of bank fraud, 46% of new account fraud, and 38% of personal information fraud victims experienced a financial loss during the past 12 months. Of those victims who experienced multiple types of identity theft, 69% reported a financial loss.

In 2012, 66% of the 16.6 million victims of identity theft reported a direct financial loss as a result of the identity theft incident. About 68% of credit card fraud victims, 74% of bank fraud victims, 42% of new account fraud victims, and 32% of personal information fraud victims reported that the offender obtained money, goods, or services. Of those victims who experienced multiple types of identity theft, 67% reported a direct financial loss associated with the incident.

Of those who reported a direct financial loss, victims who experienced the misuse of their personal information reported a mean direct loss of \$9,650 and a median direct loss of \$1,900. Victims of new account fraud incurred an average loss per incident of \$7,135 and a median loss of \$600. Victims of multiple types of fraud reported an average direct loss of \$2,140 with a median direct loss of \$400, while victims of existing account misuse had an average loss of \$1,003 per incident with a median direct loss of \$200.

In addition to any direct financial loss, 6% of all identity theft victims reported indirect losses associated with the most recent incident of identity theft. Victims who suffered an indirect loss of at least \$1 reported an average indirect loss of \$4,168, with a median of \$30. With the exception of victims of personal information fraud, identity theft victims who reported indirect financial loss had a median indirect loss of \$100 or less.

Direct and indirect identity theft losses totaled \$24.7 billion in 2012

Identity theft victims reported a total of \$24.7 billion in direct and indirect losses attributed to all incidents of identity theft experienced in 2012 (table 4).² These losses exceeded the \$14 billion victims lost from all other property crimes (burglary, motor vehicle theft, and theft) measured by the National Crime Victimization Survey in 2012. Identity theft losses were over 4 times greater than losses due to stolen money and property in burglaries (\$5.2 billion) and theft (\$5.7 billion), and eight times the total losses associated with motor vehicle theft (\$3.1 billion).

²For victims who experienced multiple incidents of identity theft, the total includes losses from all incidents experienced during the past 12 months.

TABLE 4
Mean, median, and total losses attributed to identity theft and property crime, 2012

| | Mean | Median | Total (in thousands) |
|-----------------------------|---------|--------|----------------------|
| Identity theft ^a | \$2,183 | \$300 | \$24,696,300 |
| Property crime ^b | \$915 | \$150 | \$13,991,700 |
| Burglary | 2,378 | 600 | 5,234,800 |
| Motor vehicle theft | 7,963 | 4,000 | 3,079,900 |
| Theft | 447 | 100 | 5,677,000 |

Note: See appendix table 6 for standard errors.

^aBased on 11.3 million persons 16 or older who experienced one or more incidents of identity theft with known losses of \$1 or more.

^bBased on 15.3 million household property crimes, 2.2 million burglaries, 400,000 motor vehicle thefts, and 12.7 million household thefts with known losses of \$1 or more. In 2012, 19% of completed burglaries had unknown loss amounts.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, 2012, and National Crime Victimization Survey, Identity Theft Supplement, 2012.

In 2012, 14% of identity theft victims suffered an out-of-pocket financial loss

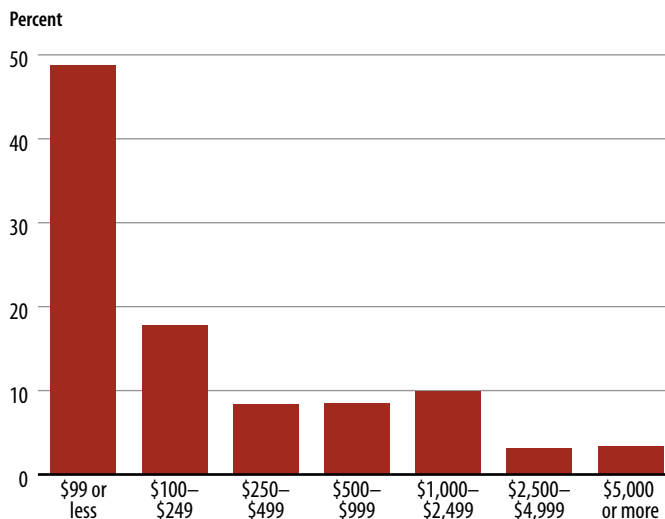
In some instances, a company (e.g., credit card or insurance company) may reimburse some or all of the financial loss, reducing or eliminating the out-of-pocket losses for victims. At the time of the interview, 14% of victims of identity theft had experienced personal out-of-pocket financial losses of \$1 or more. Of these victims who suffered an out-of-pocket financial loss, 49% had total losses of \$99 or less (figure 4). About 18% of victims reported out-of-pocket expenses of \$100 to \$249. An additional 16% of identity theft victims reported that out-of-pocket expenses of \$1,000 or more.

Victims of identity theft who experienced existing account misuse were the least likely to have credit-related problems

In addition to suffering monetary losses, some identity theft victims experienced other financial and legal problems. They paid higher interest rates on credit cards, they were turned down for loans or other credit, their utilities were turned off, or they were the subject of criminal proceedings. Victims who experienced the misuse of an existing account were generally less likely to experience financial and legal problems as a result of the incident than victims who had other personal information misused. In 2012, 2% of victims of existing account misuse experienced problems with debt collectors, compared to 17% of victims who had personal information misused (figure 5). Two percent of victims of existing account misuse experienced

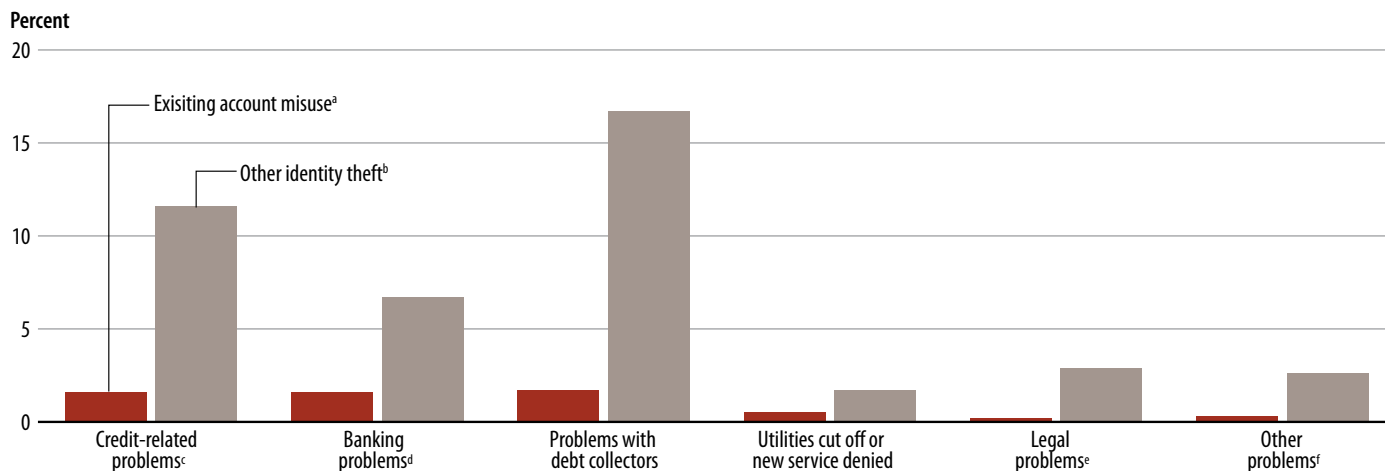
credit-related problems (e.g., higher interest rates or repeatedly having to correct information on a credit report), compared to 12% of victims of other types of identity theft. Less than 1% of victims of existing account misuse and 3% of victims of other types of identity theft had utilities cut off or service denied, legal problems (e.g., being arrested), or other problems (e.g., income tax issues).

FIGURE 4
Total out-of-pocket loss for identity theft victims experiencing a loss of \$1 or more, 2012



Note: Financial loss is computed from the 14% of identity theft victims who experienced a personal loss of at least \$1. Estimates are based on the most recent incident of identity theft. See appendix table 7 for estimates and standard errors. Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

FIGURE 5
Victims who experienced financial or legal problems as a result identity theft, by type of theft, 2012



Note: Estimates are based on the most recent identity theft incident. See appendix table 10 for estimates and standard errors.

^aIncludes victims who experienced multiple types of existing account misuse.

^bIncludes identity theft incidents involving the misuse of personal information to open a new account or for other fraudulent purposes.

^cIncludes problems such as having to correct the same information on a credit report repeatedly, being turned down for credit or loans, or paying higher interest rates.

^dIncludes problems such as being turned down for a checking account or having checks bounce.

^eIncludes being the subject of a lawsuit or other criminal proceedings, or being arrested.

^fIncludes problems such as being turned down for a job, losing a job, or problems with income taxes.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

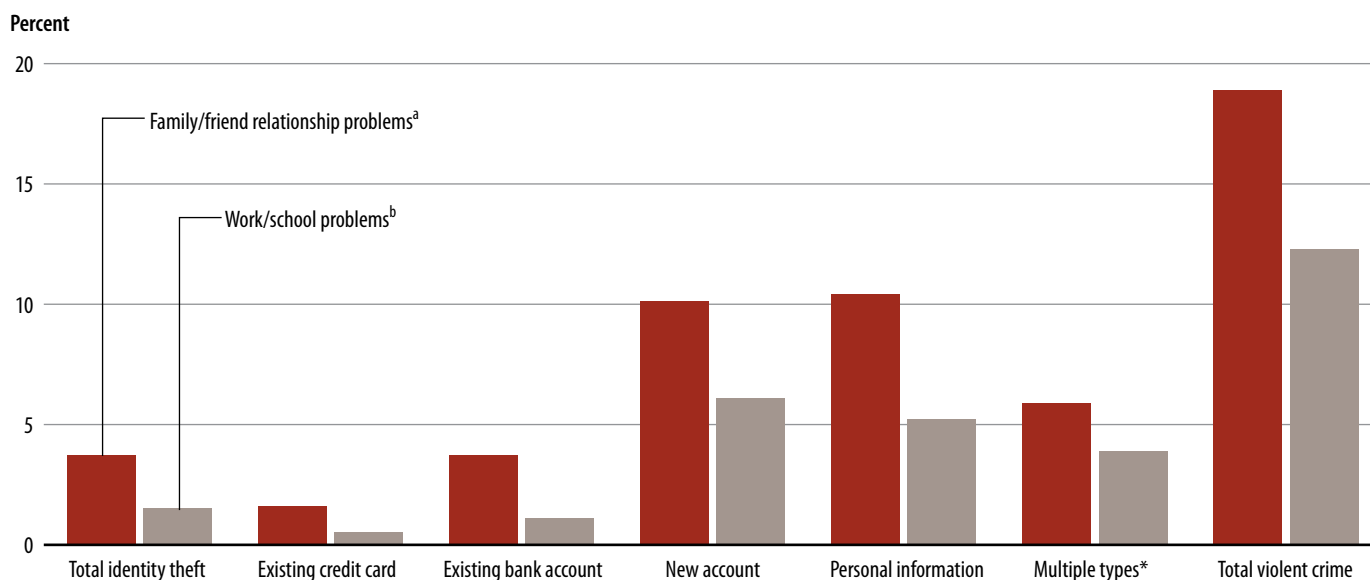
Identity theft victims were less likely than violent crime victims to have significant school, work, or relationship problems as a result of the crime

The 2012 NCVS asked victims of violent crime (including rape or sexual assault, robbery, aggravated assault, and simple assault) about the impact of the victimization on work, school, and personal relationships, and the amount of emotional distress it caused. Compared to violent crime victims surveyed in 2012, a lower percentage of identity theft victims reported significant problems at work or school or with family members or friends due to the incident (figure 6). About 1% of identity theft victims reported significant problems at work or school, compared to 12% of violent crime victims. Similarly, 4% of

identity theft victims reported significant problems with family members or friends, compared to 19% of violent crime victims.

The percentage of identity theft victims who reported significant problems at work or school as a result of the incident varied by type of identity theft. About 6% of victims who had personal information used to open a new account reported significant problems at work or school, compared to about 1% of victims of existing credit card and bank account misuse (appendix table 11). The largest percentage of identity theft victims who had significant problems with family or friends had their personal information used to create new accounts (10%) or for other fraudulent purposes (10%).

FIGURE 6
Victims of identity theft and violent crime who experienced problems as a result of the victimization, 2012



Note: Estimates are based on the most recent incident of identity theft. Victims reported their perceptions of whether the victimization led to significant problems and problems at work or school with family and friends. Total violent crime includes rape/sexual assault, robbery, aggravated assault, and simple assault. Includes violent crime victims (14%) with missing information on relationship, work, and school problems due to crime. See appendix table 11 for estimates and appendix table 12 for standard errors.

*Includes victims who experienced more than one type of identity theft in a single incident.

^aIncludes victims reporting significant problems with family members or friends, including getting into more arguments or fights than before, not feeling able to trust them as much, or not feeling as close to them as before the crime.

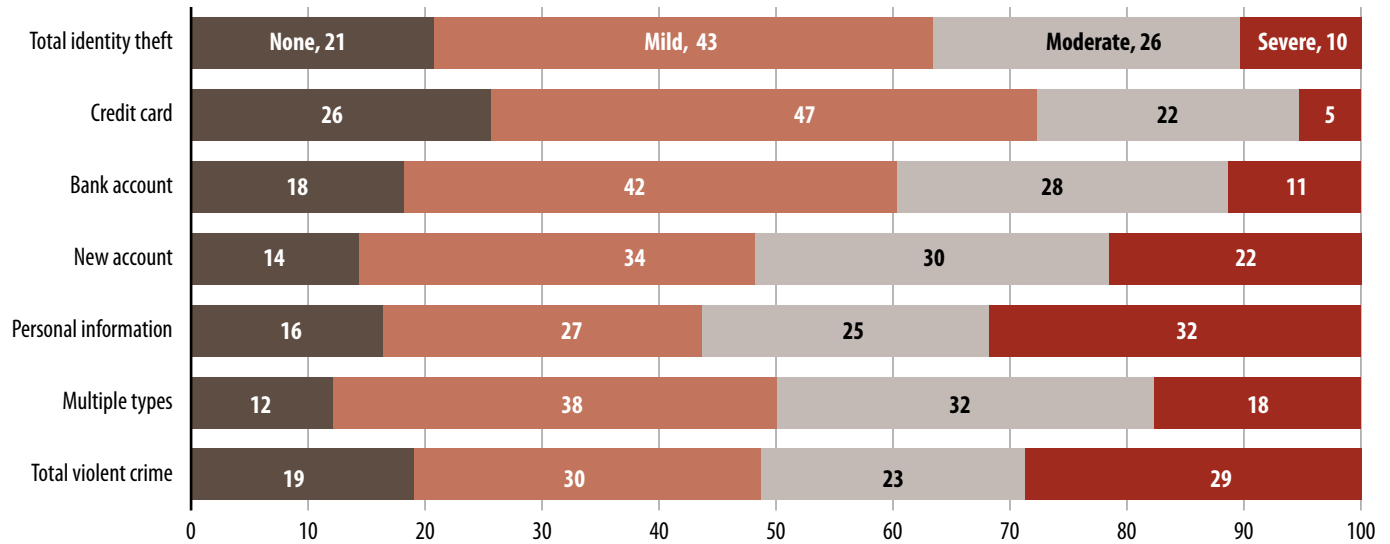
^bIncludes victims reporting significant problems with job or school, such as trouble with boss, coworker, or peers.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, 2012, and National Crime Victimization Survey, Identity Theft Supplement, 2012.

Identity theft victims (10%) were also less likely than violent crime victims (29%) to report that the victimization was severely distressing (figure 7). However, the level of emotional distress varied by type of identity theft. Thirty-two percent of

victims of personal information fraud reported that they found the incident severely distressing, compared to 5% of credit card fraud victims. Twenty-two percent of victims of new account fraud reported that the crime was severely distressing.

FIGURE 7
Level of emotional distress reported by identity theft and violent crime victims, 2012



Note: Estimates are based on the most recent incident of identity theft. Victims reported whether they found the victimization to be not at all distressing, mildly distressing, moderately distressing, or severely distressing. Detail may not sum to total due to rounding. Excludes identity theft victims (less than 1%) and violent crime victims (15%) with missing data on emotional distress. See appendix table 11 for estimates and appendix table 12 for standard errors.

*Includes victims who experienced more than one type of identity theft in a single incident.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, 2012, and National Crime Victimization Survey, Identity Theft Supplement, 2012.

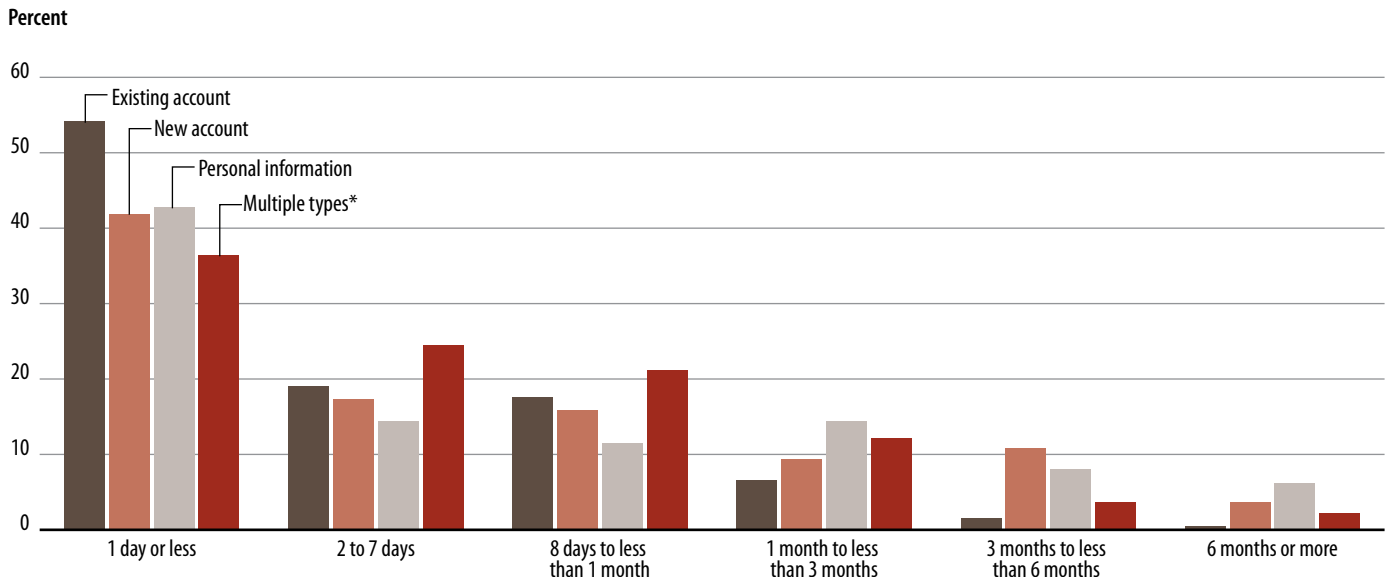
The majority of identity theft victims spent a day or less resolving associated financial and credit problems

At the time of the interview, 86% of identity theft victims had resolved any problems associated with the incident (appendix table 13). Of these, the majority spent a day or less clearing up the problems, while about 10% spent more than a month (figure 8). Victims of the misuse of existing accounts (54%) were more likely to resolve any associated financial and credit problems within a day, compared to victims of new account fraud (42%) and victims of multiple types of identity theft (36%). Among victims who had resolved all problems associated with the identity theft, 29% who experienced the

misuse of personal information for fraudulent purposes spent over a month clearing up the problems, compared to 9% of victims of existing account misuse.

Whether identity theft victims had resolved associated problems or not at the time of the interview, victims reported spending an average of about 9 hours clearing up the issues. Victims of existing credit card account misuse spent an average of 3 hours resolving problems, while victims whose personal information was used to open a new account or for other fraudulent purposes spent an average of about 30 hours resolving all problems (not shown).

FIGURE 8
Length of time spent resolving financial and credit problems associated with identity theft, by type of identity theft, 2012



Note: Estimates are based on the most recent incident of identity theft. See appendix table 13 for estimates and appendix table 14 for standard errors.

*Includes victims who experienced more than one type of identity theft in a single incident.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

14% of persons experienced identity theft at some point during their lives

Resolving the problems caused by identity theft may take more than a year for some victims. Of the 20.3 million persons age 16 or older who experienced the misuse of existing accounts or other personal information prior to 2012, 7% were still resolving the problems associated with the identity theft more than a year later (table 5). A greater percentage of persons who experienced the misuse of personal information to open a new account (16%) or for other fraudulent purposes (15%) prior to 2012 had unresolved problems more than a year later, compared to persons who experienced existing account misuse (4%).

Overall, 14% of persons age 16 or older, or 34.2 million persons, experienced one or more incidents of identity theft during their lives. The lifetime prevalence rate for identity theft varied to some degree with age. Younger persons, ages 16 to 17 (1%) and 18 to 24 (7%) and persons ages 65 or older (11%) had the lowest lifetime prevalence rates, while between 15% and 17% of persons ages 25 to 64 experienced identity theft at some point in their lives (not shown in table).

TABLE 5

Persons age 16 or older who experienced identity theft at any point in their lives, type of identity theft they experienced outside of the past year, and ongoing problems from identity theft that occurred outside of the past year, 2012

| | Number of persons | Percent of all persons | Percent with unresolved problems resulting from identity theft ^a |
|--|-------------------|------------------------|---|
| Experienced at least one incident of identity theft during lifetime | | | |
| No | 211,327,500 | 86.0% | ~ |
| Yes | 34,237,400 | 13.9 | 7.8% |
| Experienced at least one incident of identity theft outside of past 12 months | | | |
| No | 225,127,300 | 91.6% | ~ |
| Yes | 20,334,600 | 8.3 | 7.3% |
| Type of identity theft experienced | | | |
| Existing account | 15,311,100 | 6.2% | 4.0% |
| Credit card | 8,860,400 | 2.3 | 2.8 |
| Bank account | 5,721,700 | 3.6 | 5.9 |
| Other account | 729,000 | 0.3 | 7.7 |
| New account | 1,585,100 | 0.6 | 16.1 |
| Personal information | 1,947,700 | 0.8 | 14.9 |
| Multiple types | 1,450,300 | 0.6% | 20.6% |
| Existing accounts ^b | 572,800 | 0.2 | 11.1 |
| Other ^c | 877,500 | 0.4 | 26.7 |

Note: Detail may not sum to same population total due to a small number of victims who did not know whether they experienced identity theft during the lifetime or outside of the past 12 months. See appendix table 15 for standard errors.

~Not applicable.

^aBased on number of persons who experienced the identity theft.

^bIncludes victims who experienced two or more of the following: unauthorized use of a credit card, bank account, or other existing account.

^cIncludes victims who experienced two or more of the following: unauthorized use of an existing account, misuse of personal information to open a new account, or misuse of personal information for other fraudulent purposes.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

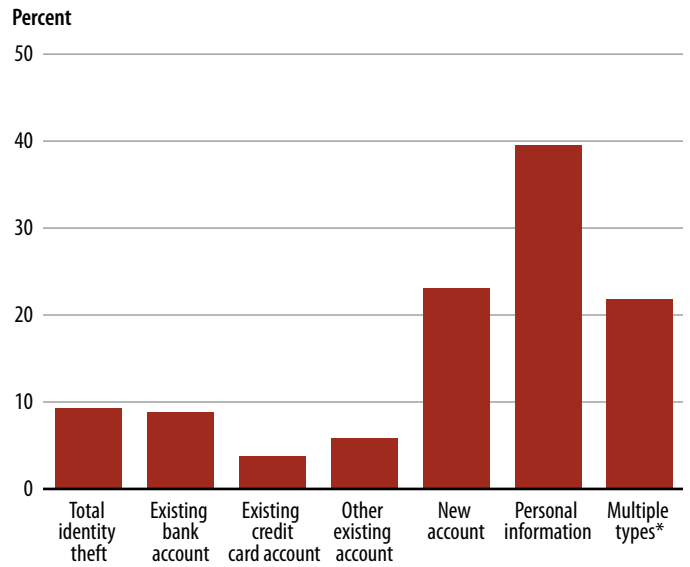
The level of emotional distress victims experienced was related to the length of time they spent resolving problems

Victims who spent more time resolving the financial and credit-related problems associated with the identity theft incident were more likely to experience problems with work and other relationships and severe emotional distress than victims who were able to resolve the problems relatively quickly. Among identity theft victims who spent 6 months or more resolving financial and credit problems due to the theft, 47% experienced severe emotional distress (figure 9). In comparison, 4% of victims who spent a day or less clearing up problems reported that the incident was severely distressing. Similarly, 14% of victims who spent 6 months or more resolving issues related to the identity theft reported having significant problems with family members or friends, compared to about 2% of victims who spent a day or less resolving problems.

Fewer than 1 in 10 identity theft victims reported the incident to police

In 2012, about 9% of identity theft victims reported the incident to police (figure 10). Victims of personal information fraud were the most likely to report the incident to police (40%), followed new account fraud victims (23%) and victims of multiple types of identity theft (22%). Fewer than 10% of victims of existing credit card (4%), existing bank account (9%), and other existing account misuse (6%) reported the incident to police.

FIGURE 10
Identity theft victims who reported the incident to police, by type of identity theft, 2012

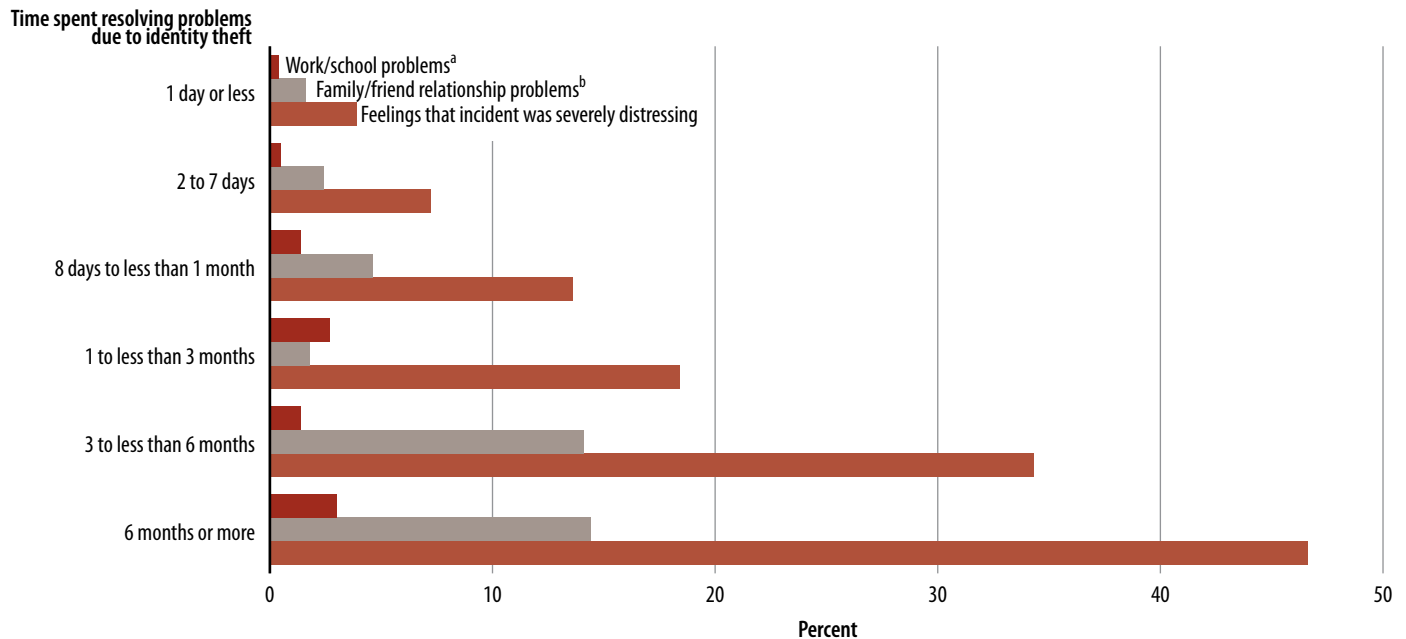


Note: Estimates are based on the most recent identity theft incident. See appendix table 17 for estimates and reasons victims did not report to police. See appendix table 18 for standard errors.

*Includes victims who experienced more than one type of identity theft in a single incident.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

FIGURE 9
Identity theft victims who reported work/school or family/friend problems or distress, by length of time spent resolving associated financial and credit problems, 2012



Note: Estimates are based on the most recent incident of identity theft. See appendix table 16 for estimates and standard errors.

^aIncludes victims reporting significant problems with job or school, such as trouble with boss, coworker, or peers.

^bIncludes victims reporting significant problems with family members or friends, including getting into more arguments or fights than before, not feeling able to trust them as much, or not feeling as close to them as before the crime.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

The 91% of identity theft victims who did not report an incident to police offered a variety of reasons for not reporting (appendix table 17). Among all victims who did not report the incident to police, the most common reason was that the victim handled it another way (58%). About a third (29%) of nonreporting victims did not contact police because they suffered no monetary loss. One in five nonreporting victims did not think that the police could help and another 15% did not know how to report the incident to law enforcement.

Of the 9% of identity theft victims who contacted a credit bureau, 7 in 10 placed a fraud alert on their credit report

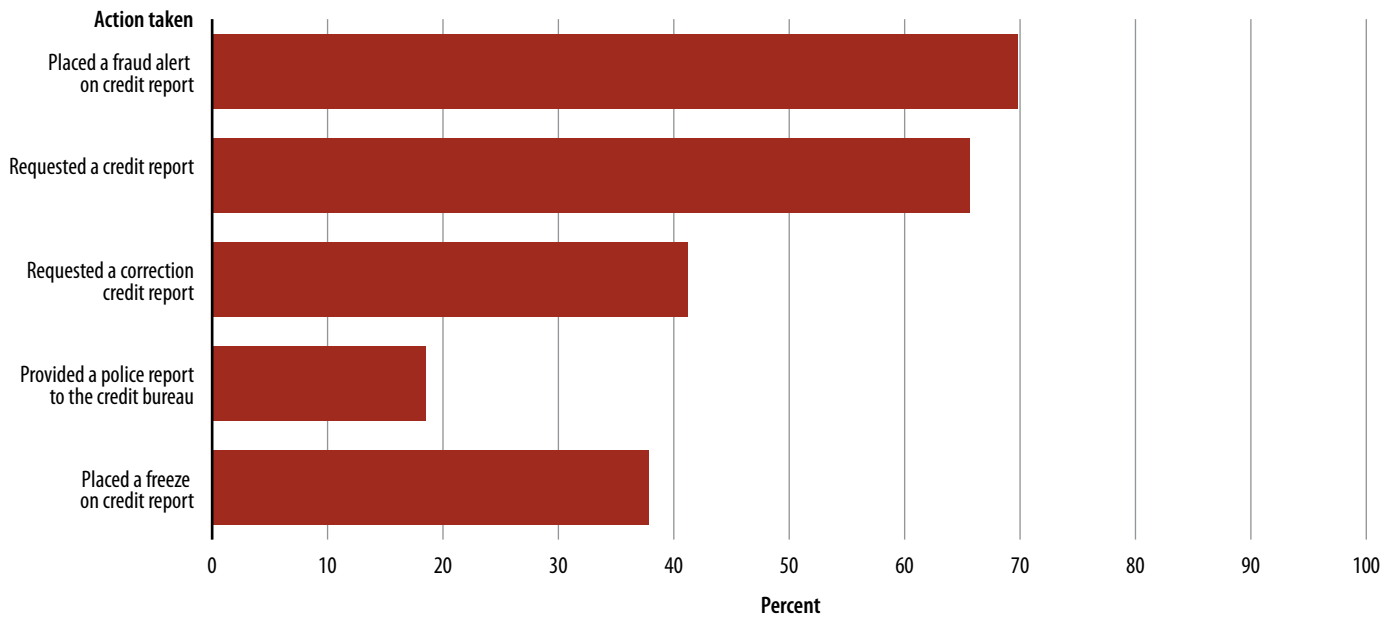
In 2012, 88% of all victims of identity theft reported the incident to one or more nonlaw enforcement agencies, either government or commercial (not shown). About 86% of identity theft victims contacted a credit card company or bank to report misuse or attempted misuse of an account or personal information (appendix table 19). Six percent of all identity theft victims contacted a credit monitoring service, 3% contacted an agency that issues identity documentation, (e.g., Social Security

Administration or an agency that issues drivers' licenses), 1% contacted the Federal Trade Commission, and 1% contacted a government consumer affairs agency or other consumer protection organization, (e.g., Better Business Bureau).

Nine percent of identity theft victims contacted a credit bureau to report the incident. Victims whose identifying information was fraudulently used to open a new account (30%) were most likely to contact a credit bureau, followed by victims of multiple types of theft (20%) and victims whose personal information was used for other fraudulent purposes (19%).

Victims of any type of identity theft who contacted a credit bureau could take several different actions. About 70% of victims who contacted a credit bureau placed a fraud alert on their credit report (figure 11). Two-thirds (66%) of victims who contacted a credit bureau requested a credit report, 41% requested corrections to their credit report, 38% placed a freeze on their credit report, and 19% provided a police report to the credit bureau.

FIGURE 11
Identity theft victims who contacted a credit bureau, by action taken, 2012



Note: Estimates are based on victims who contacted a credit bureau regarding the most recent incident of identity theft experienced within the past 12 months. Details sum to more than 100% because some victims took multiple actions with the credit bureau. See appendix table 19 for estimates and appendix table 20 for standard errors.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

About 85% of persons took some action to prevent identity theft victimization

The ITS asked persons about actions they took during the prior 12 months to prevent identity theft, such as checking credit reports, shredding documents with personal information, and changing passwords on financial accounts. In 2012, 85% of persons engaged in one or more of the preventative actions asked about in the survey (table 6). A greater percentage of victims (96%) than nonvictims (84%) engaged in at least one preventative action. However, about 12% of victims who took preventative action did so in response to experiencing identity theft in the past year.

Overall, the two most common preventative actions in 2012 were checking bank or credit statements (75%) and shredding or destroying documents with personal information (67%). A higher percentage of victims than nonvictims engaged in both of these preventative actions. However, about 13% of victims

began shredding or destroying documents with personal information as a result of experiencing identity theft during the prior 12 months and 26% began checking bank or credit statements as a result of the victimization.

Less than 10% of victims purchased identity theft protection (4%) or insurance (6%) or used an identity theft security program on the computer (6%) after experiencing identity theft, while about a quarter of victims checked financial accounts or changed passwords on these accounts as a result of the victimization.

Among persons who did not experience identity theft in 2012, 37% checked their credit report; 27% changed passwords on financial accounts; 16% used identity theft security programs on their computer; 5% purchased identity theft insurance or used a credit monitoring service; and 3% purchased identity theft protection.

TABLE 6
Actions victims and nonvictims took during the past 12 months to reduce the risk of identity theft, by whether the action was taken in response to the theft, 2012

| Type of action | Percent of persons age 16 or older | | | | |
|--|------------------------------------|------------|-------------------------------|--|---|
| | Total | Nonvictims | Victim during prior 12 months | | |
| | | | Total | Action taken in response to identity theft | Action taken independently of identity theft in past year |
| Any | 84.5% | 83.7% | 96.4% | 11.8% | 84.6% |
| Checked credit report | 37.9 | 36.8 | 53.1 | 15.0 | 38.1 |
| Changed passwords on financial accounts | 28.6 | 26.6 | 56.1 | 24.4 | 31.7 |
| Purchased identity theft insurance/credit monitoring service | 5.3 | 4.9 | 11.8 | 5.7 | 6.1 |
| Shredded/destroyed documents with personal information | 67.4 | 66.5 | 79.8 | 13.0 | 66.8 |
| Checked bank or credit statements | 74.8 | 73.6 | 91.8 | 25.6 | 66.2 |
| Used identity theft security program on computer | 16.6 | 16.1 | 24.5 | 5.7 | 18.8 |
| Purchased identity theft protection | 3.5 | 3.2 | 6.8 | 3.9 | 3.0 |

Note: Estimates are based on the most recent incident of identity theft. About 1% of victims and nonvictims did not know or did not report whether actions were taken. See appendix table 21 for standard errors.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

Methodology

Data collection

The Identity Theft Supplement (ITS) was administered as a supplement to the Bureau of Justice Statistics's (BJS) National Crime Victimization Survey (NCVS). The NCVS collects data on crime reported and not reported to the police against persons age 12 or older from a nationally representative sample of U.S. households. The sample includes persons living in group quarters (such as dormitories, rooming houses, and religious group dwellings) and excludes persons living in military barracks and institutional settings (such as correctional or hospital facilities) and the homeless. (For more information, see the *Survey Methodology in Criminal Victimization in the United States, 2008*, NCJ 231173, BJS website, May 2011.)

From January 1, 2012, through June 30, 2012, persons age 16 or older in sampled NCVS households received the ITS at the end of the NCVS interview. Proxy responders and those who complete the NCVS interview in a language other than English did not receive the ITS. All NCVS and ITS interviews were conducted using computer-assisted personal interviewing (CAPI). Interviews were conducted by telephone or by personal visit. A final sample size of 69,814 of the original NCVS-eligible respondents completed the ITS questionnaire, resulting in a response rate of 91.9%.

The combined overall NCVS-ITS unit response rate for NCVS households, NCVS persons, and ITS persons was 68.2%. Because of the level of nonresponse, a bias analysis was conducted. To the extent that those who responded to the survey and those who did not differ in important ways, there is potential for bias in estimates from the survey data. However, the result of the nonresponse bias analysis suggested that there was little or no bias of substantive importance due to nonresponse in the ITS estimates.

The ITS collected individual data on the prevalence of and victim response to the attempted or successful misuse of an existing account, misuse of personal information to open a new account, misuse of personal information for other fraudulent purposes. Respondents were asked whether they experienced any of these types of misuse during the 12 months prior to the interview. For example, persons interviewed in July 2012 were asked about identity theft incidents that occurred between July 2011 and June 2012. To simplify the discussion of the findings, this report refers to all identity theft experienced during the 12 months prior to the interviews as occurring in 2012.

Persons who reported one or more incidents of identity theft during 2012 were asked more detailed questions about the incident and response to the incident, such as how they discovered the identity theft; financial, credit, and other problems resulting from the incident; time spent resolving associated problems; and reporting to police and credit

bureaus. For most sections of the survey instrument, the ITS asked victims who experienced more than one incident during the 12-month reference period to describe only the most recent incident when answering questions. The ITS asked victims who experienced multiple incidents of identity theft during the year to report on the total financial losses suffered as a result of all incidents. The ITS asked both victims and nonvictims a series of questions about identity theft they experienced outside of the 12-month reference period and about measures they took to avoid or minimize the risk of becoming an identity theft victim.

Comparison of 2012 findings to prior BJS identity theft statistics

This report uses data that differ from previous BJS statistical collections on the topic of identity theft. Due to the differences, it was not possible to compare the identity theft estimates presented in this report to previously reported estimates.

Initial BJS reports on identity theft used household-level data from the core NCVS. Data were reported for the household as a whole rather than for individual respondents, and the questions were more limited, providing less detail on the characteristics of the incident and the victim response. For additional information, see *Identity Theft, 2005*, NCJ 219411, BJS website, November 2007, *Identity Theft Reported by Households, 2007 - Statistical Tables*, NCJ 230742, BJS website, June 2010, and *Identity Theft Reported by Households, 2005 - 2010*, NCJ 236245, BJS website, December 2010.

In 2008, BJS conducted the first Identity Theft Supplement to the NCVS. Like the 2012 ITS, the 2008 ITS collected detailed information on victim experiences with identity theft from persons age 16 or older. For more information, see *Victims of Identity Theft, 2008*, NCJ 231680, BJS website, December 2010. Following the administration of the first ITS, BJS made substantial changes to the survey instrument, making it difficult to compare across the 2008 and 2012 datasets. Some of the major changes to the survey from 2008 to 2012 included—

- Changing from a 2-year to 1-year reference period. The 2008 ITS asked about identity theft experienced in the 2 years prior to the interview. The 2-year reference period was intended to capture incidents of identity theft that were discovered more than 12 months prior to the interview but were still causing problems for the victim. The 2012 ITS used a 12-month reference period to be more consistent with the NCVS and other NCVS supplements. The 2012 ITS added a special section about identity theft experienced outside of the 1-year reference period to capture identity theft incidents with long-term consequences.
- Integrating of successful and attempted identity theft incidents. The 2008 ITS tried to distinguish attempted identity theft from successfully completed identity theft. It asked slightly different questions depending on whether respondents screened into the attempted or successful module. However, the distinction between an attempted

and successful incident of identity theft was not clear, and the two types were combined for reporting purposes to the extent possible. The 2012 ITS defined identity theft as attempted or completed misuse of personal information and collected the same information from all victims.

- Focusing on the most recent incident of identity theft for detailed follow-up questions. In the 2008 ITS, victims were asked one set of questions about the characteristics of identity theft and the response to identity theft, regardless of the number of incidents they experienced during the 2-year reference period. This made it impossible to attribute the incident characteristics or monetary loss to one specific type of identity theft. The 2012 ITS asked victims to identify whether they experienced one or more than one incidents of identity theft during the year.³ Victims who experienced more than one incident were asked to describe only the most recent incident when responding to detailed questions about the nature of and experiences with identity theft victimization.

Possible over-reporting of losses from jointly held accounts

Persons may have experienced the unauthorized use of a jointly held account. Joint accounts present a difficulty with counting financial harm or loss because of the potential for double-counting loss (e.g., both account holders report the same \$500 loss). Because financial loss was not attributed to a particular type of identity theft, victims of multiple types of identity theft may have experienced some financial loss from a joint account and some financial loss from an independently held account. Therefore, it was not possible to correct for any potential over-reporting due to joint account holders who may have been double counted.

Standard error computations

When national estimates are derived from a sample, as is the case with the ITS, caution must be taken when comparing one estimate to another. Although one estimate may be larger than another, estimates based on a sample have some degree of sampling error. The sampling error of an estimate depends on several factors, including the amount of variation in the responses, the size of the sample, and the size of the subgroup for which the estimate is computed. When the sampling error around the estimates is taken into consideration, the estimates that appear different may, not be statistically different.

One measure of the sampling error associated with an estimate is the standard error. The standard error can vary from one estimate to the next. In general, for a given metric, an estimate with a smaller standard error provides a more reliable

³Victims received the following definition of an identity theft incident: "An incident of identity theft occurs when your identity is stolen. A stolen credit card or debit card may be used multiple times, but this should be considered a single incident. Also, if multiple credit card numbers and a social security number were obtained at the same time, this should be considered a single incident."

approximation of the true value than an estimate with a larger standard error. Estimates with relatively large standard errors are associated with less precision and reliability and should be interpreted with caution.

In order to generate standard errors around estimates from the ITS, the Census Bureau produces generalized variance function (GVF) parameters for BJS. The GVFs take into account aspects of the NCVS complex sample design and represent the curve fitted to a selection of individual standard errors based on the Jackknife Repeated Replication technique. The GVF parameters were used to generate standard errors for each point estimate (i.e., numbers or percentages) in the report.

In this report, BJS conducted tests to determine whether differences in estimated numbers and percentages were statistically significant once sampling error was taken into account. Using statistical programs developed specifically for the NCVS, all comparisons in the text were tested for significance. The primary test procedure used was Student's t-statistic, which tests the difference between two sample estimates. To ensure that the observed differences between estimates were larger than might be expected due to sampling variation, the significance level was set at the 95% confidence level.

Data users can use the estimates and the standard errors of the estimates provided in this report to generate a confidence interval around the estimate as a measure of the margin of error. The following example illustrates how standard errors can be used to generate confidence intervals:

According to the ITS, in 2012, an estimated 6.7% of persons age 16 or older experienced identity theft (see table 1). Using the GVFs, BJS determined that the estimate has a standard error of 0.3 (see appendix table 1). A confidence interval around the estimate was generated by multiplying the standard errors by ± 1.96 (the t-score of a normal, two-tailed distribution that excludes 2.5% at either end of the distribution). Therefore, the confidence interval around the estimate is $6.7 \pm (0.3 \times 1.96)$ or 6.1 to 7.3. In other words, if different samples using the same procedures were taken from the U.S. population in 2012, 95% of the time the percentage of persons who experienced identity theft would be between 6.1% and 7.3%.

In this report, BJS also calculated a coefficient of variation (CV) for all estimates, representing the ratio of the standard error to the estimate. CVs provide a measure of reliability and a means to compare the precision of estimates across measures with differing levels or metrics. In cases where the CV was greater than 50%, or the unweighted sample had 10 or fewer cases, the estimate was noted with a "!" symbol (interpret data with caution; estimate is based on 10 or fewer sample cases, or the coefficient of variation exceeds 50%).

Many of the variables examined in this report may be related to one another and to other variables not included in the analyses. Complex relationships among variables were not fully

explored in this report and warrant more extensive analysis. Readers are cautioned not to draw causal inferences based on the results presented.

APPENDIX TABLE 1

Standard errors for figure 1: Persons age 16 or older who experienced at least one identity theft incident in the past 12 months by type of theft, 2012 and table 1: Persons age 16 or older who experienced at least one identity theft incident in the past 12 months, by type of theft, 2012

| Type of identity theft | Anytime during the past 12 months | | Most recent incident | | |
|------------------------|-----------------------------------|------------------------|----------------------|------------------------|------------------------|
| | Number of victims | Percent of all persons | Number of victims | Percent of all persons | Percent of all victims |
| Total | 750,223 | 0.3% | 750,223 | 0.3% | ~ |
| Existing account | 713,433 | 0.3 | 673,954 | 0.3 | 1.4 |
| Credit card | 455,777 | 0.2 | 414,852 | 0.2 | 1.7 |
| Bank | 446,837 | 0.2 | 394,659 | 0.2 | 1.7 |
| Other | 167,153 | 0.1 | 129,787 | 0.1 | 0.7 |
| New account | 127,633 | 0.1 | 92,348 | -- | 0.5 |
| Personal information | 104,992 | -- | 87,000 | -- | 0.5 |
| Multiple types | ~ | ~ | 136,881 | 0.1 | 0.8 |
| Existing account | ~ | ~ | 104,263 | -- | 0.6 |
| Other | ~ | ~ | 68,425 | -- | 0.4 |

~Not applicable.

--Less than 0.05%.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 2

Standard errors for table 2: Persons age 16 or older who experienced at least one identity theft incident during the past 12 months, by victim characteristics, 2012

| Characteristic | Any identity theft | | Misuse of existing credit card | | | Misuse of existing bank account | | | New account or personal information | |
|----------------------|--------------------|------------------------|--------------------------------|------------------------|-------------------------------------|---------------------------------|------------------------|--------------------------------------|-------------------------------------|------------------------|
| | Number of victims | Percent of all persons | Number of victims | Percent of all persons | Percent of persons with credit card | Number of victims | Percent of all persons | Percent of persons with bank account | Number of victims | Percent of all persons |
| Total | 750,223 | 0.3% | 455,777 | 0.2% | 0.3% | 446,837 | 0.2% | 0.2% | 177,890 | 0.1% |
| Sex | | | | | | | | | | |
| Male | 463,715 | 0.4 | 291,937 | 0.2 | 0.3 | 260,879 | 0.2 | 0.2 | 106,429 | 0.1 |
| Female | 493,153 | 0.4 | 283,702 | 0.2 | 0.3 | 302,628 | 0.2 | 0.3 | 119,168 | 0.1 |
| Age | | | | | | | | | | |
| 16-17 | 15,317 | 0.2 | 4,831 | 0.1 | 0.8 | 9,955 | 0.1 | 0.3 | 5,680 | 0.1 |
| 18-24 | 151,852 | 0.5 | 58,300 | 0.2 | 0.4 | 113,304 | 0.4 | 0.5 | 40,300 | 0.1 |
| 25-34 | 259,485 | 0.6 | 131,486 | 0.3 | 0.4 | 168,559 | 0.4 | 0.4 | 66,310 | 0.2 |
| 35-49 | 338,604 | 0.5 | 199,821 | 0.3 | 0.4 | 207,061 | 0.3 | 0.4 | 78,638 | 0.1 |
| 50-64 | 330,527 | 0.5 | 221,219 | 0.3 | 0.4 | 177,204 | 0.3 | 0.3 | 75,739 | 0.1 |
| 65 or older | 194,365 | 0.4 | 145,410 | 0.3 | 0.4 | 85,034 | 0.2 | 0.2 | 47,176 | 0.1 |
| Race/Hispanic origin | | | | | | | | | | |
| White | 623,114 | 0.4 | 397,484 | 0.2 | 0.3 | 355,777 | 0.2 | 0.2 | 129,204 | 0.1 |
| Black | 153,735 | 0.5 | 54,934 | 0.2 | 0.4 | 110,054 | 0.4 | 0.5 | 61,572 | 0.2 |
| Hispanic/Latino | 157,099 | 0.5 | 76,471 | 0.2 | 0.4 | 105,050 | 0.3 | 0.4 | 49,389 | 0.2 |
| Other race | 105,629 | 0.7 | 77,875 | 0.6 | 0.7 | 55,086 | 0.4 | 0.5 | 19,568 | 0.1 |
| Two or more races | 51,382 | 1.5 | 28,387 | 0.9 | 1.5 | 33,337 | 1.0 | 1.2 | 18,313 | 0.6 |
| Household income | | | | | | | | | | |
| \$24,999 or less | 179,393 | 0.4 | 66,983 | 0.2 | 0.4 | 123,421 | 0.3 | 0.4 | 67,615 | 0.2 |
| \$25,000-\$49,999 | 233,453 | 0.4 | 120,182 | 0.2 | 0.3 | 153,467 | 0.3 | 0.3 | 70,047 | 0.1 |
| \$50,000-\$74,999 | 221,677 | 0.6 | 124,607 | 0.4 | 0.4 | 140,705 | 0.4 | 0.4 | 49,998 | 0.1 |
| \$75,000 or more | 398,169 | 0.6 | 278,794 | 0.4 | 0.5 | 209,698 | 0.3 | 0.3 | 68,294 | 0.1 |
| Unknown | 244,419 | 0.4 | 154,516 | 0.3 | 0.4 | 134,298 | 0.2 | 0.3 | 56,601 | 0.1 |

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 3**Ways that victims discovered identity theft, by type of theft, 2012**

| | Any identity theft | | Existing account misuse | | Other identity theft ^a | |
|--|--------------------|----------------|-------------------------|----------------|-----------------------------------|----------------|
| | Percent | Standard error | Percent | Standard error | Percent | Standard error |
| Contacted by financial institution about suspicious activity | 42.1% | 1.7% | 45.2% | 1.8% | 15.2% | 2.5% |
| Noticed fraudulent charges on account | 18.6 | 1.2 | 19.8 | 1.3 | 7.5 | 1.8 |
| Noticed money missing from account | 9.9 | 0.9 | 10.5 | 0.9 | 4.6 | 1.3 |
| Notified by a company or agency | 6.4 | 0.7 | 4.7 | 0.6 | 20.9 | 2.9 |
| Contacted financial institution to report a theft | 5.5 | 0.6 | 5.7 | 0.7 | 3.3 | 1.1 |
| Credit card declined, check bounced, or account closed due to insufficient funds | 5.0 | 0.6 | 5.4 | 0.6 | 1.6 | 0.7 |
| Received a bill or contacted about an unpaid bill | 4.3 | 0.5 | 3.3 | 0.5 | 13.4 | 2.4 |
| Notified by a known person | 1.3 | 0.3 | 1.0 | 0.2 | 4.5 | 1.3 |
| Discovered through credit report or credit monitoring service | 1.3 | 0.3 | 0.9 | 0.2 | 4.8 | 1.4 |
| Problems applying for a loan, government benefits or with income taxes | 1.2 | 0.3 | 0.1 | 0.1 | 10.7 | 2.1 |
| Notified by police | 0.8 | 0.2 | 0.3 | 0.1 | 5.7 | 1.5 |
| Received merchandise or a card that the victim did not order or did not receive a product the victim had ordered | 0.7 | 0.2 | 0.5 | 0.2 | 1.9! | 0.8 |
| Another way ^b | 2.8 | 0.4 | 2.4 | 0.4 | 5.9 | 1.5 |

Note: Estimates are based on the most recent identity theft incident.

! Estimate based on 10 or fewer sample cases, or coefficient of variation is greater than 50%.

^aIncludes incidents involving the use of personal information to open a new account or for other fraudulent purposes.

^bVictim noticed suspicious phishing activity, hacked computer, account information missing or stolen, or discovered the theft by accident.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 4**Estimates and standard errors for figure 3: Identity theft victims who knew how their personal information was obtained, by type of theft, 2012**

| Type of identity theft | Estimate | Standard error |
|------------------------------|----------|----------------|
| Total | 32.0% | 1.6% |
| Existing credit card account | 24.4 | 1.9 |
| Existing bank account | 35.4 | 2.3 |
| Other existing account | 39.0 | 4.3 |
| New account | 36.7 | 5.2 |
| Personal information | 33.4 | 5.2 |
| Multiple types* | 46.5 | 4.3 |

*Includes victims who experienced more than one type of identity theft in a single incident.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 5**Standard errors for table 3: Identity theft victims who knew something about the offender, by type of theft, 2012**

| Type of identity theft | Victim knew something about the offender |
|------------------------|--|
| Total | 0.8% |
| Existing account | 0.7 |
| Credit card | 0.6 |
| Bank | 1.2 |
| Other | 3.0 |
| New account | 4.5 |
| Personal information | 4.6 |
| Multiple types | 2.8 |
| Existing account | 2.9 |
| Other | 5.4 |

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 6**Standard errors for table 4: Mean losses attributed to identity theft and property crime, 2012**

| | Mean |
|---------------------|---------|
| Identity theft | \$3,404 |
| Property crime | \$1,621 |
| Burglary | 2,630 |
| Motor vehicle theft | 4,881 |
| Theft | 1,129 |

Note: Standard errors for median and total losses were not calculated.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, 2012, and National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 7**Estimates and standard errors for figure 4: Total out-of-pocket loss for identity theft victims experiencing a loss of \$1 or more, 2012**

| Total out-of-pocket loss | Percent of victims | |
|--------------------------|--------------------|----------------|
| | Estimate | Standard error |
| \$99 or less | 48.8% | 3.5% |
| \$100-\$249 | 17.9 | 2.5 |
| \$250-\$499 | 8.4 | 1.7 |
| \$500-\$999 | 8.5 | 1.7 |
| \$1,000-\$2,499 | 9.9 | 1.8 |
| \$2,500-\$4,999 | 3.1 | 1.0 |
| \$5,000 or more | 3.4 | 1.0 |

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 8**Financial loss among victims who experienced at least one attempted or successful identity theft incident during the previous 12 months, by type of theft and type of loss, 2012**

| | Total identity theft | Existing account | | | | New account | Personal information | Multiple types | | |
|--|----------------------|------------------|-------------|-----------|-----------|-------------|----------------------|----------------|------------------|----------|
| | | Total | Credit card | Bank | Other | | | Total | Existing account | Other |
| Total number of victims | 16,580,500 | 14,022,100 | 6,676,300 | 6,191,500 | 1,154,300 | 683,400 | 622,900 | 1,252,000 | 824,700 | 427,400 |
| Combined direct and indirect loss | | | | | | | | | | |
| Mean | \$1,769 | \$1,008 | \$1,435 | \$580 | \$1,027 | \$6,510 | \$21,804 | \$3,187 | \$2,772 | \$3,974 |
| Median | \$300 | \$200 | \$300 | \$200 | \$200 | \$500 | \$1,500 | \$400 | \$350 | \$600 |
| Percent experiencing a loss | 67.5 | 69.7 | 68.7 | 74.3 | 50.9 | 46.2 | 37.9 | 68.8 | 68.4 | 69.5 |
| Direct loss | | | | | | | | | | |
| Mean | \$1,409 | \$1,003 | \$1,448 | \$551 | \$1,057 | \$7,135 | \$9,650 | \$2,140 | \$1,161 | \$4,119 |
| Median | \$300 | \$200 | \$300 | \$200 | \$200 | \$600 | \$1,900 | \$400 | \$300 | \$600 |
| Percent experiencing a loss | 66.4 | 69.0 | 68.1 | 73.7 | 48.6 | 42.2 | 32.5 | 67.3 | 68.3 | 65.2 |
| Direct out-of-pocket loss | | | | | | | | | | |
| Mean | \$4,313 | \$2,188 | \$4,176 | \$1,754 | \$1,600 | \$1,598 | \$19,463 | \$8,464 | \$3,691 | \$14,335 |
| Median | \$200 | \$100 | \$200 | \$100 | \$100 | \$1,000 | \$1,800 | \$200 | \$100 | \$300 |
| Percent experiencing a loss | 9.0 | 7.7 | 3.1 | 11.5 | 14.4 | 8.9 | 15.0 | 20.0 | 16.8 | 26.3 |
| Indirect loss | | | | | | | | | | |
| Mean | \$4,168 | \$257 | \$39 | \$434 | \$133 | \$75 | \$37,797 | \$5,901 | \$14,327 | \$338 |
| Median | \$30 | \$10 | \$10 | \$20 | \$10 | \$40 | \$400 | \$90 | \$50 | \$100 |
| Percent experiencing a loss | 6.3 | 5.2 | 4.0 | 6.2 | 6.7 | 10.1 | 13.6 | 12.9 | 7.8 | 22.8 |
| Total out-of-pocket loss | | | | | | | | | | |
| Mean | \$4,804 | \$1,565 | \$1,991 | \$1,444 | \$1,264 | \$863 | \$34,352 | \$9,001 | \$8,572 | \$9,409 |
| Median | \$100 | \$80 | \$40 | \$90 | \$70 | \$300 | \$700 | \$200 | \$60 | \$200 |
| Percent experiencing a loss | 13.5 | 11.6 | 6.5 | 15.8 | 19.0 | 17.4 | 23.4 | 27.3 | 20.2 | 40.9 |

Note: See appendix table 9 for standard errors.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 9

Standard errors for appendix table 8: Financial loss among victims who experienced at least one attempted or successful identity theft incident during the previous 12 months, by type of theft and type of loss, 2012

| | Total identity theft | Existing account | | | | New account | Personal information | Multiple types | | |
|--|----------------------|------------------|-------------|---------|---------|-------------|----------------------|----------------|------------------|---------|
| | | Total | Credit card | Bank | Other | | | Total | Existing account | Other |
| Total number of victims | 750,223 | 673,954 | 414,852 | 394,659 | 129,787 | 92,348 | 87,000 | 136,881 | 104,263 | 68,425 |
| Combined direct and indirect loss | | | | | | | | | | |
| Mean | \$3,051 | \$2,281 | \$2,737 | \$1,718 | \$2,303 | \$6,057 | \$11,700 | \$4,149 | \$3,856 | \$4,660 |
| Percent experiencing a loss | 1.7 | 1.8 | 2.3 | 2.2 | 4.5 | 5.4 | 5.4 | 4.1 | 4.8 | 6.2 |
| Direct loss | | | | | | | | | | |
| Mean | \$2,712 | \$2,275 | \$2,750 | \$1,674 | \$2,338 | \$6,361 | \$7,484 | \$3,369 | \$2,454 | \$4,749 |
| Percent experiencing a loss | 1.7 | 1.8 | 2.3 | 2.2 | 4.5 | 5.4 | 5.2 | 4.1 | 4.8 | 6.4 |
| Direct out-of-pocket loss | | | | | | | | | | |
| Mean | \$4,866 | \$3,408 | \$4,784 | \$3,037 | \$2,896 | \$2,894 | \$10,985 | \$6,973 | \$4,482 | \$9,283 |
| Percent experiencing a loss | 0.8 | 0.8 | 0.6 | 1.3 | 2.9 | 2.8 | 3.8 | 3.2 | 3.5 | 5.6 |
| Indirect loss | | | | | | | | | | |
| Mean | \$4,779 | \$1,134 | \$438 | \$1,482 | \$814 | \$606 | \$15,942 | \$5,747 | \$9,280 | \$1,304 |
| Percent experiencing a loss | 0.7 | 0.6 | 0.7 | 1.0 | 2.0 | 3.0 | 3.6 | 2.6 | 2.4 | 5.3 |
| Total out-of-pocket loss | | | | | | | | | | |
| Mean | \$5,152 | \$2,863 | \$3,244 | \$2,745 | \$2,563 | \$2,106 | \$15,101 | \$7,208 | \$7,021 | \$7,382 |
| Percent experiencing a loss | 1.0 | 1.0 | 1.0 | 1.6 | 3.3 | 3.9 | 4.6 | 3.7 | 3.9 | 6.4 |

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 10

Estimates and standard errors for figure 5: Victims who experienced financial or legal problems as a result of identity theft, by type of theft, 2012

| Type of problems experienced | Estimates | | | Standard errors | | |
|---|--------------------|-------------------------|-----------------------------------|--------------------|-------------------------|-----------------------------------|
| | Any identity theft | Existing account misuse | Other identity theft ^a | Any identity theft | Existing account misuse | Other identity theft ^a |
| Credit-related problems ^b | 2.6% | 1.6% | 11.6% | 0.4% | 0.3% | 2.2% |
| Banking problems ^c | 2.1 | 1.6 | 6.7 | 0.4 | 0.3 | 1.6 |
| Problems with debt collectors | 3.3 | 1.7 | 16.7 | 0.5 | 0.3 | 2.6 |
| Utilities cut off or new service denied | 0.6 | 0.5 | 1.7! | 0.2 | 0.2 | 0.8 |
| Legal problems ^d | 0.5 | 0.2! | 2.9 | 0.2 | 0.1 | 1.1 |
| Other problems ^e | 0.5 | 0.3 | 2.6 | 0.2 | 0.1 | 1.0 |

Note: Estimates are based on the most recent identity theft incident.

! Interpret estimate with caution; estimate is based on 10 or fewer sample cases or coefficient of variation is greater than 50%.

^aIncludes identity theft incidents involving the misuse of personal information to open a new account or for other fraudulent purposes.

^bIncludes problems such as having to correct the same information on a credit report repeatedly, being turned down for credit or loans, or paying higher interest rates.

^cIncludes problems such as being turned down for a checking account or having checks bounce.

^dIncludes being the subject of a lawsuit or other criminal proceedings, or being arrested.

^eIncludes problems such as being turned down for or losing a job or problems with income taxes.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 11**Identity theft and violent crime victims who experienced emotional distress, by type of identity theft or violent crime, 2012**

| | Total number of victims | Significant work- or school-related problems ^a | Significant family or friend relationship problems ^b | Distress related to crime | | | |
|------------------------------------|-------------------------|---|---|---------------------------|-------|----------|--------|
| | | | | None | Mild | Moderate | Severe |
| Total identity theft | 16,580,500 | 1.5% | 3.7% | 20.7% | 42.7% | 26.2% | 10.5% |
| Existing account misuse | 14,022,100 | 0.9 | 2.9 | 21.9 | 44.2 | 25.5 | 8.3 |
| Credit card | 6,676,300 | 0.5 | 1.6 | 25.6 | 46.7 | 22.4 | 5.3 |
| Bank | 6,191,500 | 1.1 | 3.7 | 18.2 | 42.1 | 28.3 | 11.4 |
| Other | 1,154,300 | 1.8! | 5.9 | 21.1 | 41.6 | 28.4 | 8.9 |
| New account | 683,400 | 6.1! | 10.1 | 14.3 | 33.9 | 30.2 | 21.7 |
| Personal information | 622,900 | 5.2! | 10.4 | 16.4 | 27.2 | 24.6 | 31.8 |
| Multiple types | 1,252,000 | 3.9 | 5.9 | 12.1 | 38.0 | 32.2 | 17.7 |
| Existing account ^c | 824,666 | 3.7! | 5.5 | 16.2 | 41.2 | 31.3 | 11.3 |
| Other ^d | 427,371 | 4.3! | 6.6! | 4.3! | 31.8 | 33.8 | 30.1 |
| Total violent victimization | 5,901,100 | 12.3% | 18.9% | 19.0% | 29.7% | 22.6% | 28.8% |
| Rape/sexual assault | 316,700 | 27.5 | 28.8 | 24.2! | 16.4 | 17.5 | 41.9 |
| Robbery | 695,400 | 14.0 | 27.0 | 13.0 | 20.8 | 26.0 | 40.1 |
| Aggravated assault | 892,900 | 9.8 | 12.8 | 19.2 | 24.0 | 30.3 | 26.5 |
| Simple assault | 3,996,100 | 11.4 | 18.1 | 19.5 | 33.7 | 20.7 | 26.0 |

Note: Estimates are based on the most recent identity theft incident. See appendix table 12 for standard errors.

! Interpret with caution; estimates based on 10 or fewer sample cases, or the coefficient of variation is greater than 50%.

^aIncludes victims reporting significant problems with job or school, such as trouble with boss, coworker, or peers.

^bIncludes victims reporting significant problems with family members or friends, including getting into more arguments or fights than before, not feeling able to trust them as much, or not feeling as close to them as before the crime.

^cIncludes victims who experienced two or more of the following: unauthorized use of a credit card, banking account, or other existing account.

^dIncludes victims who experienced two or more of the following: use of an existing account, misuse of personal information to open a new account, or misuse of personal information of other fraudulent purposes.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, 2012 and National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 12**Standard errors for appendix table 11: Identity theft and violent crime victims who experienced emotional distress, by type of identity theft or violent crime, 2012**

| | Total number of victims | Significant work- or school-related problems | Significant family or friend relationship problems | Distress related to crime | | | |
|------------------------------------|-------------------------|--|--|---------------------------|------|----------|--------|
| | | | | None | Mild | Moderate | Severe |
| Total identity theft | 750,223 | 0.3% | 0.5% | 1.3% | 1.7% | 1.5% | 0.9% |
| Existing account misuse | 673,954 | 0.2 | 0.5 | 1.4 | 1.8 | 1.5 | 0.8 |
| Credit card | 414,852 | 0.2 | 0.4 | 1.9 | 2.4 | 1.8 | 0.8 |
| Bank | 394,659 | 0.4 | 0.7 | 1.7 | 2.4 | 2.1 | 1.3 |
| Other | 129,787 | 1.0 | 1.8 | 3.4 | 4.3 | 3.9 | 2.3 |
| New account | 92,348 | 2.3 | 3.0 | 3.6 | 5.1 | 4.9 | 4.3 |
| Personal information | 87,000 | 2.2 | 3.2 | 3.9 | 4.9 | 4.7 | 5.2 |
| Multiple types | 136,881 | 1.4 | 1.8 | 2.6 | 4.1 | 3.9 | 3.1 |
| Existing account | 104,263 | 1.6 | 2.0 | 3.5 | 4.9 | 4.6 | 2.9 |
| Other | 68,425 | 2.4 | 3.0 | 2.4 | 6.0 | 6.1 | 5.9 |
| Total violent victimization | 355,502 | 1.3% | 1.6% | 1.6% | 2.0% | 1.8% | 2.0% |
| Rape/sexual assault | 51,953 | 5.9 | 6.0 | 5.6 | 4.8 | 4.9 | 6.7 |
| Robbery | 85,975 | 3.2 | 4.2 | 3.1 | 3.8 | 4.2 | 4.8 |
| Aggravated assault | 101,200 | 2.4 | 2.7 | 3.3 | 3.7 | 4.0 | 3.8 |
| Simple assault | 273,940 | 1.4 | 1.8 | 1.9 | 2.4 | 1.9 | 2.2 |

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 13**Identity theft victims who resolved associated problems and length of time spent resolving problems, 2012**

| Time to resolve | Total identity theft | Existing account | | | | New account | Personal information | Multiple types | | |
|---|----------------------|------------------|-------------|------|-------|-------------|----------------------|----------------|------------------|-------|
| | | Total | Credit card | Bank | Other | | | Total | Existing account | Other |
| Victim resolved problems associated with theft | | | | | | | | | | |
| No | 8.8% | 6.4% | 4.7% | 7.0% | 13.2% | 25.7% | 34.2% | 13.5% | 9.7% | 20.8% |
| Yes | 86.2 | 89.7 | 91.7 | 89.4 | 79.6 | 57.0 | 45.7 | 83.3 | 88.5 | 73.3 |
| Length of time to resolve problems | | | | | | | | | | |
| 1 day or less | 52.3 | 54.2 | 60.9 | 46.1 | 57.7 | 41.9 | 42.8 | 36.4 | 42.4 | 22.6 |
| 2 to 7 days | 19.3 | 19.0 | 17.7 | 20.7 | 17.6 | 17.3 | 14.4 | 24.4 | 24.2 | 25.1 |
| 8 days to less than 1 month | 17.7 | 17.6 | 12.5 | 23.9 | 13.4 | 15.9 | 11.5 | 21.2 | 22.4 | 18.6 |
| 1 month to less than 3 months | 7.3 | 6.6 | 6.2 | 7.0 | 7.4 | 9.4 | 14.4 | 12.1 | 7.5 | 22.9 |
| 3 months to less than 6 months | 2.1 | 1.5 | 1.5 | 1.3 | 2.7 | 10.8 | 8.0 | 3.6 | 3.1! | 4.9! |
| 6 months or more | 0.8 | 0.5 | 0.3 | 0.6 | 1.2 | 3.7 | 6.1 | 2.2 | 0.5! | 4.9! |
| Unknown length of time | 0.5 | 0.5 | 0.8 | 0.3 | -- | 1.0 | 2.8 | --! | --! | --! |
| Do not know | 5.0% | 3.9% | 3.6% | 3.6% | 7.2% | 17.3% | 20.1% | 3.2% | 1.8%! | 5.9%! |

Note: Estimates are based on the most recent identity theft incident. Detail may not sum to total due to rounding. See appendix table 14 for standard errors.

--Less than 0.05%.

! Interpret estimate with caution; estimate based on 10 or fewer sample cases, or coefficient of variation greater than 50%.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 14**Standard errors for appendix table 13: Identity theft victims who resolved associated problems and length of time spent resolving problems, 2012**

| Time to resolve | Total identity theft | Existing account | | | | New account | Personal information | Multiple types | | |
|---|----------------------|------------------|-------------|------|-------|-------------|----------------------|----------------|------------------|-------|
| | | Total | Credit card | Bank | Other | | | Total | Existing account | Other |
| Victim resolved problems associated with theft | | | | | | | | | | |
| No | 0.8% | 0.7% | 0.8% | 1.0% | 2.8% | 4.6% | 5.3% | 2.7% | 2.7% | 5.1% |
| Yes | 1.3 | 1.2 | 1.4 | 1.6 | 3.7 | 5.5 | 5.6 | 3.3 | 3.4 | 6.0 |
| Length of time to resolve problems | | | | | | | | | | |
| 1 day or less | 1.9 | 2.0 | 2.4 | 2.5 | 4.9 | 6.7 | 7.7 | 4.4 | 5.2 | 6.1 |
| 2 to 7 days | 1.3 | 1.4 | 1.7 | 1.9 | 3.5 | 4.9 | 5.2 | 3.8 | 4.4 | 6.3 |
| 8 days to less than 1 month | 1.3 | 1.3 | 1.4 | 2.0 | 3.0 | 4.8 | 4.7 | 3.6 | 4.2 | 5.6 |
| 1 month to less than 3 months | 0.8 | 0.8 | 1.0 | 1.1 | 2.3 | 3.7 | 5.2 | 2.8 | 2.5 | 6.1 |
| 3 months to less than 6 months | 0.4 | 0.3 | 0.4 | 0.4 | 1.3 | 4.0 | 3.9 | 1.5 | 1.6 | 2.9 |
| 6 months or more | 0.2 | 0.2 | 0.2 | 0.3 | 0.9 | 2.3 | 3.4 | 1.1 | 0.6 | 2.9 |
| Unknown length of time | 0.2 | 0.2 | 0.3 | 0.2 | -- | 1.2 | 2.3 | -- | -- | -- |
| Do not know | 0.6 | 0.5 | 0.7 | 0.7 | 2.0 | 3.9 | 4.3 | 1.3 | 1.1 | 2.8 |

--Less than 0.05%.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 15

Standard errors for table 5: Persons age 16 or older who experienced identity theft at any point in their lives, type of identity theft they experienced outside of the past year, and ongoing problems from identity theft that occurred outside of the past year, 2012

| | Number of persons | Percent of all persons | Percent with unresolved problems resulting from identity theft |
|--|-------------------|------------------------|--|
| Experienced at least one incident of identity theft during lifetime | | | |
| No | 1,538,646 | 0.6% | ~ |
| Yes | 1,170,040 | 0.5 | 0.6% |
| Experienced at least one incident of identity theft outside of past 12 months | | | |
| No | 1,247,612 | 0.5% | 0.1% |
| Yes | 853,299 | 0.3 | 0.7 |
| Type of identity theft experienced | | | |
| Existing account | | | |
| Existing account | 713,065 | 0.3 | 0.5 |
| Credit card | 499,949 | 0.2 | 0.5 |
| Bank account | 374,551 | 0.2 | 1.0 |
| Other account | 96,275 | -- | 2.5 |
| New account | | | |
| New account | 159,840 | 0.1 | 2.7 |
| Personal information | | | |
| Personal information | 183,122 | 0.1 | 2.4 |
| Multiple types | | | |
| Multiple types | 150,748 | 0.1 | 3.1 |
| Existing accounts | 82,447 | -- | 3.4 |
| Other | 108,544 | -- | 4.2 |

~Not applicable.

--Less than 0.05%.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 16

Estimates and standard errors for figure 9: Identity theft victims who reported work/school or relationship problems or distress, by length of time spent resolving associated financial and credit problems, 2012

| Time spent resolving problems due to identity theft | Work/school problems ^a | | Family/friend relationship problems ^b | | Feelings that incident was severely distressing | |
|---|-----------------------------------|----------------|--|----------------|---|----------------|
| | Estimate | Standard error | Estimate | Standard error | Estimate | Standard error |
| 1 day or less | 0.4% | 0.2% | 1.6% | 0.4% | 3.9% | 0.7% |
| 2 to 7 days | 0.5 | 0.3 | 2.4 | 0.8 | 7.2 | 1.4 |
| 8 days to less than 1 month | 1.4 | 0.6 | 4.6 | 1.1 | 13.6 | 2.0 |
| 1 to less than 3 months | 2.7 | 1.3 | 1.8 | 1.0 | 18.4 | 3.4 |
| 3 to less than 6 months | 1.4 | 1.6 | 14.1 | 5.1 | 34.3 | 7.2 |
| 6 months or more | 3.0 | 3.6 | 14.4 | 7.7 | 46.6 | 11.4 |

^aIncludes victims reporting significant problems with job or school, such as trouble with boss, coworker, or peers.

^bIncludes victims reporting significant problems with family members or friends, including getting into more arguments or fights than before, not feeling able to trust them as much, or not feeling as close to them as before the crime.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 17**Victims who did and did not report identity theft to police, by type of theft and reason for not reporting, 2012**

| Victim response | Total identity theft | Existing account | | | | New account | Personal information | Multiple types | | |
|--|----------------------|------------------|-------------|------|-------|-------------|----------------------|----------------|-------------------------------|--------------------|
| | | Total | Credit card | Bank | Other | | | Total | Existing account ^a | Other ^b |
| Reported to police | 9.3% | 6.2% | 3.7% | 8.8% | 5.8% | 23.0% | 39.5% | 21.8% | 17.0% | 31.1% |
| Did not report to police | 90.5 | 93.7 | 96.1 | 90.9 | 94.2 | 76.5 | 59.9 | 77.6 | 82.5 | 68.0 |
| Reasons for not reporting | | | | | | | | | | |
| Did not know to report ^c | 15.2 | 15.0 | 14.4 | 15.4 | 16.5 | 14.1 | 23.2 | 15.0 | 15.8 | 13.2 |
| No monetary loss | 28.9 | 29.9 | 32.6 | 26.6 | 30.4 | 21.4 | 20.4 | 23.4 | 23.4 | 23.3 |
| Handled it another way ^d | 57.9 | 59.2 | 59.8 | 59.8 | 52.1 | 47.0 | 34.0 | 55.8 | 59.0 | 48.4 |
| Did not think the police could help ^e | 20.2 | 19.5 | 18.4 | 18.9 | 29.3 | 25.2 | 21.2 | 25.9 | 23.5 | 31.6 |
| Offender was a family member or friend | 1.5 | 1.2 | 0.3! | 1.5 | 4.1! | 6.6! | 2.6! | 2.5! | 2.6! | 2.2! |
| Personal reasons ^f | 3.3 | 3.0 | 2.9 | 3.0 | 3.1! | 4.7! | 10.3! | 4.9 | 2.9! | 9.8! |
| Location of the theft ^g | 1.3 | 1.4 | 1.6 | 1.0 | 2.0! | 0.9! | --! | 1.0! | 0.9! | 1.2! |
| Other ^h | 1.3 | 0.7 | 0.7 | 0.7 | 1.1! | 5.0! | 12.7 | 2.5! | 1.3! | 5.5! |

Note: Estimates are based on the most recent identity theft incident. Detail may not sum to total due to victims who reported multiple reasons for not contacting police. See appendix table 18 for standard errors.

--Less than 0.05%.

! Estimate based on 10 or fewer sample cases, or coefficient of variation is greater than 50%.

^aIncludes victims who experienced two or more of the following: the unauthorized use of a credit card, bank account, or other existing account.

^bIncludes victims who experienced two or more of the following: unauthorized use of an existing account, misuse of personal information to open a new account, or misuse of personal information for other fraudulent purposes.

^cIncludes victims who did not know they could report the incident and victims who did not know what agency was responsible for identity theft crimes.

^dIncludes victims who reported the incident to another organization, such as a credit card company; victims who took care of it themselves; victims who reported that the credit card company, bank, or other organization took care of the problem; victims who reported a family member took care of the problem; and victims who thought the credit card company, bank, or other organization would handle the problem.

^eIncludes victims who didn't think the police would do anything, victims who didn't want to bother the police, victims who thought it was too late for the police to help, and victims who couldn't identify the offender or provide much information to the police.

^fIncludes victims who were afraid to report the incident, victims who were embarrassed, victims who thought it was too inconvenient, and victims who didn't want to think about the incident.

^gIncludes victims of identity theft that occurred out of state or outside of the United States.

^hIncludes victims who reported that the identity theft just occurred or is still ongoing and plan to report soon, victims who were not sure it was a crime, victims who were contacted by law enforcement, and victims who did not report for other reasons.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 18**Standard errors for table 17: Victims who did and did not report identity theft to police, by type of theft and reason for not reporting, 2012**

| Victim response | Total identity theft | Existing account | | | | New account | Personal information | Multiple types | | |
|--|----------------------|------------------|-------------|---------|-------|-------------|----------------------|----------------|------------------|-------|
| | | Total | Credit card | Banking | Other | | | Total | Existing account | Other |
| Reported to police | 0.8% | 0.7% | 0.7% | 1.2% | 1.8% | 4.4% | 5.5% | 3.4% | 3.6% | 6.0% |
| Did not report to police | 1.1 | 1.0 | 1.0 | 1.5 | 2.2 | 4.8 | 5.6 | 3.7 | 4.0 | 6.3 |
| Reasons for not reporting | | | | | | | | | | |
| Did not know to report | 1.2 | 1.2 | 1.5 | 1.6 | 3.1 | 4.0 | 5.7 | 3.1 | 3.7 | 5.0 |
| No monetary loss | 1.6 | 1.7 | 2.2 | 2.1 | 4.1 | 4.8 | 5.4 | 3.8 | 4.4 | 6.4 |
| Handled it another way | 1.9 | 1.9 | 2.4 | 2.5 | 4.6 | 6.1 | 6.5 | 4.8 | 5.4 | 7.8 |
| Did not think the police could help | 1.3 | 1.4 | 1.7 | 1.8 | 4.0 | 5.1 | 5.5 | 4.0 | 4.4 | 7.1 |
| Offender was a family member or friend | 0.3 | 0.3 | 0.2 | 0.4 | 1.5 | 2.7 | 2.0 | 1.2 | 1.5 | 2.0 |
| Personal reasons | 0.5 | 0.5 | 0.6 | 0.7 | 1.3 | 2.3 | 3.9 | 1.8 | 1.6 | 4.3 |
| Location of the theft | 0.3 | 0.3 | 0.4 | 0.3 | 1.0 | 1.0 | -- | 0.8 | 0.9 | 1.5 |
| Other | 0.3 | 0.2 | 0.3 | 0.3 | 0.8 | 2.4 | 4.4 | 1.3 | 1.0 | 3.2 |

--Less than 0.05%.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 19**Identity theft victims who contacted an organization, by type of theft, type of organization, and credit bureau action, 2012**

| Organization | Total identity theft | Existing account | | | | New account | Personal information | Multiple types | | |
|---|----------------------|------------------|-------------|-------|-------|-------------|----------------------|----------------|-------------------------------|--------------------|
| | | Total | Credit card | Bank | Other | | | Total | Existing account ^a | Other ^b |
| Percent organization | | | | | | | | | | |
| Credit card company or bank | 86.0% | 89.6% | 93.8% | 93.0% | 46.7% | 64.8% | 26.4% | 86.9% | 92.0% | 77.2% |
| Federal Trade Commission (FTC) | 1.0 | 0.4 | 0.4! | 0.1! | 1.6! | 4.9! | 5.0! | 4.4 | 1.6! | 9.7! |
| Consumer agency ^c | 0.9 | 0.6 | 0.3! | 0.6 | 2.0! | 3.8! | 1.7! | 1.8! | 1.3! | 2.6! |
| Document issuing agency ^d | 2.7 | 1.2 | 1.2 | 1.3 | 1.0! | 5.2! | 21.3 | 8.8 | 8.9 | 8.4! |
| Credit monitoring service | 5.8 | 4.2 | 4.5 | 3.7 | 4.3 | 16.0 | 11.8 | 15.4 | 12.9 | 20.4 |
| Credit bureau ^e | 8.7 | 6.2 | 6.4 | 5.7 | 7.6 | 30.0 | 19.3 | 20.2 | 11.0 | 38.0 |
| Percent credit bureau | | | | | | | | | | |
| Placed a fraud alert on their credit report | 69.8 | 63.5 | 57.7 | 71.9 | 57.6 | 81.6 | 81.4 | 76.1 | 82.6 | 72.5 |
| Requested a credit report | 65.6 | 59.8 | 52.9 | 63.8 | 77.0 | 79.7 | 80.5 | 66.9 | 59.1 | 71.2 |
| Requested corrections to their credit report | 41.2 | 36.9 | 35.1 | 39.7 | 33.9! | 63.7 | 26.9! | 44.5 | 41.8! | 46.0 |
| Provided a police report to the credit bureau | 18.5 | 12.0 | 9.7 | 15.5 | 9.6! | 27.6 | 30.3! | 27.3 | 25.7! | 28.2 |
| Placed a freeze on their credit report | 37.8 | 35.1 | 27.4 | 45.2 | 32.2! | 45.4 | 28.9! | 45.2 | 53.4 | 40.6 |

Note: Estimates are based on the most recent identity theft incident. See appendix table 20 for standard errors.

^aIncludes victims who experienced two or more of the following: the unauthorized use of a credit card, bank account, or other existing account.^bIncludes victims who experienced two or more of the following: the unauthorized use of an existing account, misuse of personal information to open a new account, or misuse of personal information for other fraudulent purposes.^cIncludes government consumer affairs agencies and agencies such as the Better Business Bureau.^dIncludes agencies that issue drivers' licenses or Social Security cards.^ePercent of victims who took actions with a credit bureau, based on the number of victims who contacted a credit bureau. Details may sum to more than 100% because some respondents took multiple actions with the credit bureau.

! Interpret with caution; estimates based on 10 or fewer sample cases or coefficient of variation is greater than 50%.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 20**Standard errors for appendix table 19: Identity theft victims who contacted an organization, by type of theft, type of organization, and credit bureau action, 2012**

| Organization | Total identity theft | Existing account | | | | New account | Personal information | Multiple types | | |
|---|----------------------|------------------|-------------|------|-------|-------------|----------------------|----------------|------------------|-------|
| | | Total | Credit card | Bank | Other | | | Total | Existing account | Other |
| Percent organization | | | | | | | | | | |
| Credit card company or bank | 1.3% | 1.2% | 1.2% | 1.3% | 4.4% | 5.3% | 4.8% | 3.0% | 2.9% | 5.7% |
| Federal Trade Commission (FTC) | 0.2 | 0.1 | 0.2 | 0.1 | 0.9 | 2.1 | 2.2 | 1.5 | 1.1 | 3.6 |
| Consumer agency | 0.2 | 0.2 | 0.2 | 0.3 | 1.0 | 1.8 | 1.2 | 0.9 | 1.0 | 1.8 |
| Document issuing agency | 0.4 | 0.3 | 0.4 | 0.4 | 0.7 | 2.1 | 4.4 | 2.2 | 2.6 | 3.4 |
| Credit monitoring service | 0.6 | 0.6 | 0.8 | 0.7 | 1.5 | 3.8 | 3.4 | 2.9 | 3.1 | 5.1 |
| Credit bureau | 0.8 | 0.7 | 0.9 | 0.9 | 2.1 | 4.9 | 4.2 | 3.3 | 2.9 | 6.3 |
| Percent credit bureau | | | | | | | | | | |
| Placed a fraud alert on their credit report | 3.9 | 4.9 | 6.6 | 6.6 | 13.0 | 7.1 | 9.0 | 7.2 | 9.9 | 9.0 |
| Requested a credit report | 4.0 | 5.0 | 6.6 | 7.0 | 11.2 | 7.4 | 9.2 | 7.9 | 12.8 | 9.2 |
| Requested corrections to their credit report | 4.0 | 4.7 | 6.2 | 7.0 | 12.3 | 8.8 | 9.9 | 8.2 | 12.7 | 9.9 |
| Provided a police report to the credit bureau | 3.0 | 3.0 | 3.6 | 4.9 | 7.4 | 7.9 | 10.3 | 7.2 | 11.1 | 8.8 |
| Placed a freeze on their credit report | 3.9 | 4.7 | 5.7 | 7.1 | 12.1 | 8.9 | 10.2 | 8.2 | 12.9 | 9.7 |

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

APPENDIX TABLE 21**Standard errors for table 6: Actions victims and nonvictims took during the past 12 months to reduce the risk of identity theft, by whether the action was taken in response to the theft, 2012**

| Type of action | Percent of persons age 16 or older | | | | |
|--|------------------------------------|------------|-------------------------------|--|---|
| | Total | Nonvictims | Victim during prior 12 months | | |
| | | | Total | Action taken in response to identity theft | Action taken independently of identity theft in past year |
| Any | 0.6% | 0.7% | 0.7% | 1.0% | 1.4% |
| Checked credit report | 0.8 | 0.8 | 1.8 | 1.1 | 1.7 |
| Changed passwords on financial accounts | 0.7 | 0.7 | 1.8 | 1.4 | 1.6 |
| Purchased identity theft insurance/credit monitoring service | 0.3 | 0.3 | 1.0 | 0.6 | 0.7 |
| Shredded/destroyed documents with personal information | 0.8 | 0.8 | 1.5 | 1.0 | 1.7 |
| Checked bank or credit statements | 0.8 | 0.8 | 1.1 | 1.4 | 1.7 |
| Used identity theft security program on computer | 0.5 | 0.5 | 1.4 | 0.6 | 1.2 |
| Purchased identity theft protection | 0.2 | 0.2 | 0.7 | 0.5 | 0.4 |

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.



The Bureau of Justice Statistics, located in the Office of Justice Programs, U.S. Department of Justice, collects, analyses, and disseminates statistical information on crime, criminal offenders, victims of crime, and the operation of justice systems at all levels of government. William J. Sabol is acting director.

This report was written by Erika Harrell, Ph.D. and Lynn Langton, Ph.D. Shannan Catalano, Ph.D. verified the report. Agency partners for the Identity Theft Supplement (ITS) included Office for Victims of Crime, National Institute of Justice, and the Federal Trade Commission.

Vanessa Curto and Jill Thomas edited the report, and Barbara Quinn produced the report.

December 2013, NCJ 243779



EXHIBIT F

GAO

Report to Congressional Requesters

June 2007

PERSONAL INFORMATION

Data Breaches Are
Frequent, but
Evidence of Resulting
Identity Theft Is
Limited; However, the
Full Extent Is
Unknown



June 2007



Highlights of [GAO-07-737](#), a report to congressional requesters

Why GAO Did This Study

In recent years, many entities in the private, public, and government sectors have reported the loss or theft of sensitive personal information. These breaches have raised concerns in part because they can result in identity theft—either account fraud (such as misuse of credit card numbers) or unauthorized creation of new accounts (such as opening a credit card in someone else's name). Many states have enacted laws requiring entities that experience breaches to notify affected individuals, and Congress is considering legislation that would establish a national breach notification requirement.

GAO was asked to examine (1) the incidence and circumstances of breaches of sensitive personal information; (2) the extent to which such breaches have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements. To address these objectives, GAO reviewed available reports on data breaches, analyzed 24 large data breaches, and gathered information from federal and state government agencies, researchers, consumer advocates, and others.

What GAO Recommends

This report contains no recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-737.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David G. Wood at (202) 512-8678 or woodd@gao.gov.

PERSONAL INFORMATION

Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown

What GAO Found

While comprehensive data do not exist, available evidence suggests that breaches of sensitive personal information have occurred frequently and under widely varying circumstances. For example, more than 570 data breaches were reported in the news media from January 2005 through December 2006, according to lists maintained by private groups that track reports of breaches. These incidents varied significantly in size and occurred across a wide range of entities, including federal, state, and local government agencies; retailers; financial institutions; colleges and universities; and medical facilities.

The extent to which data breaches have resulted in identity theft is not well known, largely because of the difficulty of determining the source of the data used to commit identity theft. However, available data and interviews with researchers, law enforcement officials, and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft, particularly the unauthorized creation of new accounts. For example, in reviewing the 24 largest breaches reported in the media from January 2000 through June 2005, GAO found that 3 included evidence of resulting fraud on existing accounts and 1 included evidence of unauthorized creation of new accounts. For 18 of the breaches, no clear evidence had been uncovered linking them to identity theft; and for the remaining 2, there was not sufficient information to make a determination.

Requiring affected consumers to be notified of a data breach may encourage better security practices and help mitigate potential harm, but it also presents certain costs and challenges. Notification requirements can create incentives for entities to improve data security practices to minimize legal liability or avoid public relations risks that may result from a publicized breach. Also, consumers alerted to a breach can take measures to prevent or mitigate identity theft, such as monitoring their credit card statements and credit reports. At the same time, breach notification requirements have associated costs, such as expenses to develop incident response plans and identify and notify affected individuals. Further, an expansive requirement could result in notification of breaches that present little or no risk, perhaps leading consumers to disregard notices altogether. Federal banking regulators and the President's Identity Theft Task Force have advocated a notification standard—the conditions requiring notification—that is risk based, allowing individuals to take appropriate measures where the risk of harm exists, while ensuring they are only notified in cases where the level of risk warrants such action. Should Congress choose to enact a federal notification requirement, use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notifications of breaches that present little risk.

Contents

| | | |
|--------------------|--|----|
| Letter | | 1 |
| | Results in Brief | 5 |
| | Background | 7 |
| | Available Evidence Indicates That Data Breaches Occur Frequently and Under Varying Circumstances | 10 |
| | Consequences of Data Breaches Are Not Fully Known, but Clear Evidence of Identity Theft Has Been Found in Relatively Few Breaches | 21 |
| | Breach Notification Requirements Can Serve to Encourage Better Data Security Practices and Alert Consumers, but They Also Present Costs and Challenges | 31 |
| | Agency Comments | 40 |
| Appendix I | Scope and Methodology | 42 |
| Appendix II | GAO Contact and Staff Acknowledgments | 45 |
| | GAO Contact | 45 |
| | Staff Acknowledgments | 45 |
| Table | | |
| | Table 1: Twenty-Four Large Publicly Reported Data Breaches and Evidence of Resulting Identity Theft, January 2000 - June 2005 | 26 |
| Figure | | |
| | Figure 1: Application of Notification Standards under Different Breach Scenarios | 37 |

Abbreviations

| | |
|-------|---|
| DHS | Department of Homeland Security |
| FBI | Federal Bureau of Investigation |
| FDIC | Federal Deposit Insurance Corporation |
| FTC | Federal Trade Commission |
| SSN | Social Security number |
| USPIS | United States Postal Inspection Service |
| VA | Department of Veterans Affairs |

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

June 4, 2007

The Honorable Spencer Bachus
Ranking Member
Committee on Financial Services
House of Representatives

The Honorable Michael N. Castle
House of Representatives

The Honorable Darlene Hooley
House of Representatives

The Honorable Steven C. LaTourette
House of Representatives

The Honorable Dennis Moore
House of Representatives

As a result of advances in computer technology and electronic storage, many different sectors and entities now maintain electronic records containing vast amounts of personal information on virtually all American consumers. In recent years, a number of entities—including financial service firms, retailers, universities, and government agencies—have collectively reported the loss or theft of large amounts of sensitive personal information. Some of these data breaches—such as those involving TJX Companies and the Department of Veterans Affairs (VA)—have received considerable publicity and have highlighted concerns about the protections afforded sensitive personal information.¹ Policymakers, consumer advocates, and others have raised concerns that data breaches can contribute to identity theft, in which an individual's sensitive personal

¹In January 2007, The TJX Companies, Inc., publicly disclosed a data breach that compromised sensitive personal information, including credit and debit card data, associated with more than 45 million customer accounts. In May 2006, VA reported that computer equipment containing sensitive personal information on approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee. The equipment was eventually recovered, and forensic analysts concluded that it was unlikely that the personal information contained therein was compromised. See GAO, *Privacy: Lessons Learned About Data Breach Notification*, [GAO-07-657](#) (Washington, D.C.: Apr. 30, 2007).

information is used fraudulently. The Federal Trade Commission (FTC), which is responsible for taking complaints from victims and sharing them with law enforcement agencies, has noted that identity theft is a serious problem—millions of Americans are affected each year, and victims may face substantial costs and time to repair the damage to their good name and credit record.

Although there is no commonly agreed-upon definition, the term “data breach” generally refers to an organization’s unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers.² Data breaches can take many forms and do not necessarily lead to identity theft. The term “identity theft” is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else’s name. Depending on the type of information compromised and how it is misused, identity theft victims can face a range of potential harm, from the inconvenience of having a credit card reissued to substantial financial losses and damaged credit ratings.

Beginning with California in 2002, at least 36 states have enacted breach notification laws—that is, laws that require certain entities that experience a data breach to notify individuals whose personal information was lost or stolen. There is no federal statute that requires most companies or other entities to notify affected individuals of data breaches, although federal banking regulatory agencies have issued guidance on breach notification

²In this report we use “personally identifiable information” to refer to any information that can be used to distinguish or trace an individual’s identity—such as name, Social Security number, driver’s license number, and mother’s maiden name—because such information generally may be used to establish new accounts, but not to refer to other “means of identification,” as defined in 18 U.S.C. § 1028(7), including account information such as credit or debit card numbers.

to the banks, thrifts, and credit unions they supervise.³ In addition, the Office of Management and Budget has issued guidance—developed by the President’s Identity Theft Task Force—on responding to data breaches at federal agencies.⁴ Because a number of bills have been introduced in Congress that would establish a national breach notification requirement, you asked us to review the costs and benefits of such a requirement and the link between data breaches and identity theft.⁵ As agreed with your offices, this report examines (1) what is known about the incidence and circumstances of breaches of sensitive personal information; (2) what information exists on the extent to which breaches of sensitive personal information have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements.

This report focuses on breaches of sensitive personal data that can be used to commit identity theft, and not on breaches of other sensitive data, such as medical records or proprietary business information. To address the first two objectives, we obtained and analyzed information on data breaches that have been reported in the media and aggregated by three

³See Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (Mar. 29, 2005). The five federal banking regulatory agencies are the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the National Credit Union Administration. The National Credit Union Administration issued its guidance (which was substantially identical) separately from the other four regulators (see Security Program and Appendix B—Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, 70 Fed. Reg. 22764 (May 2, 2005)).

⁴The President’s Identity Theft Task Force—chaired by the Attorney General and cochaired by the Chairman of the Federal Trade Commission and comprising 17 federal agencies and departments—was charged with developing a comprehensive national strategy to combat identity theft. Exec. Order No. 13,402, *Strengthening Federal Efforts to Protect Against Identity Theft*, 71 Fed. Reg. 27945 (May 10, 2006). The task force’s guidance was distributed in a memorandum from the Office of Management and Budget to the heads of federal agencies and departments. See Office of Management and Budget Memorandum for the Heads of Departments and Agencies, *Recommendations for Identity Theft Related Data Breach Notification*, Sept. 20, 2006. In May 2007, the Office of Management and Budget issued a memorandum that updated the September 2006 guidance and, among other things, required agencies to develop and implement breach notification policies within 120 days. See Office of Management and Budget Memorandum for the Heads of Executive Departments and Agencies, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, M-07-16 (May 22, 2007).

⁵See, for example, Data Security Act of 2007, H.R. 1685, 110th Cong. (2007); Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007); Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007); and Identity Theft Prevention Act, S. 1178, 110th Cong. (2007).

private research and advocacy organizations, as well as information on breaches collected by state agencies in New York and North Carolina, federal banking regulators, and federal law enforcement agencies.⁶ We also collected information on breaches experienced by federal agencies compiled by the House Government Reform Committee in 2006 and by the Department of Homeland Security (DHS).⁷ In addition, we conducted a literature search of relevant articles, reports, and studies. We also conducted interviews with, and obtained documents from, representatives of federal agencies, including the FTC, the Department of Justice, DHS, and the federal banking regulatory agencies; selected state government agencies and the National Association of Attorneys General; private and nonprofit research organizations; and consumer protection and privacy advocacy groups. Further, we obtained information from industry and trade associations representing key sectors—including financial services, retail sales, higher education, health care, and information services—that have experienced data breaches. In addition, for the second objective, we examined the 24 largest (in terms of number of records breached) data breaches reported by the news media from January 2000 through June 2005 and tracked by private groups. For each of these breaches, we reviewed media reports and other publicly available information, and conducted interviews, where possible, with representatives of the entities that experienced the breaches, in an attempt to identify any known instances of identity theft that resulted from the breaches. We also examined five breaches that involved federal agencies, which were selected because they represented a variety of different circumstances. For the third objective, we reviewed the federal banking regulatory agencies' proposed and final guidance related to breach notification, and interviewed representatives of each agency regarding their consideration of potential costs, benefits, and challenges during development of the guidance. Further, we reviewed the strategic plan and other documents issued by the President's Identity Theft Task Force. In addition, we conducted a review of the effects of California's breach notification law, which included interviewing and gathering information from California

⁶The three private organizations are Attrition, Identity Theft Resource Center, and Privacy Rights Clearinghouse. We reviewed data on breaches in New York and North Carolina because they represent two large states that maintain centralized information on data breaches.

⁷The House Government Reform Committee was renamed the House Oversight and Government Reform Committee in the 110th Congress.

state officials and selected California companies, educational institutions, and other entities subject to the law's notification requirements.

We conducted our review from August 2006 through April 2007 in accordance with generally accepted government auditing standards. A more extensive discussion of our scope and methodology appears in appendix I.

Results in Brief

While comprehensive data do not exist, available evidence suggests that breaches of sensitive personal information have occurred frequently and under widely varying circumstances. For example, more than 570 data breaches have been reported in the news media from January 2005 through December 2006, according to our analysis of lists maintained by three private organizations that track such breaches. Further, a House Government Reform Committee survey of federal agencies identified more than 788 data breaches at 17 agencies from January 2003 through July 2006. Of the roughly 17,000 federally supervised banks, thrifts, and credit unions, several hundred have reported data breaches to their federal regulators over the past 2 years. In addition, officials in New York State—which requires public and private entities to report data breaches to a centralized source—reported receiving notice of 225 breaches from December 7, 2005, through October 5, 2006. Data breaches have occurred across a wide range of entities, including federal, state, and local government agencies; retailers; financial institutions; colleges and universities; and medical facilities. Some studies indicate that most publicly reported breaches resulted from intentional actions, such as a stolen laptop computer, rather than accidental occurrences, such as a lost laptop computer, but this may be because breaches related to criminal activity are perhaps more likely to be reported. Media-reported breaches have varied significantly in size, ranging from 10 records to tens of millions of records. Most of these breaches have compromised data that included personally identifiable information, while others have involved only account information such as credit card numbers.

The extent to which data breaches result in identity theft is not well known, in large part because it can be difficult to determine the source of the data used to commit identity theft. Although we identified several cases where breaches reportedly have resulted in identity theft—that is, account fraud or unauthorized creation of new accounts—available data and interviews with researchers, law enforcement officials, and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft. For example, our review of the 24 largest

breaches that appeared in the news media from January 2000 through June 2005 found that 3 breaches appeared to have resulted in fraud on existing accounts, and 1 breach appeared to have resulted in the unauthorized creation of new accounts. For 18 of the breaches, no clear evidence had been uncovered linking them to identity theft; and for the remaining 2, we did not have sufficient information to make a determination. Determining the link between data breaches and identity theft is challenging, primarily because identity theft victims often do not know how their personal information was obtained, and it may be up to a year or more before stolen data are used to commit a crime. Some studies by private researchers have found little linkage between data breaches and identity theft, although our review found these studies had methodological limitations. Finally, the circumstances of a breach can greatly affect the potential harm that can result. For example, unauthorized creation of new accounts generally can occur only when a breach includes personally identifiable information. Further, breaches that are the result of intentional acts generally are considered to pose more risk than accidental breaches, according to federal officials.

Requiring consumer notification of data breaches may encourage better data security practices and help deter or mitigate harm from identity theft, but it also involves monetary costs and challenges such as determining an appropriate notification standard. Representatives of federal banking regulators, other government agencies, industry associations, and other affected parties told us that breach notification requirements have encouraged companies and other entities to improve their data security practices to minimize legal liability or avoid public relations risks that may result from a publicized breach of customer data. Further, notifying affected consumers of a breach gives them the opportunity to mitigate potential risk—for example, by reviewing their credit card statements and credit reports, or placing a fraud alert on their credit files. Some privacy advocates and others have noted that even when the risk of actual financial harm is low, breach notification is still important because individuals have a basic right to know how their personal information is being handled and when it has been compromised. At the same time, affected entities incur monetary costs to comply with notification requirements. For example, 31 companies that responded to a 2006 survey said they incurred an average of \$1.4 million per breach, for costs such as mailing notification letters, call center expenses, courtesy discounts or services, and legal fees. In addition, organizations subject to notification requirements told us they face several challenges, including the lack of clarity in some state statutes about when a notification is required, difficulty identifying and locating affected individuals, and difficulty

complying with varying state requirements. Notification standards—that is, the circumstances surrounding a data breach that “trigger” the required notification—vary among the states. Some parties, such as the National Association of Attorneys General, have advocated that a breach notification requirement should apply broadly in order to give consumers a greater level of protection and because the risk of harm is not always known. The guidance provided by federal banking regulators lays out a more risk-based approach, aimed at ensuring that affected individuals receive notices only when they are at risk of identity theft or other related harm. Such an approach was also adopted by the President’s Identity Theft Task Force, which recommended a risk-based standard for breach notification applicable to both government agencies and private entities. As we have noted in the past, care is needed in defining appropriate criteria for incidents that merit notification. Should Congress choose to enact a federal breach notification requirement, use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notifications of breaches that present little risk.

This report contains no recommendations. We provided a draft of this report to FTC and provided selected portions of the draft to federal banking regulatory agencies and relevant federal law enforcement agencies. These agencies provided technical comments, which we have incorporated in this report as appropriate.

Background

Breaches of sensitive personal data in recent years at companies, universities, government agencies, and other organizations have heightened public awareness about data security and the risks of identity theft, and have led to the introduction of breach notification requirements in many state legislatures. As of April 2007, at least 36 states had enacted some form of law requiring that affected individuals be notified in the event of a data breach; California’s law, enacted in 2002, was the first such state requirement.⁸ States’ notification requirements vary, particularly with regard to the applicable notification standard—the event or circumstance that triggers a required notification. Requirements also vary in terms of the data to which they apply—for example, some apply to paper documents as well as electronic records.

⁸Cal. Civ. Code § 1798.82.

There is currently no federal statute that requires most companies and other entities that experience a data breach to notify individuals whose personal information was lost or stolen. However, the Gramm-Leach-Bliley Act established requirements for federally supervised financial institutions to safeguard customer information.⁹ To clarify these requirements, the federal banking regulators issued interagency guidance in 2005 to the banks, thrifts, and credit unions they supervise related to their handling of data breaches. Under this guidance, these institutions are expected to develop and implement a response program to address unauthorized access to customer information maintained by the institution or its service providers; and if they experience a breach, they are to notify their primary federal regulator as soon as possible and—depending on the circumstances of the incident—notify their affected customers. In addition, in September 2006 the President’s Identity Theft Task Force developed guidance for federal agencies on responding to breaches involving agency data, including the factors to consider in determining whether to notify affected individuals. The task force released a strategic plan for combating identity theft in April 2007, which contained among its recommendations a proposal for establishing a national breach notification requirement.¹⁰ Further, in December 2006, the Department of Veterans Affairs Information Security Enhancement Act of 2006 became law, which, among other things, requires VA to prescribe regulations providing for the notification of data breaches occurring at the department.¹¹ A number of bills have been introduced in Congress that would more broadly require companies and other entities to notify

⁹Pub. L. No. 106-102, tit. V, subtit. A, 113 Stat. 1338 (Nov. 12, 1999) (*codified at* 15 U.S.C. § 6801-6809).

¹⁰President’s Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* (Washington, D.C.: Apr. 11, 2007).

¹¹Pub. L. No. 109-461, tit. IX, 120 Stat. 3450 (Dec. 22, 2006), *codified at* 38 U.S.C. § 5721-5728, 7901-7907.

individuals when such breaches occur, and Congress has held several hearings related to data breaches.¹²

Identity theft occurs when individuals' identifying information is used without authorization in an attempt to commit fraud or other crimes.¹³ There are two primary forms of identity theft. First, identity thieves can use financial account identifiers, such as credit card or bank account numbers, to take over an individual's existing accounts to make unauthorized charges or withdraw money. Second, thieves can use identifying data, which can include such things as SSNs and driver's license numbers, to open new financial accounts and incur charges and credit in an individual's name, without that person's knowledge. This second form of identity theft is potentially the most damaging because, among other things, it can take some time before a victim becomes aware of the problem, and it can cause substantial harm to the victim's credit rating. While some identity theft victims can resolve their problems quickly, others face substantial costs and inconvenience repairing damage to their credit records. According to FTC, millions of Americans have their identities stolen each year. Roughly 85 percent of these cases involve the misuse of existing accounts and 35 percent involve new account creation or other fraud. (Twenty percent of the total involve both.) Identity thieves obtain sensitive personal information using a variety of methods. One potential source is a breach at an organization that maintains large amounts of sensitive personal information. However, identity theft can also occur as a result of the loss or theft of data maintained by an individual, such as a lost or stolen wallet or a thief digging through household trash.

¹²For example, *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before the Senate Comm. on Banking, Housing, and Urban Affairs*, 109th Cong., 1st Sess. (2005); *Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use: Hearing Before the Senate Comm. on the Judiciary*, 109th Cong., 1st Sess. (2005); *Assessing Data Security: Preventing Breaches and Protecting Sensitive Information: Hearing Before the House Comm. on Financial Services*, 109th Cong., 1st Sess. (2005); *Securing Consumers' Data: Options Following Security Breaches: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the House Comm. on Energy and Commerce*, 109th Cong., 1st Sess. (2005).

¹³For additional information on identity theft, see GAO, *Identity Theft: Some Outreach Efforts to Promote Awareness of New Consumer Rights Are Under Way*, [GAO-05-710](#) (Washington, D.C.: Jun. 30, 2005) and *Identity Theft: Prevalence and Cost Appear to be Growing*, [GAO-02-363](#) (Washington, D.C.: Mar. 1, 2002).

The Identity Theft and Assumption Deterrence Act of 1998 made identity theft a federal crime and charged FTC with taking complaints from identity theft victims; sharing these complaints with federal, state, and local law enforcement agencies; and providing the victims with informational materials to assist them.¹⁴ Because identity theft is typically not a stand-alone crime but rather a component of one or more crimes such as bank fraud, credit card fraud, and mail fraud, a number of federal law enforcement agencies can have a role in investigating identity theft crimes, including the Federal Bureau of Investigation (FBI), U.S. Postal Inspection Service (USPIS), U.S. Secret Service (Secret Service), the Office of the Inspector General of the Social Security Administration, and Immigration and Customs Enforcement.

Available Evidence Indicates That Data Breaches Occur Frequently and Under Varying Circumstances

Available evidence from media reports, federal and state agencies, and private institutions, collectively, suggests that data breaches occur with some frequency. For example, our analysis of the lists of data breaches compiled by three private research and advocacy organizations shows more than 570 breaches reported by the news media from January 2005 through December 2006. Data breaches have occurred across a range of entities, including federal, state, and local government agencies; retailers; financial institutions; colleges and universities; and medical facilities. Breaches have varied in size and have resulted from both criminal actions and accidental incidents. Most of the breaches reported in the news media have involved data that included personal identifiers such as SSNs, while others have involved only account information such as credit card numbers.

Several Sources Indicate That Breaches of Sensitive Personal Information Are Frequent

No federal agency or other organization tracks all data breaches, and definitions of what constitutes a data breach may vary. Although there are no comprehensive data on the extent of data breaches nationwide, government officials, trade association representatives, researchers, and consumer and privacy advocates we interviewed agreed that breaches of sensitive personal information occur frequently. For example, representatives of a variety of organizations—including the Department of

¹⁴Pub. L. No. 105-318, 112 Stat. 3007 (Oct. 30, 1998). In addition to FTC, other federal agencies maintain data on identity theft. For example, the Internet Crime Complaint Center, a joint venture of the FBI and the National White Collar Crime Center, receives Internet-related identity theft complaints, which it shares with law enforcement agencies throughout the country.

Justice, California's Office of Privacy Protection, the Consumer Data Industry Association (a trade group representing many information resellers), and the Ponemon Institute (a private research organization)—characterized data breaches in the United States as being “prevalent” or “common.” Although we did not identify comprehensive data on the extent of data breaches, available information from several sources does corroborate the anecdotal evidence that such breaches occur frequently.¹⁵

Media Reports

Over the past few years, several hundred data breaches have been reported each year by newspapers and other news media. Three private organizations that focus on information privacy and security issues—Privacy Rights Clearinghouse, Identity Theft Resource Center, and Attrition—track data breaches reported in newspapers, magazines, and other publicly available sources of news and information.¹⁶ Our analysis of the three lists of data breaches maintained by these organizations indicated that at least 572 breaches were reported in the news media from January 2005 through December 2006.¹⁷ These breaches were reported to

¹⁵Because the breaches cited in this section of the report derive from different sources, there may be some overlap among the numbers cited by these sources.

¹⁶Privacy Rights Clearinghouse is a nonprofit consumer education and advocacy project whose purpose is to advocate for consumers' privacy rights in public policy proceedings. Identity Theft Resource Center is a nonprofit organization that provides consumer and victim support and advises governmental agencies, legislators, and companies on the issue of identity theft. Attrition is an information security-related Web site maintained by volunteers.

¹⁷Representatives of these three organizations indicated that their definition of a data breach was consistent with the definition used in this report. However, we did not independently confirm whether the individual breaches reported by the media and tracked by these groups met the criteria for this definition, and it is possible that some of them do not. We reviewed these lists as they appeared as of February 15, 2007; additional breaches that occurred during the 2-year period we reviewed may have been subsequently added as they were discovered. Our analysis eliminated overlap among the three lists; the 572 breaches we cite represent unique breaches that appeared on at least one list.

have affected more than 80 million records.¹⁸ However, for several reasons, these lists likely understate the true extent of data breaches in the United States. First, organizations might not voluntarily disclose data breaches that they experience. Second, some breaches that organizations do disclose may not appear in the news media, particularly if the breach was limited in scope. Finally, the three organizations compiling these lists may not have identified all of the breaches reported in the news media—for example, many breaches did not appear on all three lists, suggesting that none represents an exhaustive list of all breaches that have appeared in the news.

Federal Law Enforcement Agencies

Officials at federal law enforcement agencies told us that each year they conduct a significant number of criminal investigations that involve alleged breaches of sensitive personal information. For example, officials of the FBI's Cyber Division told us that presently it has more than 1,300 pending cases of computer or network intrusions where data breaches resulted from unauthorized electronic access to computer systems, such as hackings, at public and private organizations.¹⁹ Officials at the Secret Service, which investigates certain cases where financial information has been lost or stolen, told us that in 2006, the service opened 327 cases involving network intrusions or other breaches at retailers, banks, credit card processors, telephone companies, educational institutions, and other organizations. Officials noted that they have seen a steady increase in the number of data breaches since 1986, when they began tracking computer fraud violations. Investigators at USPIS, the division of the U.S. Postal

¹⁸There were 83 million records collectively reported to have been affected by the 572 breaches. However, in some cases, the number of records affected was unknown or unreported, and the total does not reflect those breaches. Also, the number of breached records containing personal information may not be the same as the number of individuals affected by breaches because some individuals may be victims of more than one breach or may have multiple records compromised in a single breach. Finally, in addition to the 83 million records, as many as 40 million additional records may have been affected by a single breach involving the credit card processor CardSystems, although the exact number of affected records is unclear. In a complaint following the breach, FTC alleged that a hacker obtained unauthorized access to magnetic stripe data for tens of millions of credit and debit cards. However, according to testimony by a CardSystems official, only 263,000 of these records (containing 239,000 discrete account numbers) included sensitive personal information.

¹⁹According to these officials, not all 1,300 pending computer intrusion cases necessarily involved breaches that compromised sensitive personal information, although the vast majority have. The term hacking is commonly used to refer to accessing a computer system without authorization, with the intention of destroying, disrupting, or carrying out illegal activities on the network or computer system.

House Government Reform
Committee and DHS

Service that investigates mail fraud, external mail theft, fraudulent changes of addresses, and other postal-related crimes, told us that the agency does not specifically track the number of data breaches in the private sector. However, despite limited data, investigators said their impression is that such data breaches likely occur frequently.

To obtain information on the prevalence of data breaches at federal agencies, in July 2006 the House Government Reform Committee asked federal agencies to provide details about incidents involving the loss or compromise of any sensitive personal information held by an agency or contractor from January 1, 2003, through July 10, 2006. Our analysis of the committee's report found that 17 agencies reported that they experienced at least one breach and, collectively, the agencies reported to the committee more than 788 separate incidents.²⁰

The Federal Information Security Management Act of 2002 requires all federal agencies to report computer security incidents to a federal incident response center.²¹ The U.S. Computer Emergency Readiness Team—a component of DHS that monitors computer security incidents at federal agencies—serves as this response center. As such, data breaches at federal agencies involving certain sensitive information must be reported to the

²⁰Government Reform Committee, U.S. House of Representatives, *Staff Report: Agency Data Breaches Since January 1, 2003* (Washington, D.C.: Oct. 13, 2006). The federal agencies covered in the report were the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, and Veterans Affairs, as well as the Office of Personnel Management and the Social Security Administration. In addition to 788 incidents reported by 16 federal agencies, the Committee received information on data breaches from the Department of Veterans Affairs, which the report characterized only as “hundreds” of incidents.

²¹Pub. L. No. 107-347, tit. III, 116 Stat. 2946 (Dec. 17, 2002), *codified at* 44 U.S.C. § 3541-3549; 40 U.S.C. § 11331.

team within 1 hour of discovery of the incident.²² DHS staff told us that they receive information about breaches at federal agencies on a daily basis. In fiscal year 2006, the center tracked 477 incidents at 59 federal agencies or at federal contractors with access to government-owned data, according to information available as of January 29, 2007. In addition, a March 2007 audit investigation found that at least 490 laptop computers owned by the Internal Revenue Service and containing taxpayer information had been lost or stolen since 2003.²³

Federal Banking Regulators

The 2005 guidance issued by the five federal banking regulators provided that a depository institution should notify its primary federal regulator when it becomes aware of an incident involving unauthorized access to or use of sensitive customer information.²⁴ The guidance applies to breaches that have occurred at the financial institutions themselves, as well as third-party entities such as data processors that act as service providers and maintain customer information.²⁵ The five regulators differ in their methods and criteria for tracking breaches, but collectively they have tracked several hundred breaches over the past few years at roughly

²²Office of Management and Budget Memorandum for Chief Information Officers, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, M-06-19 (July 12, 2006). The U.S. Computer Emergency Readiness Team defines a computer security incident as “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practice” and the Office of Management and Budget requires reporting if the incident includes personally identifiable information, which under its definition refers to “any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual’s identity, such as their name, Social Security number, date and place of birth, mother’s maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.”

²³Treasury Inspector General for Tax Administration, *The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices*, Ref. No. 2007-20-048 (Washington, D.C.: Mar. 23, 2007).

²⁴70 Fed. Reg. 15736 (Mar. 29, 2005) and 70 Fed. Reg. 22764 (May 2, 2005).

²⁵Only data breaches at the financial institutions and at third-party entities that are their service providers and maintain their customer information are subject to the guidance; this requirement is codified at 12 C.F.R. Pt. 30, App. B, Supp. A § II(A)(2); 12 C.F.R. Pt. 208, App. D-2, Supp. A § II(A)(2); 12 C.F.R. Pt. 225, App. F, Supp. A § II(A)(2); 12 C.F.R. Pt. 364, App. B, Supp. A § II(A)(2); 12 C.F.R. Pt. 570, App. B, Supp. A § II(A)(2); and 12 C.F.R. Pt. 748, App. B § II(A)(2). However, data collected by the regulators may also include some breaches that affected their institutions but were not covered by the guidance.

17,000 institutions they supervise and at third-party entities.²⁶ For example, the Federal Deposit Insurance Corporation (FDIC)—the primary federal supervisor for more than 5,000 state-chartered banks that are not members of the Federal Reserve System—received reports of 194 breaches at its regulated institutions from May 2005 through December 2006, as well as reports of 14 breaches at third-party companies that also affected these institutions' customers. Similarly, officials at the Office of Thrift Supervision—which supervises more than 860 savings associations—told us that from April 2005 through December 2006, 56 of its institutions reported breaches at the institution itself and approximately 72 reported breaches at third-party entities that maintained their customer information.

State Agencies

Some states require entities experiencing data breaches to report them to designated state agencies.²⁷ For example, the New York State Information Security Breach and Notification Act requires entities that experience security breaches to notify the state Attorney General's Office, Consumer Protection Board, and the state Office of Cyber Security and Critical Infrastructure Coordination in cases when New York residents must be notified.²⁸ Such data breaches include the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of unencrypted private information. Officials of the Office of New York State Attorney General told us that from December 7, 2005, through October 5, 2006, their office received notice of 225 breaches. Similarly, a North Carolina law requires that breaches of personal information (maintained in computerized, paper, or other media) affecting at least 1,000 persons be reported to the Consumer Protection Division of the state Office of the Attorney General.²⁹ An official in that office told us that from December 2005 through December 2006, it had received reports of 91 breach incidents.

²⁶Regulators note that while they track breaches occurring at third-party service providers involving customer information of regulated financial institutions, these breaches are typically due to lapses in data security by the third-party entity and not the financial institution itself.

²⁷We did not determine the precise number of states with centralized reporting requirements. For illustrative purposes, we obtained information on data breaches from New York and North Carolina because they are two large states known to require that data breaches be reported to state agencies.

²⁸N.Y. Gen. Bus. Law § 899-aa.

²⁹N.C. Gen. Stat § 75-65.

Other Sources

Information that we obtained from several other sources suggests that breaches of sensitive personal information occur with some frequency across a variety of sectors. For example,

- EDUCAUSE, a nonprofit association that addresses technology issues in higher education, conducted a survey in 2005 on data security at higher education institutions in the United States and Canada. Twenty-six percent of the 490 institutions that responded said they had experienced a security incident in the past year that resulted in the compromise of confidential information.³⁰
- The American Hospital Association collected information, at our request, in October 2006 from a nonrepresentative group of 46 large hospitals on breaches of sensitive personal information (excluding medical records) that they had experienced since January 2003. Collectively, 13 of the 46 hospitals reported a total of 17 data breach incidents.³¹
- The Ponemon Institute, a private company that researches privacy and security practices, conducted a survey of 51,433 U.S. adults and received responses from 9,154 (a response rate of about 18 percent). About 12 percent of the survey respondents said they recalled receiving notification of a data security breach involving their personal information.³²
- The CMO Council, an organization serving marketing executives, reported that 16 percent of consumers who responded to a Web-based panel reported that a company had lost or compromised their personal,

³⁰EDUCAUSE Center for Applied Research, *Safeguarding the Tower: IT Security in Higher Education 2006*, Volume 6, 2006.

³¹The association received information from 46 of the 78 hospitals it surveyed, a response rate of 59 percent. As agreed in advance, to preserve confidentiality the association provided us with a summary of their findings but did not identify the hospitals, and we did not independently verify the data.

³²Ponemon Institute, LLC, *National Survey on Data Security Breach Notification* (Sept. 26, 2005). The reliability of this study's findings may be limited by a low survey response rate.

financial, or medical information. An additional 32 percent of respondents said they were not sure.³³

- Several other studies, while not focusing specifically on breaches of sensitive personal information, have found more generally that information security vulnerabilities are widespread among U.S. and global companies.³⁴

Information from multiple sources indicates that data breaches at companies, government agencies, retailers, and other entities have occurred frequently in recent years, involving millions of records of sensitive personal information. We have reported in the past that no federal law explicitly requires most companies and other entities to safeguard all of the sensitive personal information they may hold. We also have suggested that to ensure that sensitive personal information is protected on a more consistent basis, Congress should consider expanding requirements to safeguard such information.³⁵ The frequency of data breaches identified in this report underscores the need for entities in the public and private sectors to improve the security of sensitive personal information and further corroborates that additional federal action may be needed in this area.

Source, Cause, Size, and Content of Breaches Have Varied Widely

According to government officials, researchers, and media reports, data breaches have occurred among a wide variety of entities and as a result of both intentional actions and accidental losses. These breaches also have varied in size and in the types of data compromised.

Type of Entity

Data breaches have been reported at a wide range of public and private institutions, including federal, state, and local government agencies; public

³³CMO Council, *Securing the Trust of Your Brand: How Security and IT Integrity Influence Corporate Reputation*, September 2006. The reliability of this study's findings may be limited because they are based on a self-selected group of respondents to a Web-based panel. Also, we were unable to determine a response rate because, according to a CMO Council representative, the total number of survey respondents was not available.

³⁴For example, see Deloitte, *2006 Global Security Survey* (2006); Small Business Technology Institute, *Small Business Information Security Readiness* (San Jose, California: July 2005); Ponemon Institute, LLC, *U.S. Survey: Confidential Data at Risk* (Aug. 15, 2006); and Ponemon Institute, LLC, *Benchmark Study of European and U.S. Corporate Privacy Practices* (Apr. 26, 2006).

³⁵GAO, *Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data*, [GAO-06-674](#) (Washington, D.C.: Jun. 26, 2006).

and private colleges and universities; hospitals and other medical facilities; retailers; banks and other financial institutions; information resellers; and others. For example, in the weeks leading up to the highly publicized 2005 CardSystems breach, the media also had reported breaches at, among other entities, a large hospital, a university, a global financial institution, a federal regulatory agency, and a major technology company.

According to Attrition, of the breaches it tracked as reported in the news media in 2005 and 2006, 33 percent of the breaches occurred at educational institutions, 32 percent at financial services institutions, 25 percent at government agencies, and 10 percent at medical facilities, although breaches reported in the news media may not be representative of all breaches.³⁶ Similarly, the data security firm ID Analytics examined 70 data breaches that were reported by the news media from February through September 2005. According to company officials, 46 percent of these breaches occurred at educational institutions, 16 percent at financial institutions, 14 percent at retailers, 11 percent at government agencies, 7 percent at medical facilities, and 6 percent at information resellers.³⁷

Another way to analyze where data breaches have occurred is to look at the number of *records* breached (as opposed to the number of breaches themselves). Our analysis of the list maintained by Attrition found that 54 percent of breached records involved financial institutions, 34 percent involved government agencies, 4 percent involved educational institutions, and 3 percent involved medical facilities. ID Analytics' report found that 57 percent of breached records involved financial institutions, 22 percent involved retailers, 13 percent involved educational institutions, 4 percent involved information resellers, 2 percent involved government agencies, and 2 percent involved medical facilities.

Cause of Breach

According to government officials, researchers, and media reports, data breaches of sensitive personal information have occurred as a result of both intentional actions as well as negligence or accidental losses. In some cases, individuals intentionally steal information for the purpose of

³⁶For our analysis, we used the categories provided by Attrition for the industry sector where the breach occurred. We did not independently verify the accuracy of these categorizations.

³⁷ID Analytics, Inc., *National Data Breach Analysis* (San Diego, California: January 2006). The data we cite reflect a combination of data presented in the report and additional data provided to us by ID Analytics.

committing fraud or identity theft. Breaches involving intentional actions have included:

- *Hacking*, or accessing computer systems without authorization. For example, in 2007 the retailer TJX Companies reported unauthorized intrusions into its computer systems that may have breached millions of customers' credit card and driver's license information.
- *Employee theft*. For example, in 2006, a former employee of the American Red Cross pled guilty to stealing personally identifiable information from a blood donor database.
- *Theft of physical equipment*. In 2005, for instance, a laptop containing the names and SSNs of more than 98,000 students, alumni, and others was stolen from the University of California at Berkeley.
- *Deception or misrepresentation to obtain unauthorized data*. In 2005, the information reseller ChoicePoint acknowledged that the personal records it held on approximately 162,000 consumers had been compromised by individuals who posed as legitimate subscribers to the company's information services.

Breaches involving negligence or accidental losses of data have included the following:

- *Loss of laptop computers or other hardware*. For example, in 2006, the Department of Labor reported that an employee lost a laptop containing personal information on 1,137 individuals.
- *Loss of data tapes*. For example, in 2004, Bank of America lost backup tapes containing personal information of 1.2 million government charge card holders while the tapes were being transported to a data center.
- *Unintentional exposure on the Internet*. In 2006, according to media reports, the U.S. Department of Education left unprotected on a Web site the personally identifiable information, including SSNs, of up to 21,000 recipients of federal student loans.
- *Improper disposal of data*, such as leaving sensitive personal data on unshredded documents in a publicly accessible dumpster.

We did not identify comprehensive data that reliably provide overall statistics on the causes of known data breaches. However, our review of the 24 largest data breaches reported in the news media (discussed in

more detail later in this report) found that 12 breaches apparently involved intentional acts by hackers or employees illegally accessing or using data, 5 involved stolen laptops or other computer equipment, 4 involved lost computer backup tapes, 2 involved the use of deception to gain access to data, and 1 involved the possible unauthorized disclosure of data. In addition, some studies indicate that most breaches reported in the news media resulted from intentional acts rather than accidental occurrences such as a lost laptop computer. For example, in its study of 70 breaches, ID Analytics determined that 48 involved thefts committed with the apparent intention of accessing sensitive data. Eleven of the breaches involved thefts where sensitive consumer information was apparently stolen inadvertently as part of another crime (such as the theft of a laptop computer for its resale value), and another 11 breaches involved accidental loss (such as misplacement of a laptop computer). However, these data may overrepresent the proportion of all breaches that involve criminal activity, as such breaches are probably more likely than accidental losses to be reported to authorities and by the news media.

Number of Records Breached

Our analysis of the list maintained by Attrition of breaches reported by the news media found the median number of records breached to be 8,650. However, these data breaches varied considerably in size—ranging, for example, from a breach involving 10 records at a law firm to a breach involving as many as tens of millions of records at a credit card processing company. The breaches involving federal agencies that were reported to the House Government Reform Committee also varied in size—for example, several affected fewer than five records, while a breach at VA affected 26.5 million records.

Types of Data Breached

Comprehensive information does not exist on the types of data involved in all known data breaches. Among the list maintained by Attrition of breaches reported by the news media in 2005 and 2006—which may not be representative of all breaches—more than half involved SSNs and 11 percent involved credit card numbers (and 3 percent of the total involved both). In the remaining breaches, other types of account or personal information were involved, or the type of data breached was not reported. Logically, there may be an association between the type of data compromised and the type of entity experiencing the breach. For example, several educational institutions have experienced breaches of SSNs, which they may maintain as student identifiers, and several retail stores have experienced breaches of credit card numbers, which they often maintain on their customers.

Consequences of Data Breaches Are Not Fully Known, but Clear Evidence of Identity Theft Has Been Found in Relatively Few Breaches

Comprehensive information on the outcomes of data breaches is not available. Several cases have been identified in which a data breach appears to have resulted in identity theft, but available data and information from law enforcement and industry association representatives indicated that most breaches have not resulted in detected incidents of identity theft. For example, of 24 very large breaches we reviewed, 3 appeared to have resulted in fraud on existing accounts and 1 in the unauthorized creation of new accounts. Determining the link between data breaches and identity theft is challenging because, among other things, identity theft victims often do not know how their personal information was obtained. However, the circumstances of a breach, including the type of information compromised and how the breach occurred, can greatly affect the potential risk of identity theft.

Federal Law Enforcement Agencies and Industry Associations Identified Limited Instances of Breaches Leading to Identity Theft

In general, representatives of law enforcement agencies, industry and trade associations, and consumer and privacy advocacy organizations told us that no comprehensive data are available on the consequences of data breaches. Several cases have been identified where there is evidence that a data breach resulted in identity theft, including account fraud or unauthorized creation of new accounts. At the same time, available data and information from the officials we contacted indicated that most breaches have not resulted in detected incidents of identity theft.

We asked representatives of the FBI, Secret Service, USPIS, and Immigration and Customs Enforcement—a component of DHS that has investigated cases where stolen identities were used to secure jobs—the extent to which data breaches they investigated resulted in some form of identity theft. Representatives of all of these agencies told us that their investigations of data breaches do not typically allow them to fully ascertain how stolen data are used. Similarly, they noted that investigations of identity theft do not always reveal the source of the data used to commit the crime.

However, the representatives were able to provide us with a limited number of examples in which data breaches they investigated had allegedly resulted in some form of identity theft. For example, in a 2006 investigation by USPIS, an employee of a credit card call center allegedly compromised at least 35 customers' accounts and used some of the information to purchase approximately \$65,000 in gift cards. The representatives of federal law enforcement agencies noted that cases in which data breaches have been linked to identity theft often have involved instances of unauthorized access by employees. For example, an official at

Immigration and Customs Enforcement stated that her agency, in cooperation with other agencies, has investigated cases in which government employees allegedly had improperly accessed and sold sensitive personal information that was then used by illegal immigrants to secure employment.

In addition, in 2005 FTC settled charges with BJ's Wholesale Club in which alleged security breaches resulted in several million dollars in fraudulent purchases using customers' credit and debit card data.³⁸ As discussed later in this report, FTC has also taken enforcement actions related to data breaches at several other companies, including ChoicePoint, CardSystems, and DSW, in which it uncovered evidence that the breaches resulted in identity theft.

Many of the law enforcement officials said that, based on their experience, data breaches that result in harm have usually involved fraud on existing accounts (such as credit card fraud) rather than the unauthorized creation of new accounts. Secret Service representatives noted that using illicit credit and debit card numbers and bank account information is much easier and less labor intensive than using personally identifiable information to fraudulently open new accounts. Officials at Secret Service, FBI, and USPIS all said that identity theft involving the creation of new accounts often results not from data breaches, but from other sources, such as retrieving personal information by sifting through a family's household trash.

In examining a selection of five breaches that occurred from 2003 through 2005 that were reported as having involved five federal agencies—Department of Justice, FDIC, Internal Revenue Service, National Park Service, and the Navy—we found that the circumstances behind these breaches varied widely. At least two of the breaches occurred at vendors or contractors that held sensitive data on agency employees, rather than at the agency itself. In addition, we found that a breach reported in the news media as having involved the National Park Service actually involved a not-for-profit organization that manages eParks, according to a representative of that organization. Four of the five breaches reported as having involved federal agencies were not believed to have resulted in identity theft, according to officials of the entities involved. The breach at

³⁸*In the Matter of BJ's Wholesale Club, Inc.*, F.T.C. No. 0423160 (2005). A consent agreement does not constitute an admission of a violation of law.

FDIC resulted in an estimated 27 cases of identity theft when data inappropriately accessed by a former FDIC intern were used to take out more than \$425,000 in fraudulent loans in the names of FDIC employees, according to agency officials.³⁹

Industry and trade associations representing entities that maintain large amounts of information—banks, retailers, colleges, information resellers, and hospitals—told us that they had limited knowledge about the harm caused by data breaches that occur in their industries. However, in some cases, they provided information or anecdotal evidence on the extent to which such breaches may have led to some form of identity theft. For example, the 46 hospitals that the American Hospital Association surveyed at our request reported that of 17 breaches that had occurred since 2003, three had resulted in fraudulent activity on existing accounts and another three resulted in other forms of identity theft, including one case where the information was used to file false income tax refunds. The identity theft in these cases involved small numbers of victims—usually just one.

Representatives of the American Council on Education and two other higher education associations stated that while data breaches at colleges and universities were not uncommon, they were aware of little to no identity theft that had resulted from such breaches. Representatives of the American Bankers Association, the National Retail Federation, and the Consumer Data Industry Association told us they were unable to determine how prevalent data breaches are among their institutions or how often such breaches lead to consumer harm. Representatives at the National Retail Federation noted that breaches at retailers may be more likely to result in fraud on existing accounts than in new account creation, since most retailers do not maintain the personally identifiable information needed to steal someone's identity.

³⁹According to an FDIC representative, the agency took several steps to address the possible misuse of employee information, including promptly notifying affected employees and offering them 2 years of credit monitoring services.

Of 24 Large Publicly Reported Breaches, 4 Apparently Resulted in Known Cases of Identity Theft

Using lists of data breaches compiled by the Identity Theft Resource Center, Privacy Rights Clearinghouse, and Congressional Research Service, we identified the 24 largest breaches (measured by number of records) that were reported in the news media from January 2000 through June 2005.⁴⁰ To gather information on these incidents, we interviewed or collected written responses from representatives of the entity experiencing the breach and reviewed publicly available information, such as media reports, news releases, testimonies, and court documents. In some cases, when feasible, we also spoke with law enforcement investigators. We identified those cases where this information collectively indicated that the breach appeared to have resulted in some form of identity theft. Ultimately, the determination of whether particular conduct violated a law prohibiting identity theft would be a matter of law for the courts.

Although these lists characterized each of these 24 incidents as data breaches, the circumstances of the incidents varied. While 19 of the incidents clearly met our definition of data breach (i.e. unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information), four cases involved hackers who may or may not have actually accessed sensitive information. In one other incident, a university employee with access to sensitive personal data was indicted on unrelated fraud charges. A university official told us he did not believe this incident should necessarily be characterized as a data breach since there was no evidence the employee actually misused university data.

The available evidence that we reviewed indicated that 18 of these 24 breaches were not known to have resulted in any identity theft. As shown in table 1, three breaches were believed to have resulted in account fraud and one resulted in the unauthorized creation of new accounts. In two

⁴⁰These three organizations periodically update their lists by adding breaches they learn about that occurred in the past, including some that occurred between January 2000 and June 2005. Our list of the 24 largest media-reported breaches was based on information provided by these lists as of August 2006. We were not aware of the Attrition list at the time we made our selection. See Congressional Research Service, *Personal Data Security Breaches: Context and Incident Summaries*, Order Code RL33199 (Washington, D.C.: Dec. 16, 2005). Because our time frame covered only breaches that occurred on or before June 30, 2005, our list does not include highly publicized breaches that occurred subsequently, such as those involving the Department of Veterans Affairs and the TJX Companies. Several banks have reported fraudulent transactions on existing accounts resulting from the TJX breach, according to a January 24, 2007, press release by the Massachusetts Bankers Association.

other cases, we were not able to gather sufficient information on whether harm appeared to have resulted from the breach. Further, because of the challenges in linking data breaches with identity theft, in some cases our review may not have uncovered instances of harm potentially resulting from these breaches. In some instances, investigators or company representatives reported that they were able to determine with a high degree of certainty—through forensic investigation or other means—that unauthorized parties had not accessed the data. In other instances, these representatives said that they were not aware of any account fraud that resulted, but they acknowledged that there was no way to know for sure. Moreover, determining potential harm may be particularly challenging with very large breaches because the volume of records involved can make it difficult to link individual victims to the breach.

Table 1: Twenty-Four Large Publicly Reported Data Breaches and Evidence of Resulting Identity Theft, January 2000 - June 2005

The fact that we did not identify evidence of identity theft from a breach does not necessarily mean that no such harm has occurred or will occur in the future.

| Year^a | Type of organization | Nature of breach | Available evidence of identity theft?^b |
|-------------------------|-----------------------------|-----------------------------|--|
| 2000 | Retail | Hacking | Account fraud |
| 2000 | Retail | Hacking | None identified |
| 2002 | Healthcare | Stolen computer equipment | None identified |
| 2003 | Higher education | Stolen computer equipment | None identified |
| 2004 | Financial services | Stolen computer equipment | None identified |
| 2004 | Higher education | Hacking | None identified |
| 2004 | Higher education | Hacking | None identified |
| 2004 | Higher education | Hacking | None identified |
| 2004 | Financial services | Lost data tapes | None identified |
| 2005 | Financial services | Hacking | Account fraud |
| 2005 | State government | Hacking | None identified |
| 2005 | Information services | Deception/Misrepresentation | Unauthorized new accounts |
| 2005 | Higher education | Hacking | None identified |
| 2005 | Higher education | Stolen computer equipment | None identified |
| 2005 | Retail | Hacking | Account fraud |
| 2005 | Information services | Deception/Misrepresentation | Unknown |
| 2005 | Healthcare | Stolen computer equipment | None identified |
| 2005 | Retail | Hacking | Unknown |
| 2005 | Financial services | Lost data tapes | None identified |
| 2005 | Financial services | Employee crime | None identified |
| 2005 | State government | Hacking | None identified |
| 2005 | Media | Lost data tapes | None identified |
| 2005 | Financial services | Lost data tapes | None identified |
| 2005 | Higher education | Other ^c | None identified |

Source: GAO.

Note: To identify the 24 largest data breaches reported in the news media from January 2000 through June 2005, GAO analyzed lists of such breaches maintained by Identity Theft Resource Center, Privacy Rights Clearinghouse, and Congressional Research Service.

^aYear breach occurred or was publicized.

^bThe presence or lack of evidence of identity theft resulting from a breach was based on our review of news reports and other publicly available information, as well as interviews, as feasible, with representatives of entities experiencing the breach and law enforcement officials investigating the breach. The fact that we were unable to identify evidence at this time of identity theft resulting from a breach does not mean that no such harm has occurred or that none will occur in the future. Further, factual determinations of the existence and cause of identity theft in any particular case are matters for the courts to decide.

^cIn this case, a former university employee with access to sensitive personal information had been indicted on bank fraud charges unrelated to the university. Some press reports characterized this as a breach, but according to a representative of the university, there is no evidence that the employee misused university data.

The one large breach we identified that apparently resulted in the unauthorized creation of new accounts involved ChoicePoint, an information reseller. In 2005, the company acknowledged that the personal records it held on approximately 162,000 consumers had been compromised by individuals who posed as legitimate subscribers to the company's information services. FTC reached a civil settlement in 2006 with the company that established a fund for consumer redress to reimburse potential victims of identity theft, and the agency has worked with law enforcement officials to identify such victims.⁴¹

The three large breaches we identified that appeared to result in fraud on existing accounts included the following:

- CardSystems, a credit card payment processor, reported a May 2005 breach in which a hacker accessed data such as names, card account numbers, and expiration dates. The total number of compromised accounts is unclear. FTC staff alleged in a 2006 civil complaint that the breach had compromised data associated with tens of millions of credit and debit cards, but a CardSystems official stated in congressional testimony that only 239,000 accounts were compromised. Officials of the Office of the Comptroller of the Currency—who surveyed the national banks they supervise in order to determine the amount of fraudulent charges that resulted from the breach—said that customers of 110 banks were affected by this incident and losses of more than \$13

⁴¹*United States v. ChoicePoint, Inc.*, No. 1:06-cv-00198-JTC (N.D. Ga., Feb. 15, 2006). As part of the settlement, ChoicePoint admitted no violations of the law. According to ChoicePoint, the company has subsequently taken steps to enhance its customer screening process and to assist affected consumers. FTC staff told us that law enforcement officials have determined that as many as 2,900 people have experienced the fraudulent creation of new accounts as a result of the breach. According to a ChoicePoint official, the criminal indictments indicated that 46 people may have been defrauded, but the accused individuals may not have used data acquired from ChoicePoint in all the crimes cited in the indictments.

million in fraudulent charges on customers' cards were reported by 24 of these institutions.

- DSW, a shoe retailer, said in an April 2005 news release that it had experienced a data breach in which a hacker accessed the names and card numbers associated with 1.4 million credit and debit card transactions at 108 of its stores, as well as checking account numbers and driver's license numbers from 96,000 check transactions. According to a complaint filed by FTC in March of 2006, there allegedly have been fraudulent transactions on some of these accounts.
- CD Universe, an Internet-based music store, reportedly experienced a breach in December 1999 in which a hacker accessed as many as 300,000 names, addresses, and credit card numbers from the company Web site, according to media reports and a company official. The hacker allegedly used some of the stolen credit card numbers to obtain money for himself.⁴²

Challenges Exist in Determining the Link between Data Breaches and Identity Theft

Determining the link between data breaches and identity theft is challenging for several reasons. First, identity theft victims often do not know how their personal information was obtained. According to FTC, in approximately 65 percent of the identity theft complaints it received from October 1, 2005, through August 31, 2006, the victim did not know or report how the information was compromised. Second, victims may misattribute how their data were obtained. For example, federal officials and representatives of a private group that assists victims said that consumers who are notified of a breach often assume that any perceived mistakes on their credit card statements or credit report were a result of the breach. As a result, no government agency maintains comprehensive data on the underlying cause of identity theft. FTC told us that its Identity Theft Data Clearinghouse is limited to self-reported complaints and therefore does not contain statistically reliable information that would allow the agency to determine a link between data breaches and identity theft. Similarly, according to FBI, data maintained by the Internet Crime Complaint Center does not include information sufficient to determine the link between data breaches and identity theft.

⁴²This breach occurred in December 1999 but was included in the 24 breaches we reviewed because it was reported in the media in January 2000.

Third, law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. Finally, conducting comprehensive studies of data breaches and identity theft can be hindered by issues of privacy and confidentiality. For example, companies that have experienced breaches may be unable or unwilling to provide information about affected individuals to researchers.

Some studies conducted by private researchers have sought to determine the extent to which data breaches result in identity theft, but our review found them to contain methodological limitations.⁴³ One research firm conducted a study of four data breaches, analyzing credit and other application data for suspicious relationships that indicated fraud.⁴⁴ The study estimated that no more than 0.10 percent of individuals whose data had been breached experienced resulting identity theft in the form of unauthorized new account creation. However, because the study reviewed only four data breaches, it cannot be considered representative of other breaches. Moreover, two of these breaches did not involve personally identifiable information and thus would not be expected to create a risk of fraud involving new account creation.

Another private research firm surveyed approximately 9,000 individuals about whether they had ever received a notification from an organization about the loss or theft of their personal information.⁴⁵ Of the approximately 12 percent of individuals who reported they had received such a notification, 3 percent—or 33 people—said they believed they had suffered identity theft as a result. However, these data are subject to limitations; among other things, individuals are often unaware of whether any fraud they have suffered was, in fact, due to a data breach. A third firm projected in a study that 0.8 percent of consumers whose information a

⁴³Although we found limitations in how these studies linked data breaches and identity theft, we determined other aspects of these studies to be sufficiently reliable, and we refer to them elsewhere in this report.

⁴⁴ID Analytics, Inc., *National Data Breach Analysis* (2006).

⁴⁵Ponemon Institute, *National Survey* (2005). As noted earlier, this study may also be limited by a low survey response rate.

data breach compromised would experience fraud as a result.⁴⁶ However, we question the reliability of this estimate, in part because of assumptions made about the number of consumers affected by data breaches.

Type of Data Compromised and Other Factors Influence Potential for Resulting Consumer Harm

The type of data compromised in a breach can effectively determine the potential harm that can result. For example, credit or debit card information such as card numbers and expiration dates generally cannot be used alone to open unauthorized new accounts. Some of the largest and most highly publicized data breaches in recent years largely involved credit or debit card data rather than personally identifiable information. As a result, these breaches put affected consumers at risk of account fraud but not necessarily at risk of fraud involving unauthorized creation of new accounts—the type of identity theft generally considered to have a more harmful direct effect on consumers. While credit and debit card fraud is a significant problem—the FTC estimates it results in billions of dollars in losses annually—existing laws limit consumer liability for such fraud and, as a matter of policy, some credit and debit card issuers may voluntarily cover all fraudulent charges.⁴⁷ In contrast, the unauthorized creation of new accounts—such as using someone else’s identity to open credit card or bank accounts, originate home mortgages, file tax returns, or apply for government benefits—can result in substantial financial costs and other hardships.

In addition to the type of data compromised in a breach, several additional factors can influence the extent to which a breach presents the risk of identity theft. These include the following:

- *Intent.* Breaches that are the result of intentional acts—such as hacking into a server to obtain sensitive data—generally are considered to pose more risk than accidental breaches such as a lost laptop or the

⁴⁶Javelin Strategy & Research, *Data Breaches and Identity Fraud: Misunderstanding Could Fail Consumers and Burden Businesses* (Pleasanton, California, August 2006).

⁴⁷For unauthorized credit card charges, consumer liability is limited to a maximum of \$50 per account, 15 U.S.C. § 1643. For unauthorized ATM or debit card transactions, the Electronic Fund Transfer Act limits consumer liability, depending on how quickly the consumer reports the loss or theft of the card. Pub. L. No. 90-321, tit. IX, as added Pub. L. No. 95-630, tit. XX, § 2001, 92 Stat. 3728 (Nov. 10, 1978); 15 U.S.C. § 1693g. Consumers may incur additional costs if they inadvertently pay charges they did not incur. In addition, account fraud can cause inconvenience or temporary hardship—such as losing temporary access to account funds or requiring the cancellation and reactivation of cards and the redirecting of automatic payments and deposits.

unintentional exposure of sensitive data on the Internet, according to federal agency officials. However, in some cases, such as the theft of a laptop containing personal information, it may be unknown whether the laptop was stolen for the hardware, the personal data, or both.

- *Encryption.* Encryption—encoding data so that it can only be read by authorized individuals—can in some cases prevent unauthorized access. However, some forms of encryption are more effective than others, and encryption does not necessarily preclude fraudulent use of data—for example, if the key used to unencrypt the data is also compromised.
- *Hardware requirements.* Data that only can be accessed using specialized equipment and software may be less likely to be misused in the case of a breach. For example, some entities that have lost data tapes have stated that criminals would require specific data reading equipment and expertise in how to use it to access the information.
- *Number of records.* Larger breaches may pose a greater overall risk that at least one individual would become a victim of identity theft. At the same time, given the resources needed to commit identity theft, breaches of very large numbers of records may pose less risk to any one individual whose data were compromised.

Breach Notification Requirements Can Serve to Encourage Better Data Security Practices and Alert Consumers, but They Also Present Costs and Challenges

Breach notification requirements have several potential benefits, including creating incentives for entities to improve their data security practices (and thus prevent potential breaches from occurring), allowing affected consumers to take measures to prevent or mitigate identity theft, and serving to respect individuals' basic right to know when their personal information is compromised. At the same time, breach notification requirements present costs, both for developing compliance strategies and for actual notifications in the event of a breach. Further, there is the risk of overnotification, or inundating consumers with frequent notifications of breaches that may present little or no risk of identity theft or other harm. Thus, policymakers face the challenge of setting a notification standard that allows individuals to take steps to protect themselves where the risk of harm exists, while ensuring they are only notified in cases where the level of risk warrants such action.

Notification Requirements May Create Incentives for Improved Data Security and Allow Consumers the Opportunity to Mitigate Risks

According to our review of studies and interviews with representatives in government, academia, and private industry, breach notification requirements have several potential benefits, as follows:

- *Incentives for Improved Data Security.* Breach notification requirements can provide an incentive for companies and other entities to increase their data security measures to avoid the possible financial and reputational risks that can be associated with a publicly reported data breach.⁴⁸ Representatives we contacted in the private, nonprofit, and government sectors told us that they believe that existing breach notification requirements in state laws, or the breach notification provisions in federal banking regulatory guidance, have provided entities with incentives to improve data security practices. For example, some representatives of companies and other organizations noted that passage of state notification laws led to companies reexamining data security procedures and making improvements, such as encrypting sensitive data and restricting consumer data that can be accessed online. Similarly, federal banking regulators told us that they believe their notification guidance has motivated regulated institutions to enhance data security. For example, according to officials at the Office of Thrift Supervision, its institutions have taken steps such as improving electronic firewalls and implementing formal incident response reporting systems.
- *Prevention of Identity Theft.* Breach notification can provide consumers with the opportunity to take steps to protect themselves from possible identity theft. For example, consumers whose account information has been breached can monitor their bank or credit card statements for suspicious activity or close the affected accounts. Consumers whose personally identifiable information, such as SSN, has been breached can review their credit reports for suspicious activity or may choose to purchase a credit monitoring product that alerts them to changes that could indicate identity theft. In addition, affected consumers can place a fraud alert on their credit reports, which requires businesses to take certain identity verification steps before

⁴⁸Such costs can be significant. For example, according to a 2006 survey, 31 companies that responded to the survey incurred an average of \$98 per record, or \$2.6 million per company, in costs associated with the loss of existing customers, recruitment of new customers, and damage to the reputation of their brand name. Ponemon Institute, LLC, *2006 Annual Study: Cost of a Data Breach*, 2006. Due to sampling limitations, these findings are not necessarily representative of the costs incurred by all companies that experience breaches.

issuing credit.⁴⁹ In some states, consumers can implement credit freezes, which block unauthorized third parties from obtaining the consumer's credit report or score.⁵⁰ Limited information exists on the steps individuals actually take when notified of a breach. In the 2005 Ponemon Institute survey of individuals that received notification letters, 50 percent said they did nothing, while the rest indicated they took actions such as monitoring their credit reports, canceling credit or debit cards, or closing bank accounts.⁵¹

- *Respecting Consumers' Right to Know.* Some consumer advocates and others have argued that consumers have a right to know how their information is being handled. According to this view, basic rights of privacy dictate that consumers should be informed when their personal information has been compromised, even if the risk of harm is minimal. The principle that individuals should have ready means of learning about the use of their personal information is embedded in the Fair Information Practices, a set of internationally recognized privacy protection principles.⁵²
- *Improving Public Awareness.* Public reporting of data breaches may raise general awareness among consumers about the risks of identity theft and ways they can mitigate these risks, such as periodically reviewing their credit reports. In addition, publicity surrounding a data breach resulting from notification can serve to deter the use of stolen information because presumably the thief knows that the breach is likely being investigated and the stolen data are being carefully monitored.

⁴⁹See 15 U.S.C. § 1681c-1.

⁵⁰Congressional Research Service, *Identity Theft Laws: State Penalties and Remedies and Pending Federal Bills* (Washington, D.C.: Jan. 11, 2007).

⁵¹Ponemon Institute, *National Survey* (2005). As noted earlier, this study may be limited by a low survey response rate.

⁵²The Fair Information Practices were first proposed in 1973 by a U.S. government advisory committee. A revised version was developed in 1980 by the Organization for Economic Cooperation and Development, a group of 30 member countries that are market democracies. For more information, see GAO, *Personal Information: Agency and Reseller Adherence to Key Privacy Principles*, [GAO-06-421](#) (Washington, D.C.: Apr. 4, 2006).

Breach Notification Requirements Present a Variety of Potential Costs

According to company representatives, researchers, regulators, and others, there are several different types of costs that may be associated with breach notification requirements. To begin with, entities subject to breach notification requirements may incur certain costs, regardless of whether they actually suffer a breach, or—if they do—regardless of whether they have to notify consumers. For example, entities may incur costs for developing and formalizing incident response plans.

There are also the costs associated with actual notifications—potentially including printing, postage, legal, investigative, and public relations expenses.⁵³ Although comprehensive data on these costs do not exist, a 2006 Ponemon Institute survey of companies experiencing a data breach found that 31 companies that responded incurred an average of \$1.4 million per breach, or \$54 per record breached, for costs related to mailing notification letters, call center expenses, courtesy discounts or services, and legal fees.⁵⁴ Similarly, a study by Gartner Research found that ChoicePoint spent \$79 per affected account following its 2005 breach for professional fees, legal expenses, and communications to affected customers.⁵⁵ A representative of the San Jose Medical Group told us it spent \$100,000 to send notification letters to 187,000 patients following a data breach that occurred in 2005. Entities also may incur costs related to staffing call centers to field inquiries from consumers about the breach. For example, representatives of the University of California at Berkeley told us that following a 2005 breach of 98,000 records, the university spent \$75,000 in staffing, telecommunications, and other call center costs.

Finally, banks whose customers' account information is breached also may incur costs for remedial steps such as canceling existing accounts or replacing affected customers' credit or debit cards—although such steps may not be required by the applicable breach notification requirements.

⁵³The distinction between the costs associated with a notification requirement versus a breach itself can be ambiguous. For example, the cost of postage can clearly be attributed to notification, whereas legal costs can be attributed to notification, the breach itself, or both, depending on the circumstances.

⁵⁴Ponemon Institute, *Annual Study* (2006). As noted earlier, due to sampling limitations, these findings are not necessarily representative of the costs incurred by all companies that experience breaches.

⁵⁵Gartner Research, *Data Protection Is Less Costly Than Data Breaches* (Stamford, Connecticut: September 16, 2005). The report, issued in 2005, based its findings on the breach having affected 145,000 records, but company officials later reported that 162,000 records were affected.

Entities experiencing a breach also often provide affected individuals with free credit monitoring services. For example, a representative of a large financial management company noted that offering free credit monitoring services after a breach has become standard industry practice, and costs, on average, between \$20 and \$40 per customer.

Challenges Exist in Complying with and Developing Breach Notification Requirements

Officials of companies and other entities we interviewed identified challenges such as interpreting ambiguous statutory language, identifying and locating affected consumers, and developing effective notification letters. In addition, policymakers face challenges in developing breach notification requirements, particularly in setting the appropriate standard to establish the circumstances under which consumers should be notified.

Complying with Notification Requirements

Companies and other entities we interviewed said they can face a number of challenges related to complying with the breach notification requirements in state laws or federal banking guidance. These include the following:

- *Interpreting ambiguous provisions.* Entities subject to breach notification requirements sometimes face challenges interpreting certain terms or provisions of notification laws. For example, an information security expert told us that some laws do not adequately define encryption, which could refer to anything from simple password protection to complex coding. Similarly, federal banking regulators acknowledged that their institutions sometimes face difficulty determining whether misuse of breached information is “reasonably possible,” such as when little information exists about the location of the data, the intent of a criminal who stole data, or the effectiveness of security features designed to render data inaccessible.
- *Addressing who is responsible.* Notification requirements do not always fully address who should bear the cost of and responsibility for notification, particularly in cases where a third party is responsible for the breach. For example, representatives of some federal banking regulators and industry associations cited particular challenges associated with breaches of credit and debit card information by retailers. Banks that issue credit and debit cards compromised by a merchant that is not the bank’s service provider are generally not required by the banking regulators’ guidance to notify their customers, but nevertheless in some cases, they feel obliged to do so. Bank representatives with whom we spoke expressed concern that breaches of credit card information by third parties can adversely affect a bank’s

reputation and result in costs related to notifying customers and reissuing cards.

- *Identifying affected consumers.* Some entities we interviewed said that it can be difficult to identify which consumers may have been affected by a breach and obtain their contact information. For example, one representative at a state agency involved in a breach told us officials were unsure what data had been downloaded among records that may have been accessed on 600,000 people. Obtaining accurate and current mailing addresses for affected parties also can be difficult and costly, many entities told us. This can be a particular problem for entities, such as merchants, that have breached credit card numbers but do not themselves possess the mailing addresses associated with those numbers.
- *Developing clear and effective notification letters.* We have noted in the past that public notices should be useful and easy to understand if they are to be effective.⁵⁶ However, the 2005 study conducted by the Ponemon Institute found that 52 percent of survey respondents who received a notification letter said the letter was not easy to understand.⁵⁷ In addition, consumers might be confused by other mail solicitations that may resemble notification letters. For example, officials at one large national bank noted that marketing solicitations for credit monitoring services often are made to resemble breach notification letters, potentially desensitizing or confusing consumers when a true notification letter arrives.
- *Complying with multiple state laws.* Officials of companies with customers in multiple states and their trade associations noted that they face the challenge of complying with breach notification requirements that vary among the states, including who must be notified, the level of risk that triggers a notice, the nature of the notification, and exceptions to the requirement. Officials of companies we contacted noted that it is challenging to comply with these multiple requirements since most breaches involve customers in many states.

⁵⁶See GAO-06-833T, *Privacy: Preventing and Responding to Improper Disclosures of Personal Information* (Washington, D.C.: Jun. 8, 2006), pp. 15-18, which discusses specific elements that should be incorporated in a breach notification.

⁵⁷Ponemon Institute, *National Survey* (2005). As noted earlier, this study may be limited by a low survey response rate.

Setting an Appropriate Notification Standard

Existing state laws vary in terms of the notification standard—that is, the event or circumstance that triggers a required notification. For example, California has an expansive standard that requires notification in nearly all cases where unencrypted sensitive personal data “is reasonably believed to have been acquired by an unauthorized individual.” Other states employ a risk-based approach that incorporates into the standard the extent to which the data are likely to be misused. The standards vary in terms of what is required in cases where the risk of harm is unknown. For example, Vermont requires notification unless an entity can demonstrate that misuse of the breached data “is not reasonably possible.” In contrast, North Carolina requires notification only when it has been determined that the breach has resulted, or is reasonably likely to result, in illegal use of the data or creates a material risk of harm to a consumer. As shown in figure 1, whether or not a breach is subject to notification can depend on the specific notification standard.

Figure 1: Application of Notification Standards under Different Breach Scenarios

| | | Scenarios | | |
|---|---|------------------------------------|--|---|
| | | Hacker accesses a company database | Laptop stolen but recovered and data not misused or copied | Data on computer screen viewed by unauthorized passerby |
| <p>Broader standard (more incidents result in notification)</p> <p>Narrower standard (fewer incidents result in notification)</p> | <p>Notification required whenever sensitive personal information is...</p> <p>...lost, stolen, or viewed by an unauthorized person</p> | | | |
| | <p>...obtained by an unauthorized person</p> | | | |
| | <p>...obtained by an unauthorized person <i>and</i> misuse is reasonably possible</p> | | | |

Source: GAO (analysis); Art Explosion (images).

Note: Figure presents hypothetical scenarios and notification standards and is shown for illustrative purposes only.

Because of the difficulty of complying with multiple state requirements, many companies and industry representatives have argued for a consistent federal standard for breach notification that would preempt state notification laws. However, the National Association of Attorneys General, as well as some consumer and privacy groups, have expressed concern that a federal breach notification law could weaken consumer protections if it were to preempt stronger state laws. These groups have advocated a strong notification standard because, they say, the link between breaches and identity theft is not always clear and entities are not well equipped to assess the risk of harm resulting from a given breach. As a result, too narrow a notification standard may prevent consumers from taking action in cases that do in fact present some risk. Also, as noted earlier, some privacy groups and others believe that consumers have basic rights to be notified when their personal information has been breached, no matter what the circumstances. Moreover, they say that fears of “overnotification”—where consumers are inundated by frequent notifications—are unfounded, given that they are aware of no evidence of this occurring in states that currently have strict notification requirements.

By contrast, some representatives of the federal banking regulatory agencies, FTC, private companies, and other experts have expressed concern about overly expansive breach notification standards. They say that such standards may require businesses to notify consumers about minor and insignificant breaches. This in turn could eventually lead to overnotification and cause consumers to spend time and money taking proactive steps that are not necessary or, alternatively, to ignore notices when action is warranted. In addition, businesses and federal banking regulators have expressed concern about the financial burden that overnotification could cause. Overly broad notification standards could also have the effect of limiting entities’ reputational incentives for improving data security, if nearly all entities regularly issue notifications as a result of minor breaches. Representatives of the federal banking regulatory agencies have noted that they sought to strike an appropriate balance with their notification standard. Their guidance provides that, when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused.⁵⁸ If the institution determines that

⁵⁸12 C.F.R. Pt. 30, App. B, Supp. A § III(A); 12 C.F.R. Pt. 208, App. D-2, Supp. A § III(A); 12 C.F.R. Pt. 225, App. F, Supp. A § III(A); 12 C.F.R. Pt. 364, App. B, Supp. A § III(A); 12 C.F.R. Pt. 570, App. B, Supp. A § III(A); and 12 C.F.R. Pt. 748, App. B § III(A).

misuse of the information has occurred or is reasonably possible, it should notify affected customers as soon as possible. The guidance is intended to provide notice to customers only when there is a reasonable expectation of misuse.⁵⁹

Similarly, the guidance for federal agencies developed by the President's Identity Theft Task Force recommended that if an agency experiences a breach, it should analyze the risk of identity theft and tailor its response—which may include notifying individuals—to the nature and scope of the risk presented. The guidance noted that such a risk assessment can minimize the potentially significant costs of notification where little risk exists. The task force's April 2007 strategic plan recommended the development of a national standard requiring all entities that maintain sensitive consumer information, in both the public and private sectors, to provide notice to consumers and law enforcement in the event of a breach. As with its guidance to federal agencies, the task force recommended that the standard be risk based to provide notice when consumers face a significant risk of identity theft but to avoid excessive notification.

As we have noted in the past, care is needed in defining appropriate criteria for data breaches that merit notification.⁶⁰ The frequency of data breaches identified in this report suggests that a national breach notification requirement may be beneficial, in large part because of its role in further encouraging entities to improve their data security practices. However, because breaches vary in the risk they present, and because most breaches have not resulted in detected incidents of identity theft, a notification that is risk based appears appropriate. Should Congress choose to enact a federal breach notification requirement, use of the risk-based approaches that the federal banking regulators and the President's

⁵⁹The guidance states that institutions should notify their primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, even for incidents that may not warrant customer notification. Banking regulators told us they review institutions' response programs as part of their supervisory procedures and, in many cases, work with institutions as they respond to specific incidents to ensure their actions are in accordance with the guidance. See 12 C.F.R. Pt. 30, App. B, Supp. A § II(A)(1)(b); 12 C.F.R. Pt. 208, App. D-2, Supp. A § II(A)(1)(b); 12 C.F.R. Pt. 225, App. F, Supp. A § II(A)(1)(b); 12 C.F.R. Pt. 364, App. B, Supp. A § II(A)(1)(b); 12 C.F.R. Pt. 570, App. B, Supp. A § II(A)(1)(b); and 12 C.F.R. Pt. 748, App. B § II(A)(1)(b).

⁶⁰GAO, *Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data*, GAO-06-674 (Washington, D.C.: Jun. 26, 2006) and GAO-06-833T.

Identity Theft Task Force advocate could avoid undue burden on organizations and unnecessary and counterproductive notifications to consumers.

Agency Comments

We provided a draft of this report to FTC, which provided technical comments that were incorporated in this report as appropriate. In addition, we provided selected portions of the draft to the Board of Governors of the Federal Reserve System, the Department of Justice, DHS, FDIC, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Social Security Administration, and USPS, and also incorporated their technical comments as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. We will then send copies of this report to the Chairman, House Committee on Financial Services; the Chairman and Ranking Member, Senate Committee on Banking, Housing, and Urban Affairs; the Chairman and Ranking Member, Senate Committee on the Judiciary; the Chairman and Ranking Member, House Committee on the Judiciary; the Chairman and Vice Chairman, Senate Committee on Commerce, Science, and Transportation; and the Chairman and Ranking Member, House Committee on Energy and Commerce. We will also send copies to the Chairman of the Board of Governors of the Federal Reserve System, the Attorney General, the Secretary of the Department of Homeland Security, the Chairman of the Federal Deposit Insurance Corporation, the Chairman of the Federal Trade Commission, the Chairman of the National Credit Union Administration, the Comptroller of the Currency, the Director of the Office of Thrift Supervision, the Commissioner of the Social Security Administration, and the Postmaster General and Chief Executive Officer of the U.S. Postal Service. We will also make copies available to others upon request. In addition, the report will be available at no charge on GAO's Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-8678 or woodd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.

David G. Wood

David G. Wood

Director, Financial Markets and
Community Investment

Appendix I: Scope and Methodology

Our report objectives were to examine (1) what is known about the incidence and circumstances of breaches of sensitive personal information; (2) what information exists on the extent to which breaches of sensitive personal information have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements. We use the term “data breach” to refer to the unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information by a company, government agency, university, or other public or private entity. Our scope was limited to breaches involving personal data, including financial data, that could be used to commit identity theft or other related harm, and we excluded breaches involving other types of sensitive data, such as medical records or proprietary business information. For the purposes of this report, the term “identity theft” is used broadly to refer to both fraud on existing accounts and the unauthorized creation of new accounts.

To address all three objectives, we conducted a literature search of relevant articles, reports, and studies. We also collected and analyzed documents from, and interviewed, officials of government agencies that investigate and track data breaches, including the Federal Trade Commission, the Department of Homeland Security, the Department of Justice, the U.S. Postal Inspection Service, and the Social Security Administration. We also interviewed staff at the five federal banking regulators—the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration. In addition, we spoke with representatives of the National Association of Attorneys General and organizations that address consumer protection and privacy issues, including Consumers Union, Electronic Privacy Information Center, Privacy Rights Clearinghouse, Attrition, and the Identity Theft Resource Center. We also spoke with three academic researchers who study issues related to data breaches and notification and an attorney who helps companies address data privacy and security issues. In addition, we reviewed studies on data breaches conducted by private and nonprofit research organizations, including the Ponemon Institute, ID Analytics, and Javelin Strategy and Research. We interviewed the studies’ authors and took other steps to ensure that the data and methodologies were sufficiently reliable for our purposes. We also spoke with representatives of the California Office of Privacy Protection and its advisory group and reviewed the office’s recommended practices for notification.

Appendix I: Scope and Methodology

To address the first objective on the incidence and circumstances of data breaches, we reviewed lists of news media-reported data breaches that are compiled and maintained by three private research and advocacy organizations—Privacy Rights Clearinghouse, Attrition, and the Identity Theft Resource Center. We analyzed the three independent lists to create a single, nonduplicative list of data breaches that had been reported in the news media from January 2005 through December 2006. We took measures to ensure the lists were of sufficient quality for our purposes, including spot checking selected data and interviewing representatives of the three organizations on their methodologies. The Privacy Rights Clearinghouse, Attrition, and Identity Theft Resource Center lists contained 436, 453, and 462 breaches, respectively, for the time period we analyzed. Of the 572 breaches they collectively compiled, 59 percent appeared on all three lists, 19 percent appeared on two, and 22 percent appeared on one. Our analysis was based on the lists as they stood on February 15, 2007; these data may have changed because the lists are occasionally updated when the compilers learn of new breaches that may have occurred in the past.

We also collected available data from federal law enforcement agencies on the breaches they have investigated in recent years. In addition, the five federal banking regulators provided, at our request, data on the breaches of which they have been notified by the institutions they supervise. These data varied in usefulness and comprehensiveness because of the regulators' differing methods of counting and tracking breaches and maintaining data on them. We also gathered data from two states, New York and North Carolina, which were selected because they were two large states that maintain centralized information on breaches. Further, we obtained available data from industry and trade associations representing key sectors—such as financial services, retail sales, higher education, hospitals, and information services—that have experienced data breaches. We also collected information on breaches experienced by federal agencies compiled by the House Government Reform Committee and the U.S. Computer Emergency Readiness Team, a component of the Department of Homeland Security.

To address the second objective, we selected for more detailed examination the 24 largest (in terms of number of records breached) data breaches reported in the news media from January 2000 through June 2005. We selected these breaches in August 2006 using the lists maintained by Privacy Rights Clearinghouse and Identity Theft Resource Center, as well as a similar compilation of breaches collected by the Congressional Research Service. We were not aware of the Attrition list at the time we

Appendix I: Scope and Methodology

made our selection. For each of these breaches, we reviewed news reports as well as publicly available documents such as testimonies and criminal indictments. We also conducted interviews, where possible, with representatives of the entities that experienced the breach and law enforcement agencies that investigated the breach. We identified those cases where this information collectively indicated that the breach appeared to have resulted in some form of identity theft. Ultimately, the determination of whether particular conduct violated a law prohibiting identity theft would be a matter of law for the courts. We did not directly contact individuals whose data had been affected by the breaches because of privacy concerns and because we did not have a systematic means of identifying them. We also reviewed five breaches that reportedly involved federal agencies—the Navy; the Internal Revenue Service; the Federal Deposit Insurance Corporation; the National Park Service; and the Department of Justice. These were selected to represent breaches that included different causes, types of data, and involvement by third-party vendors.

To examine the potential benefits, costs, and challenges associated with breach notification requirements, we reviewed the federal banking regulators' proposed and final guidance related to breach notification, and interviewed representatives of each agency regarding their consideration of potential costs, benefits, and challenges during development of the guidance. Further, we reviewed the strategic plan and other documents issued by the President's Identity Theft Task Force. In addition, we conducted a review of the effects of California's breach notification law. We interviewed representatives of, and gathered information from, seven organizations to learn about their experiences complying with California's breach notification law. These organizations were selected to represent a range of organization sizes and industry sectors. We also interviewed representatives of the California State Information Security Office, California State Assembly, California Office of Privacy Protection, and California Bankers Association.

We conducted our review from August 2006 through April 2007 in accordance with generally accepted government auditing standards.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

David G. Wood, (202) 512-8678 or woodd@gao.gov

Staff Acknowledgments

In addition to the contact named above, Jason Bromberg, Assistant Director; Randy Fasnacht; Marc Molino; Kathryn O'Dea; Carl Ramirez; Linda Rego; Barbara Roesmann; and Winnie Tsen made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548