The Consumer Data Insecurity Report:
Examining the Data Breach — Identity Fraud Paradigm in Four Major Metropolitan Areas

Sponsored by:

Independently produced by:
CONTENTS

Forward .......................................................................................................................................................... 3
Overview .......................................................................................................................................................... 4
Executive Summary ......................................................................................................................................... 5
Key Findings .................................................................................................................................................. 7
  General ......................................................................................................................................................... 7
  Business ..................................................................................................................................................... 7
  Government ............................................................................................................................................... 8
Metropolitan Area Fraud Victim Profiles ........................................................................................................ 10
The Data Breach — Identity Fraud Paradigm ....................................................................................................... 13
How Consumers React to Fraud ...................................................................................................................... 17
Victims’ Expectations ........................................................................................................................................ 21
Methodology ................................................................................................................................................... 30
Appendix .......................................................................................................................................................... 31

TABLE OF FIGURES

Figure 1: Fraud Victims Who Received Data Breach Notifications, by Metropolitan Area ........................................ 10
Figure 2: How Compromised Information Was Misused, by Metropolitan Area .................................................. 11
Figure 3: Types of Fraud Experienced by Fraud Victims, by Metropolitan Area .................................................. 12
Figure 4: Type of PII Breached and Misused, by Industry ..................................................................................... 13
Figure 5: Type of Financial Account Information Breached and Misused, by Industry ........................................... 14
Figure 6: Type of Organization Where Information Was Compromised ................................................................ 15
Figure 7: Number of Identity Fraud Occurrences for Data Breach Victims and Non-Data Breach Victims ........... 16
Figure 8: Actions Taken by Victims as a Result of Experiencing Identity Fraud .................................................... 17
Figure 9: Agencies Contacted After Fraud by All Fraud Victims and Victims Whose PII Was Breached, by Type of Organization Where Breach Occurred .................................................................................... 18
Figure 10: How Fraud Affected Data Breach Victims' Level of Trust, by the Industry Where Breach Occurred .. 19
Figure 11: Data Breach Fraud Victims’ Level of Confidence That the Industry in Which Breach Occurred Could Protect Them From Future Fraud .............................................................................................................. 20
Figure 12: Perceived Effectiveness of Fraud Prevention Activities Among All Fraud Victims and by Metropolitan Area .................................................................................................................................................. 21
Figure 13: Industries That Should Be Held Accountable and Business Avoidance Postbreach, by Fraud Victims Whose Information Was Breached at FIs, Retailers, and Other Organizations ......................................................... 22
Figure 14: Organizations That Should Be Held Responsible for Protecting Accounts During Recent Fraud, According to Non-data breach Victims and Data Breach Victims ......................................................................................... 23
Figure 15: Organizations That Should Be Held Responsible for Restoring Identity After Recent Fraud, According to Non-data breach Victims and Data Breach Victims ......................................................................................... 24
Figure 16: Agreement With Statement, by Type of Organization Where Information Was Breached ................. 25
Figure 17: Fraud Victims’ Attitudes Regarding Data Breaches ............................................................................ 26
Figure 18: Agreement With Statement, by Metropolitan Area .............................................................................. 27
Figure 19: When Notification Should Be Provided After a Data Breach, by Fraud Victims .................................... 28
Figure 20: Type of Organization Where Information Was Compromised, by Most Recent Fraud Incident ...... 31
Figure 21: Information Compromised in Most Recent Fraud Incident, by Victim Type ........................................ 31
Figure 22: Rate of Fraud Victimization by Type of Data Breached ....................................................................... 32
FORWARD

This white paper was sponsored by the National Consumer League. It explores the attitudes, experiences, and perceptions of fraud victims in four metropolitan areas: Chicago, Los Angeles, Miami, and Minneapolis. The white paper was independently produced by Javelin Strategy & Research, a Greenwich Associates LLC company. Javelin maintains complete independence in its data collection, findings, and analysis.
OVERVIEW

As the use of consumers’ personally identifiable information (PII) by businesses continues to evolve, sensitive data is constantly being placed at risk of compromise. To ensure that consumers can take necessary actions to protect themselves after a breach has occurred, 47 states have enacted data breach notification laws.\(^1\) Yet despite the patchwork of state laws and industry-specific federal legislation and regulations,\(^2,3\) the past couple of years have been especially trying for both consumers and breached organizations. Among all types of sensitive data, financial information is most favored by criminal organizations, which are now more than ever successfully targeting this data for theft and subsequent misuse.

To better understand the data breach-identity fraud paradigm, Javelin surveyed fraud victims in four major metropolitan areas across the U.S.: Chicago, Los Angeles, Miami, and Minneapolis. In comparing the experiences of fraud victims who had suffered a data breach with those who did not, the effects of data breaches on the integrity of consumer identities are readily apparent. It is evident that data breaches have become part of the public consciousness, specifically because of their role in facilitating identity fraud. This has severe implications for all stakeholders, as affected consumers are holding a variety of organizations accountable for failing to protect their PII from being compromised, bought, sold, and misused by fraudsters, hackers, and other criminal entities. Changing the status quo is critical to maintaining consumer trust in an environment where PII is successfully stolen en masse, on an all too regular basis.

---


EXECUTIVE SUMMARY

Despite the broad patchwork of data security breach notification laws and regulations currently in place, data breach-fueled identity fraud is on the rise. In 2013, nearly 1 in 3 data breach victims suffered identity fraud, compared with 1 in 9 in 2010. Yet not only has the actual connection between data breaches and fraud continued to grow, but also media coverage of recent high-profile data breaches has served to reinforce the connection between data breaches and fraud in the minds of consumers. Consumer trust is of paramount value for businesses, and being compromised in a data breach puts these businesses at risk of losing customers.

Businesses are being heavily targeted for financial account information by criminals and hackers, which has contributed to the substantial growth of certain types of identity fraud. Nationally, there was a dramatic increase in the volume of existing card fraud (ECF), which grew from $8 billion in 2012 to $11 billion in total fraud losses in 2013. Examining the experiences of fraud victims in four major metropolitan areas reveals that while there are some similarities related to national fraud trends among victims in these separate regions, there are also important distinctions among them.

Consumer awareness of breaches is on the rise, as all consumers, and fraud victims specifically, were more likely to be notified of a data breach in 2013, compared with 2012. Given such awareness of imminent or potential threat to their identities, consumers believe that taking appropriate steps to safeguard their data will help with protecting their identity. Unfortunately, certain remedies that have been relied upon by affected organizations and promoted by government officials are ineffective in the prevention of fraud in many cases, yet continue to be prescribed to victims.

---

2 ibid.
3 ibid.
4 ibid.
Fraud victims themselves do not seem to discriminate between business organizations and financial institutions when assigning blame for a data breach. In reaction to a data breach, victims will specifically avoid doing business with affected organizations — diminishing the future profitability of these businesses. And while victims hold all organizations involved accountable for information compromise, they feel differently as to who is responsible for protecting accounts and undoing damage caused by fraud, based on whether their lost information was compromised in a data breach or an event unrelated to a data breach.

According to victims, the government has a significant role to play and issues to address in the fight against data breaches. Victims expect the federal government to ensure that businesses adhere to data security standards, while at the same time they believe that existing regulations are generally insufficient. Tacit support from victims for stronger federal protections has joined the chorus of voices from the financial industry who had supported changes to previously proposed legislation. While the passage of a national data breach law has remained elusive, the damage that breaches represent to the integrity of consumer identities and the success of businesses might prove too difficult for legislators to continue to ignore.
KEY FINDINGS

General

While data breaches are the predominant source of misused credentials, data breach notification might help prevent against multiple fraud incidents.
Defrauded data breach victims overwhelmingly attribute their fraud to the breach of their credentials (61% say they are certain that this was the source of the misused credentials). However, data breach victims are 15% less likely to suffer multiple fraud events compared with all fraud victims (50% vs. 59% suffered only one fraud incident).

Nearly a third of fraud victims fails to take any action to prevent further fraud.
This means that victims are more likely to take no action than to respond to the fraud in any other way. The second and third most common actions taken are receiving email or mobile alerts about credit card or checking accounts (24%) and putting fraud alerts on credit reports (23%).

Business

Breaches greatly affect consumer confidence, especially for retailers. Six in 10 victims whose information was compromised in a retailer breach said their level of trust in the retailer declined significantly. This diminished confidence is less for victims of breached FIs (28% say their confidence declined significantly). Retailers are also up against the lowest degree of confidence in their ability to protect victims’ information in the future. Only 10% of victims whose PII was breached at a retailer were very confident that the organization could protect them from future fraud.

Large retailer breaches are a locus of data breaches and consumer fraud. Half of defrauded data breach victims indicate that their information was compromised in a large retailer data breach. Further still, among those defrauded data breach victims who knew that breached information was used to commit the fraud, 33% say that the information was compromised from this same segment of businesses.
Victims believe not only businesses but also FIs should be held accountable, with 1 in 5 victims avoiding doing business with these organizations after his or her information is breached. Fifty-two percent of fraud victims believe businesses and organizations should be held accountable in the wake of a data breach, and 48% say the same of FIs. Nineteen percent of victims whose information was breached at one of these locations say that they would avoid doing business with the organization in the future.

Organizations should prepare for more stringent federal legislation regarding data protection, and continued consumer lawsuits. Just over a quarter of fraud victims believe that current federal data security requirements are sufficient for protecting health care and financial data. This indicates there is political will for passing pending national legislation for greater accountability for all custodians of sensitive PII. Victims also overwhelmingly believe that consumers should be able to take legal action against breached organizations regardless of where their information was breached.

Government

Immediate and comprehensive data breach notifications are needed. While nearly 9 in 10 victims believe that data breach notifications should be immediate, most states make allowances for delayed notifications. Data breach notifications offer an opportunity for organizations to educate affected consumers about the circumstances of the breach, their effect on the integrity of consumers’ identities, efforts undertaken by the breached organization to protect their identities going forward, and how consumers can ultimately protect themselves. The current patchwork of state laws and federal regulations are proving insufficient as the connection between breaches and fraud has never been stronger and as consumers vote with their wallet, changing their patronage behaviors postbreach.

Government should facilitate the cooperative development of a clear, actionable set of data security best practices. The business community is well incentivized to stand side-by-side with consumers in advocating for change. Among affected industries, consumers indicate that they are most likely to lose trust in retailers after a breach. For this industry especially, in light of continued media scrutiny and pressure from the financial industry and government officials, participating in efforts to shape the national debate is crucial. Government must do more as only 28% of victims consider existing federal regulations to be sufficient for protecting sensitive information such as financial account data and protected health information (PHI), yet 70% believe the federal government should be responsible for ensuring that businesses meet data security standards.
METROPOLITAN AREA FRAUD VICTIM PROFILES

The threat that data breaches represent to the integrity of consumer identities is not unique to any region of the country. Examining the experiences of fraud victims in four metropolitan areas, though, reveals that while there are some similarities among victims in these separate regions, there are also important distinctions among them.

Javelin’s annual identity fraud study elucidates the strong correlation between data breach and identity fraud. This connection is prominent in the areas highlighted in this study — in Los Angeles and Miami, 4 in 5 fraud victims had received a breach notification. This effect is comparatively subtle in the Midwest cities — in Chicago a little over 7 in 10 had received a breach notification, while in Minneapolis 2 in 3 received a breach notification (see Figure 1).

4 in 5 Fraud Victims in Los Angeles and Miami Have Been Notified That Their PII Was Compromised in a Data Breach

Figure 1: Fraud Victims Who Received Data Breach Notifications, by Metropolitan Area

<table>
<thead>
<tr>
<th>Metropolitan Area</th>
<th>Percent of Fraud Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chicago</td>
<td>72%</td>
</tr>
<tr>
<td>Los Angeles</td>
<td>82%</td>
</tr>
<tr>
<td>Minneapolis</td>
<td>66%</td>
</tr>
<tr>
<td>Miami</td>
<td>80%</td>
</tr>
</tbody>
</table>

Q8. Have you EVER been notified by a business or other institution that your personal or financial information has been lost, stolen or compromised in a data breach?

May 2014, n = 50
Base: Fraud victims by metropolitan area.
© 2014 Javelin Strategy & Research
When it comes to information misuse, making quick purchases seems to be the most effective way for criminals to use stolen information. In 2013, online purchase (40% of fraud victims) and in-store purchase (36%) were the leading methods in which fraud victims’ information was misused, according to Javelin’s annual ID fraud study.\(^8\) The same holds true for fraud victims in Chicago, Los Angeles, Miami, and Minneapolis. While in Minneapolis, online purchase (50%) trumps all other areas in the extent of victims affected by this method (See Figure 2), in-store purchase seems to be the most common method for information misuse in Los Angeles (44%) (See Figure 2).

Nationally, there was a dramatic increase in the volume of ECF, with total fraud losses growing from $8 billion in 2012 to $11 billion in 2013.\(^9\) And given the prevalent misuse of compromised information for online and in-store purchases reported by fraud victims in Chicago, Los Angeles, Miami, and Minneapolis (see

**Fraudulent Purchases Are the Most Common Means of Misuse, With Online Purchases Favored in the Midwest and In-Person Transactions More Popular on the Coasts**

**Figure 2: How Compromised Information Was Misused, by Metropolitan Area**
Figure 2), it is not surprising that they were most likely to experience the same type of fraud (see Figure 3). Victims in Chicago are affected the most by ECF, with 82% of victims, while Minneapolis victims arguably fare better with 70% of victims in the area having experienced ECF (see Figure 3).

Existing noncard fraud (ENCF), which also grew significantly nationally from 2012 to 2013, is the second most popular fraud type across all areas. A major contributor to the growing incidence of ENCF is the confluence of poor password habits and the exfiltration of password lists by hackers. As consumers reuse passwords across a greater number of online sites, their risk of fraud rises — when passwords are compromised in a data breach, each password could expose multiple consumer accounts to unauthorized access. Among the areas examined, fraud victims in Miami and Minneapolis were more likely to experience ENCF compared with fraud victims in Los Angeles and Chicago (see Figure 3).

Tracking With National Fraud Rates, Existing Card Fraud Most Likely to Plague Victims Regardless of Where They Live

Figure 3: Types of Fraud Experienced by Fraud Victims, by Metropolitan Area

<table>
<thead>
<tr>
<th>Metropolitan Area</th>
<th>Existing Card Fraud</th>
<th>Existing Non-Card Account Fraud</th>
<th>New-Account Fraud</th>
<th>Account Takeover Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chicago</td>
<td>82%</td>
<td>16%</td>
<td>38%</td>
<td>18%</td>
</tr>
<tr>
<td>Los Angeles</td>
<td>76%</td>
<td>30%</td>
<td>42%</td>
<td>26%</td>
</tr>
<tr>
<td>Minneapolis</td>
<td>70%</td>
<td>20%</td>
<td>50%</td>
<td>24%</td>
</tr>
<tr>
<td>Miami</td>
<td>74%</td>
<td>16%</td>
<td>50%</td>
<td>36%</td>
</tr>
</tbody>
</table>

Q12A through Q12D: Thinking about the most recent fraud incident, what type of personal/financial information was misused?

May 2014, n = 50
Base: Fraud victims by metropolitan area.
© 2014 Javelin Strategy & Research

11 Ibid.
THE DATA BREACH — IDENTITY FRAUD PARADIGM

The days of Dumpster diving and pickpocketing as mainstays of a fraudster’s PII-gathering efforts have come and gone. Personally identifiable information stored and transmitted by organizations, regardless of industry, now attracts the attention of skilled criminal organizations around the world. Once in possession of this data, much of it can be readily misused to commit fraud or, instead, sold or traded in underground forums to other criminals for subsequent misuse. In 2013, nearly 1 in 3 data breach victims experienced identity fraud. Yet not only has the actual connection between data breaches and fraud continued to grow, but also media coverage of recent high-profile data breaches has served to reinforce the connection between data breaches and fraud in the minds of consumers.

Although access to highly sensitive or account-specific PII might render criminals more capable of perpetrating fraud, the information they seek is not restricted to this data. Social Security numbers are clearly the most comprised nonfinancial PII, especially at FIs (23% of fraud victims and industries other than retailers (32%). However, less sensitive, nonfinancial PII such as full name and physical address is right at the top of personal information compromised as reported by fraud victims across industries (see Figure 4).

The Proverbial ‘Keys to the Kingdom,’ Social Security Numbers Are the Most Compromised Type of Nonfinancial PII

Figure 4: Type of PII Breached and Misused, by Industry

<table>
<thead>
<tr>
<th>Type of PII</th>
<th>Percent of Fraud Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Security number</td>
<td>32%</td>
</tr>
<tr>
<td>Full name</td>
<td>23%</td>
</tr>
<tr>
<td>Physical address</td>
<td>18%</td>
</tr>
<tr>
<td>ATM PIN on your debit card</td>
<td>18%</td>
</tr>
<tr>
<td>PIN on your credit card</td>
<td>16%</td>
</tr>
<tr>
<td>Username and password for your online banking accounts</td>
<td>11%</td>
</tr>
<tr>
<td>Driver’s license number</td>
<td>10%</td>
</tr>
<tr>
<td>Email account and password such as that for Yahoo! Mail or Gmail</td>
<td>9%</td>
</tr>
<tr>
<td>Username and password for Internet payment accounts such as...</td>
<td>9%</td>
</tr>
<tr>
<td>Health insurance information</td>
<td>7%</td>
</tr>
<tr>
<td>Medical records</td>
<td>7%</td>
</tr>
<tr>
<td>Mobile phone and personal details on the phone</td>
<td>6%</td>
</tr>
<tr>
<td>A passport</td>
<td>6%</td>
</tr>
<tr>
<td>Username and password for nonfinancial Internet accounts such...</td>
<td>5%</td>
</tr>
<tr>
<td>Military ID card</td>
<td>4%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
</tbody>
</table>

Q12A. Thinking about the most recent fraud incident you experienced, what type of financial information was misused?

Financial account information, though, is the most heavily targeted by criminals and hackers (see Figure 5). This is unsurprising when considering that consumers whose card data was compromised experienced existing-card fraud (ECF) at a rate nearly eight times higher than that of all consumers (35.7% vs. 4.6%, respectively). The relationship between breached cards and fraud is increasing, with consumers whose credit or debit card number was breached in 2013 experiencing a 37% higher fraud rate than those whose card numbers were breached in 2012 (see appendix, Figure 22). This is not to say that breached SSNs are not of great value to criminals. The theft of SSNs places consumers at a substantial risk of fraud. SSN breach victims experience new-account fraud (NAF) at a rate nearly 18 times higher than that of all consumers.13

**Card Data Is the Foremost Target for Data Theft and Subsequent Misuse**

![Figure 5: Type of Financial Account Information Breached and Misused, by Industry](image)

Q12A. Thinking about the most recent fraud incident you experienced, what type of financial information was misused?

<table>
<thead>
<tr>
<th>Financial institution</th>
<th>Retail</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>A major credit card account number issued by my bank</td>
<td>41%</td>
<td>16%</td>
</tr>
<tr>
<td>A debit card account number issued by my bank</td>
<td>29%</td>
<td>14%</td>
</tr>
<tr>
<td>A bank account number (including checking, savings, or money market account)</td>
<td>10%</td>
<td>12%</td>
</tr>
<tr>
<td>An Alternative payments provider such as PayPal, Amazon payments, Google Checkout</td>
<td>6%</td>
<td>14%</td>
</tr>
<tr>
<td>Other types of payment card number (gift card / prepaid card)</td>
<td>4%</td>
<td>12%</td>
</tr>
<tr>
<td>A store credit or debit card account number</td>
<td>3%</td>
<td>12%</td>
</tr>
<tr>
<td>Another type of financial account (investment account / retirement account / insurance account / car loan / student...</td>
<td>1%</td>
<td>7%</td>
</tr>
<tr>
<td>Other</td>
<td>5%</td>
<td>9%</td>
</tr>
</tbody>
</table>

May 2014, n = 57, 69, 96
Base: Fraud victims whose misused information was compromised at above types of organizations.
© 2014 Javelin Strategy & Research

Late 2013 saw a rash of major retailer breaches, including those at Michaels, Neiman Marcus, and Target, where millions of records were compromised.\textsuperscript{14} It is not surprising that large retail merchant leads the list of organizations where consumers’ information was compromised (50%). A distant second on this list is the credit card issuer (22%), followed by consumers’ primary bank (16%).

This contrasts significantly with consumer perceptions before the aforementioned major retailer breaches, in which it was believed that the majority of breaches occurred within the financial industry.\textsuperscript{15} Given the high-profile nature of these breaches, the responsibility for these breaches was readily apparent to consumers. In previous retailer breaches, which received negligible media coverage, consumers might have been confused by FI and card issuer notification efforts designed to prepare them for card reissuance or a reduction in transaction approvals, and mistakenly assigned responsibility for breaches to FIs or card issuers.\textsuperscript{16}

**Large Retailers Are the Locus of the Highest Rate of Breach Notifications**

![Bar chart showing percentage of data breach victims by type of organization](image)

- Large retail merchant: 50%
- Credit card issuer: 22%
- Primary financial institution: 16%
- Healthcare provider: 14%
- Gas station: 8%
- Large online-only merchant: 8%
- Another financial institution: 8%
- Government agency: 7%
- Alternative payment provider: 7%
- University: 6%
- Social networking site: 5%
- Small online-only merchant: 5%
- Online gaming site: 5%
- Cloud application: 5%
- Restaurant or hotel: 5%
- Small retail merchant: 4%
- Virtual wallet provider: 4%
- Other organization: 4%

**Q8b:** Please indicate the type of organization where your information was compromised or stolen.

May 2014, \( n = 150 \)

Base: Fraud victims whose information was compromised in a data breach. © 2014 Javelin Strategy & Research


\textsuperscript{15} 2014 Data Breach Fraud Impact Report: Consumers Shoot the Messenger and Financial Institutions Take the Bullet, Javelin Strategy & Research, June 2014.

\textsuperscript{16} Ibid.
Although almost half of fraud victims don't know where the information used in the most recent fraud incident was compromised (49%), this is especially true for victims of events that were unrelated to a data breach such as a stolen device or wallet (88%), (see Appendix, Figures 20 and 21, respectively). Unfortunately, those victims who are unaware of how their data was compromised were not in a position to react until they were notified of the fraud — they could not take immediate steps, after the loss of their PII, to protect their identity nor could they prevent the continued theft of their PII from the compromised source.

Data breach victims, on the other hand, are more aware of their information compromise and related misuse, which might be due to breach notifications sent by the concerned organizations (see Appendix, Figure 21). Presumably, this contributes to data breach victims being less likely to suffer multiple fraud incidents compared with non-data breach victims (41% are data breach victims experience multiple fraud incidents vs. 50% of non-data breach victims), (see Figure 7), because knowing where the breach occurred and what information was compromised helps consumers take steps to help prevent future fraud.

Consumers Whose Information Was Compromised in a Data Breach Are Less Likely to Suffer From Multiple Fraud Incidents

Figure 7: Number of Identity Fraud Occurrences for Data Breach Victims and Non-Data Breach Victims

Q10. How many times have you been a victim of identity fraud?

Data Breach Victims
- 1 time: 7%
- 2 times: 25%
- 3 times: 59%

Non-Data Breach Victims
- 1 time: 4%
- 2 times: 20%
- 3 times: 50%
HOW CONSUMERS REACT TO FRAUD

It might be intuitive to think that once defrauded, victims would go overboard with preventive measures to avoid future information compromise. However, nearly 1 in 3 victims took no action after fraud occurred (see Figure 8). Of the many options available to victims to help protect their identity, actively monitoring financial accounts seems to be some of the most popular steps taken toward prevention as victims are most likely to sign up for activity alerts from their banks (24%) and begin using online banking (18%) (see Figure 8).

1 in 3 Victims Refrains From Taking Any Action After Victimization

Figure 8: Actions Taken by Victims as a Result of Experiencing Identity Fraud

Q19. As a result of being a fraud victim, are any of the following statements true of you? Top ten options shown

May 2014, n = 200
Base: All fraud victims.
© 2014 Javelin Strategy & Research
Especially clear is consumers’ low level of awareness of where to obtain assistance after they’ve been victimized. Although banks and credit card companies are the clear favorites among fraud victims, just over 2 in 5 victims contacted these organizations (44% and 43%, respectively) for advice, help, or more information. Interestingly, contacting the bank or a credit card company is more popular among victims whose PII was breached at a retailer than victims whose PII was breached at a FI (50% vs. 41%, respectively). Among victims who contacted these two agencies, satisfaction remains high (59% and 70%, respectively). Conversely, the proportion of fraud victims who contacted law enforcement, a credit monitoring service, or a federal agency is way lower — at 13%, 12%, and 10%, respectively—and victims are more likely to contact these agencies when their breach occurred at organizations other than FIs or retailers (see Figure 9).

**Victims Contact FIs and Credit Card Companies for Postfraud Assistance**

*Figure 9: Agencies Contacted After Fraud by All Fraud Victims and Victims Whose PII Was Breached, by Type of Organization Where Breach Occurred*

Q16. After discovering you were a victim of identity fraud, did you reach out to any of the following organizations for assistance, advice, or additional information?

- Your bank or credit union
- Your credit card company
- A credit bureau such as: Experian, Equifax, TransUnion, or Innovis
- I did not reach out to any organizations after discovering I was a victim of identity fraud
- Local or state law enforcement agency
- A credit monitoring or identity protection service provider such as: Identity Guard, LifeLock, etc.
- A federal agency such as the Federal Trade Commission, IRS, or Social Security Administration
- Local or state government agency such as the State Department of Motor Vehicles, State Attorney General’s Office, etc.
- Another organization

May 2014, n = varies 69 to 200
Base: All fraud victims, fraud victims by type of organization where information breached.
© 2014 Javelin Strategy & Research
Consumer trust is of paramount value to businesses, and being compromised in a data breach definitely puts these businesses at risk of losing customers. Fourteen percent of victims said they avoid certain merchants (see Figure 8), while nearly 6 in 10 victims said their trust in retailers has significantly decreased after their information was compromised (see Figure 10). Evidence can be found in the 2013 Target breach, which shook the core of the company as its stock price plummeted and key executives resigned in an effort to show responsibility and maintain consumer trust.\textsuperscript{17}

**When Breached Information Is Used to Commit Fraud, Victims Are Most Likely to Lose Trust in Retailers**

Figure 10: How Fraud Affected Data Breach Victims’ Level of Trust, by the Industry Where Breach Occurred

Q21. How has your most recent fraud incident impacted your level of trust with the organization where your information was compromised? “Somewhat decreased” and “significantly decreased” shown.  

\textsuperscript{17} 2014 Data Breach Fraud Impact Report: Consumers Shoot the Messenger and Financial Institutions Take the Bullet, Javelin Strategy & Research, June 2014.
In addition to losing the most trust in the wake of a data breach, retailers also fared poorly compared with FIs or other organizations when it came to fraud victims’ expectations that the organization would be able to protect their data in the future (10% vs. 24% vs. 26%, respectively) (see Figure 11). In the wake of recent high-profile breaches, it’s clear that retailers have a long and hard battle ahead of them to regain consumer trust and confidence.

Victims Are Also Least Confident That Retailers Can Protect Their Information in the Future

Figure 11: Data Breach Fraud Victims’ Level of Confidence That the Industry in Which Breach Occurred Could Protect Them From Future Fraud

Q26. How confident are you that this organization can protect you from fraud in the future?

May 2014, n = 57, 69, 96
Base: Fraud victims whose misused information was compromised at above types of organizations.
© 2014 Javelin Strategy & Research
VICTIMS’ EXPECTATIONS

Consumer awareness of breaches is on the rise, as all consumers, and fraud victims specifically, were more likely to be notified of a data breach in 2013, compared with 2012 (32% vs. 12% and 68% vs. 51%, respectively).18 Given such awareness of imminent or potential threat to their identities, consumers believe that taking appropriate steps to safeguard their data will help protect their identity. According to fraud victims, electronic monitoring of financial accounts (46%) and their credit card company’s fraud detection system (44%) prove to be the two most effective activities in preventing ID theft, placing almost the same level of responsibility on themselves and their credit card company (see Figure 12).

Interestingly, fraud victims believe signing up for an identity protection service is the least effective method — only 23% of victims picked this activity — to prevent ID theft, with victims in Minneapolis the least convinced of this option (12% of

Electronic Monitoring Considered Most Effective at Fraud Prevention

Figure 12: Perceived Effectiveness of Fraud Prevention Activities Among All Fraud Victims and by Metropolitan Area

fraud victims). Yet despite this perception, providing or subsidizing these services has become a remedy that government officials are pressing breached organizations to offer. In many cases victims might better understand the value of these services through experience, as commonly prescribed credit monitoring is of little value in preventing fraud related to breached credit and debit cards.19

Fraud victims do not seem to discriminate between businesses and FIs when assigning blame for a data breach. While 52% of victims consider businesses to be responsible for data breaches, 48% blame FIs (see Figure 13). This is true even among victims whose PII was breached at a FI (51% believe FIs should be held accountable and 46% believe retailers should be held accountable) and those whose PII was breached at a retailer (45% believe FIs should be held accountable and 51% believe retailers should be held accountable). Regardless, government agencies get the least of the blame, with only 24% of victims holding them accountable for a breach (see Figure 13).

Victims Believe All Organizations Should Be Held Accountable and Some Would Vote with Their Wallets

Figure 13: Industries That Should Be Held Accountable and Business Avoidance Postbreach, by Fraud Victims Whose Information Was Breached at FIs, Retailers, and Other Organizations

Q27. Please read each of the following statements carefully, and indicate your level of agreement on a scale of 1 to 10, where 1 = strongly disagree and 10= strongly agree. 9–10 shown.

While fraud victims hold all organizations involved accountable for information compromise, they feel differently based on whether the information was lost due to a data breach or an event unrelated to a data breach. Data breach victims are not only more likely to consider the breached organization responsible for protecting their accounts compared with non-data breach victims (49% vs. 40%), but they are also more likely to hold their FIs responsible for account protection (40% vs. 28%) (see Figure 14).

Data Breach Victims Are More Likely to Believe That Breached Organizations as Well as Their Banks Are Responsible for Protecting Accounts

Figure 14: Organizations That Should Be Held Responsible for Protecting Accounts During Recent Fraud, According to Non-data breach Victims and Data Breach Victims

Q29. Which of the following would you say were responsible for protecting your account in your most recent fraud incident?
When it comes to restoring their identities and lost funds, data breach victims maintain that breached organizations are responsible (53% of breach victims vs. 38% of nonbreach victims), while non-data breach victims say payment card companies are responsible (49% of breach victims vs. 60% of nonbreach victims) (see Figure 15).

Data Breach Victims Would Like to See Breached Organization Restore Lost Funds; Non-data breach Victims Say Card Companies Should Instead

Figure 15: Organizations That Should Be Held Responsible for Restoring Identity After Recent Fraud, According to Non-data breach Victims and Data Breach Victims

Q29b. Which of the following would you say were responsible for restoring your identity and lost funds in your most recent fraud incident?

- The organization/Website from where your information was stolen or compromised
- Your payment Card Company
- Your bank
- You

Percent of fraud victims

![Bar chart showing the percent of fraud victims who believe different entities should be held responsible for restoring their identity and lost funds. The chart shows that 53% of data breach victims believe the organization/Website is responsible, while 38% believe it is the non-data breach victims. For payment card companies, 49% of data breach victims believe they should be responsible compared to 60% for non-data breach victims. For banks, 47% of data breach victims believe they should be responsible compared to 46% for non-data breach victims. For individuals, 25% of data breach victims believe they should be responsible compared to 36% for non-data breach victims.](image-url)
Consumer patience seems to be a thing of the past as an overwhelming number of fraud victims believe they should be able to take legal action against companies where their information was breached (64%), (see Figure 16). Furthermore, this sentiment is consistent regardless of where the information was breached — 64% of FI breach victims, 66% of retailer breach victims, and 70% of another organization breach victims believe this is important.

Regardless of Where Information Was Breached, Victims Believe Consumers Should Be Able to Take Legal Action

**Figure 16: Agreement With Statement, by Type of Organization Where Information Was Breached**

Q30: Please indicate the degree to which you agree or disagree with the following statements on a scale of 1 to 5 where 1 = strongly disagree and 4 = strongly agree. Consumers should be able to take legal action against companies where their information is breached. Options 4 and 5 shown.

May 2014, n = 57, 69, 96
Base: Fraud victims whose misused information was compromised at above types of organizations.
© 2014 Javelin Strategy & Research
Data breaches can attract a constant stream of class-action lawsuits from consumers and businesses. For example, the Target breach has spawned 90 lawsuits. Moreover, as consumer awareness increases, the difference in the level of consumer protection and action by organizations can be seen when contrasting the Target breach with the earlier, prolific breach of TJX. In 2008, TJX provided credit monitoring services only to victims who faced a higher risk of ID theft. In 2013, Target provided this service to all customers, whether they were victims or not, due to consumer backlash and government pressure.

**Fraud Victims Favor Legal Action Against Breached Organization**

Figure 17: Fraud Victims’ Attitudes Regarding Data Breaches

Q30. Please indicate the degree to which you agree or disagree with the following statements on a scale of 1 to 5 where 1 = strongly disagree and 5 = strongly agree. 9-10 shown.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Percent of fraud victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breached organizations should be required to notify credit reporting agencies if there is a possibility that the stolen...</td>
<td>85%</td>
</tr>
<tr>
<td>Breached organizations should notify consumers whenever a data breach occurs no matter what</td>
<td>84%</td>
</tr>
<tr>
<td>The federal government should be responsible for ensuring that businesses adhere to data security standards, regardless of the...</td>
<td>70%</td>
</tr>
<tr>
<td>Breached organizations should be required to notify the media</td>
<td>67%</td>
</tr>
<tr>
<td>Consumers should be able to take legal action against companies where their information was breached</td>
<td>64%</td>
</tr>
<tr>
<td>Breached organizations should notify consumers of a data breach only when there is potential for harm stemming from the breach.</td>
<td>44%</td>
</tr>
<tr>
<td>The current federal data security requirements are sufficient for protecting health care and financial data</td>
<td>28%</td>
</tr>
</tbody>
</table>

May 2014, n = 200  
Base: All fraud victims  
© 2014 Javelin Strategy & Research

---

22 Ibid.
Although victims don’t hold government responsible for a breach, they do, however, expect federal government to ensure that businesses adhere to data security standards (70%), (see Figure 17). National data breach legislation is supported by the financial industry, which is calling for greater accountability from industries that store or transmit sensitive PII and financial account data. The financial industry’s recommendations are geared toward retailers, and industry groups — including the Independent Community Bankers of America and the National Association of Federal Credit Unions — are leading the lobbying effort to amend pending national legislation to reflect these recommendations.23

Businesses need to be aware of these initiatives and how consumer perception of existing legislation has created a climate in which proposed national legislation is likely to become law. Consumers are jittery about sharing their PII with organizations — only 28% of victims believe that current federal data security requirements are sufficient for protecting their data (see Figure 17). This is especially true for Minneapolis, where only 16% of victims believe they are adequate (see Figure 18).

**Fewer Than 2 in 5 Fraud Victims in Any Metro Area Surveyed Consider Federal Legislation Sufficient to Protect Consumer Data**

![Figure 18: Agreement With Statement, by Metropolitan Area](image)

### Figure 18: Agreement With Statement, by Metropolitan Area

- **Los Angeles**: 36% (28%)
- **Miami**: 30% (28%)
- **Chicago**: 28% (28%)
- **Minneapolis**: 16% (28%)

Q30: Please indicate the degree to which you agree or disagree with the following statements on a scale of 1 to 5 where 1 = strongly disagree and 5 = strongly agree. The current federal data security requirements are sufficient for protecting health care and financial data. Options 4 and 5 shown.

May 2014, n = 50
Base: Fraud victims by metropolitan area.
© 2014 Javelin Strategy & Research

The circumstances under which consumers must be notified of a breach varies, but these notifications offer an opportunity for organizations to educate affected consumers on the circumstances of the breach, their effect on the integrity of their identities, efforts undertaken by the breached organization to protect their identities going forward, and how consumers can ultimately protect themselves. Consumers clearly want to be in the know in case of a breach. While a little over 2 in 5 victims believe that consumers should be notified only when a breach has potential for harm, an overwhelming number of victims (84%) believe that breached organizations should notify consumers no matter the circumstance (see Figure 17). In addition, fraud victims also believe that breached organizations should notify credit reporting agencies (85%) and the media (67%) (see Figure 17).

**Fraud Victims Overwhelmingly Prefer Speedy Notification When It Comes to Data Breach**

*Figure 19: When Notification Should Be Provided After a Data Breach, by Fraud Victims*

Q31. Considering that a business or organization is required to notify affected customers of a data breach, how soon after a breach is confirmed should customers be notified?

May 2014, n = 200
Base: All fraud victims.
© 2014 Javelin Strategy & Research
When notifying consumers of a breach, speed is of the essence. This is not a new criticism — after TJX disclosed the details of its breach in 2007, it was heavily criticized by analysts, the media, and consumers alike for holding back information. ²⁴ Eighty-six percent of fraud victims believe consumers should be notified immediately no matter what (see Figure 19), providing the breach organizations a significant opportunity to maintain the relationship postbreach by dispelling any misinformation related to the event, reassuring consumers that the organization is now secure, and detailing best practices to prevent identity fraud. How and when consumers are notified can contribute to their perception of an organization after a breach, and organizations that wish to maintain a positive relationship with consumers should ensure transparent and immediate notification.

METHODOLOGY

In March 2014, the National Consumers League retained Javelin Strategy & Research to conduct a comprehensive research study on data breach and fraud victims’ experiences, behaviors, and attitudes. The NCL conducted an online survey of 200 fraud victims in the Chicago, Los Angeles, Miami, and Minneapolis metropolitan areas. The results of this study are not nationally representative and cannot be extrapolated to groups outside fraud victims in these four metropolitan areas. The overall margin of sampling error is +/- 6.93 percentage points at the 95% confidence level. The margin of error is larger for subsets of respondents.
APPENDIX

Nearly Half of Consumers Do Not Know Where the Information Used to Defraud Them Was Compromised

Figure 20: Type of Organization Where Information Was Compromised, by Most Recent Fraud Incident

Q13. To the best of your knowledge, where was the information used in your most recent fraud incident compromised?

Majority of Those Who Are Not Aware of the Location of Compromise Are Non-data breach Victims

Figure 21: Information Compromised in Most Recent Incident, by Victim Type

Q13. To the best of your knowledge, where was the information used in your most recent fraud incident compromised?
Fraud Incidence is Increasingly Correlated with Card Breaches

Figure 22: Rate of Fraud Victimization by Type of Data Breached

Q5: How long ago did you discover that your personal or financial information had been misused? In the past 12 months.

October 2012 - 2013, n varies 75 - 320
Base: Data breach victims in the past 12 months by type of information breached.

© 2014 Javelin Strategy & Research
ABOUT JAVELIN

Javelin Strategy & Research, a division of Greenwich Associates, provides strategic insights into customer transactions, increasing sustainable profits and creating efficiencies for financial institutions, government agencies, payments companies, merchants, and other technology providers. Javelin’s independent insights result from a uniquely rigorous three-dimensional research process that assesses customers, providers, and the transactions ecosystem.

Authors: Al Pascual, Senior Analyst, Fraud & Security
Publication Date: June 2014
Editor: Oie Lian Yeh