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

**METHODODOLOGY**

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.


**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 fraud instead of existing non-card account fraud. 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. 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

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

<table>
<thead>
<tr>
<th>Year</th>
<th>All consumers</th>
<th>Non data breach victims</th>
<th>Data breach victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>4.4%</td>
<td>1.4%</td>
<td>22.5%</td>
</tr>
<tr>
<td>2011</td>
<td>4.9%</td>
<td>2.4%</td>
<td>18.9%</td>
</tr>
<tr>
<td>2012</td>
<td>5.3%</td>
<td>2.9%</td>
<td>11.8%</td>
</tr>
</tbody>
</table>
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, 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.

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

<table>
<thead>
<tr>
<th>Companies Mentioned</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>MasterCard</td>
</tr>
<tr>
<td>American Express</td>
<td>McAfee</td>
</tr>
<tr>
<td>Apple</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Discover</td>
<td>PayPal</td>
</tr>
<tr>
<td>EBay</td>
<td>Target</td>
</tr>
<tr>
<td>Europay</td>
<td>Trend Micro</td>
</tr>
<tr>
<td>Facebook</td>
<td>Visa</td>
</tr>
<tr>
<td>Global Payments</td>
<td>Wal-Mart</td>
</tr>
<tr>
<td>Google</td>
<td>Zappo’s</td>
</tr>
<tr>
<td>Macy’s</td>
<td></td>
</tr>
</tbody>
</table>
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](mailto:marketing@javelinstrategy.com)

3) **Fax or Mail** using the form below:

<table>
<thead>
<tr>
<th>Report Title</th>
<th>Publication Date</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.