



## Mobile Payments & Online Shopping Survey of U.S. Consumers

---

### Sponsored by ThreatMetrix

Independently conducted by Ponemon Institute LLC

Publication Date: October 2011

# Mobile Payments & Online Shopping Survey of U.S. Consumers

October 2011

## Part 1. Introduction

Increasingly, consumers are turning to new online technologies and social media tools to engage in a variety of transactions. While they may offer more convenience, they also pose potential risks to the security of personal information and financial assets. Do consumers understand these risks and are they taking appropriate precautions?

Ponemon Institute is pleased to present the results of the *Mobile Payments and Online Shopping Survey*. Sponsored by Threatmetrix, the survey focused on issues relating to consumers' concerns about mobile payments, mobile banking, eCommerce, social network shopping and government payments.

The study surveyed 722 U.S. consumers who self-reported that they are active users of the Internet. On average, respondents spend 24 hours per week on the Internet. Fifty-seven percent make purchases daily or weekly. Despite the amount of time spent on the Internet, 79 percent have either some concerns (53 percent) or serious concerns (26 percent) about fraud when shopping online and 72 percent are concerned in general about becoming a victim of online fraud.

Forty-five percent of respondents report that they have been a victim of online fraud. However, this could include not only identity theft and the loss of financial assets but phishing and other online scams that attempt to gain consumers' personal information.

## Summary of findings

The study looked at five different activities consumers engage in when online. These are: mobile payments, mobile banking, eCommerce, shopping on social networks, and government payments. Our key findings are as follows.

### ▪ Mobile Payments

**Commitment to protect consumers from online fraud is important.** Sixty-one percent of respondents in our study own a smartphone and forty percent of these respondents pay bills using these devices. Online services most often used to make payments are PayPal (61 percent) and credit cards (53 percent). Eighty-four percent say that a commitment to prevent fraud is either very important or important when selecting an online payment service provider.

### ▪ Mobile Banking

**Concerns about security are keeping consumers from mobile banking.** Only 29 percent of respondents conduct mobile banking. However, those who do so say it is because of convenience (51 percent) and increased security (25 percent). In fact, 67 percent of consumers in the study who use mobile banking feel completely or partially protected. On average, they plan to use mobile banking for approximately 40 percent of their online purchases. Those who do not conduct mobile banking say it is because of diminished security (51 percent).

### ▪ eCommerce

**Consumers will be shopping both in stores and online during the coming Cyber Monday and Holiday season.** According to 67 percent of respondents their online purchases on Cyber

Monday and during the holiday season will either exceed in-store purchases (33 percent) or stay at the same level (34 percent). The most popular devices to be used are desktop or laptop computers (49 percent) or smartphones such as Androids, iPhones or Blackberry (37 percent). The most popular purchases using a mobile payments option on a smartphone or tablet are: groceries (78 percent), music downloads (77 percent), online service subscriptions or memberships (75 percent) and apps for smartphones or tablets (73 percent).

To protect themselves from online fraud and other abuses, 56 percent only use mobile banking applications that they trust, 55 percent know where their computer or mobile device is at all times, 52 percent only shop at websites that they know and trust and 50 percent only use a mobile device that is dependable and trusted.

- **Shopping on Social Networks**

**Google is more trusted than Facebook.** Fifty-three percent of consumers do not seem to believe that Facebook's storefronts are committed to protecting them against fraudsters and 23 percent are unsure. More than half (51 percent) say Google is more effective than Facebook at keeping them safe from online criminals.<sup>1</sup>

- **Government Mobile Payments**

**When it comes to paying the government, consumers prefer writing a check to making a mobile payment.** Only 11 percent of respondents say they have made a mobile payment to the government. Thirty-seven percent say they would never make a mobile payment to government and 10 percent are unsure. The main reason is that 63 percent feel more comfortable making a traditional payment such as a written check and 61 percent say they like having written proof when making payments to the government. In addition, 34 percent do not trust government to protect them from fraud and abuse when online or making mobile payments. Similarly, 34 percent do not trust government to protect them against the consequences of cyber warfare.

---

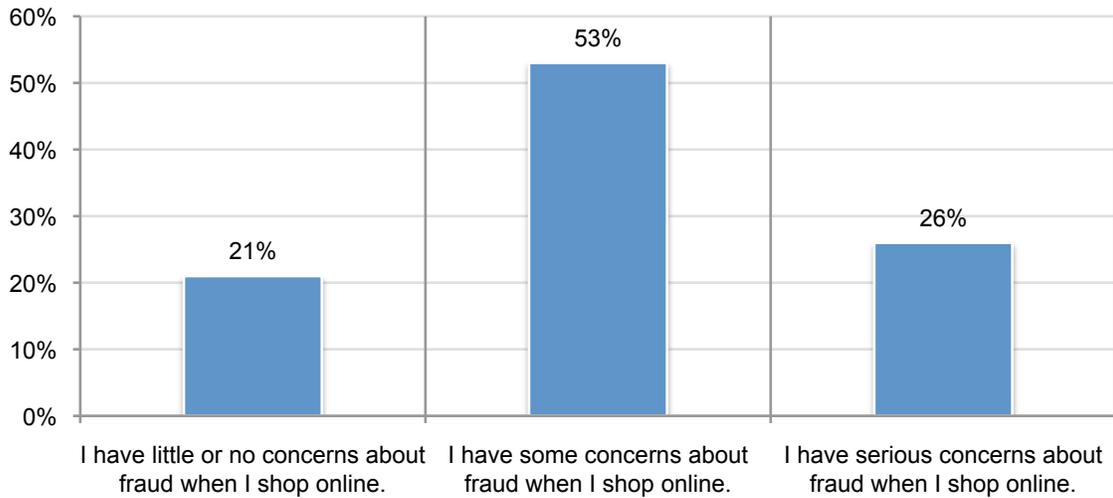
<sup>1</sup>Our survey only mentions Google and Facebook because their popularity among U.S. consumers.

## Part 2. Key Findings

The study looked at five activities consumers engage in when online or in social networks. These are: mobile payments, mobile banking, eCommerce, shopping on social networks and mobile payments to government entities. This section provides a detailed analysis of findings from each one of these five activities included in our survey.

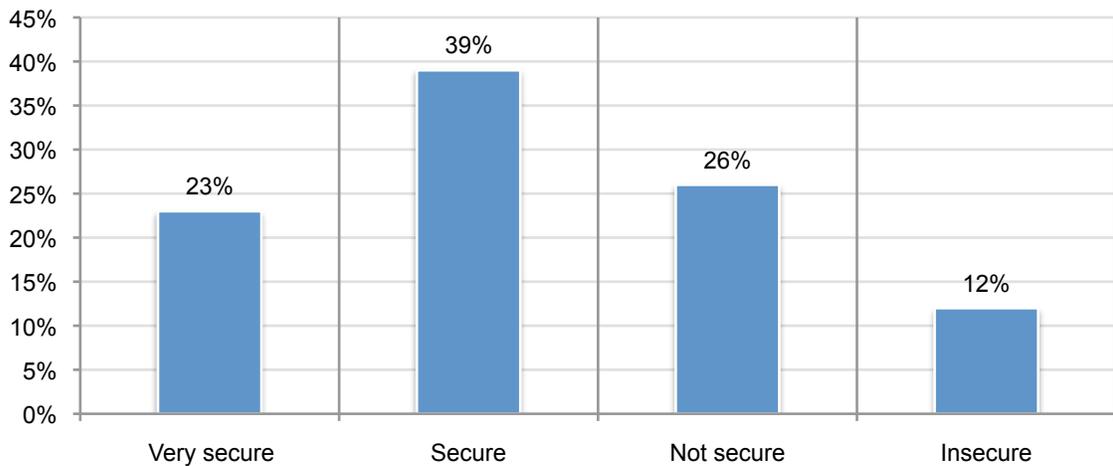
As shown in Bar Chart 1, more than half (79 percent) of consumers have concerns about fraud when shopping online.

**Bar Chart 1: Please choose the one statement that best describes your degree of concern about fraud when you shop online.**



Despite these concerns, 62 percent of respondents feel very secure (23 percent) or secure (39 percent) when they shop online (as shown in Bar Chart 2).

**Bar Chart 2: In terms of the possibility of fraud and other abuses, how secure do you feel when you shop online?**

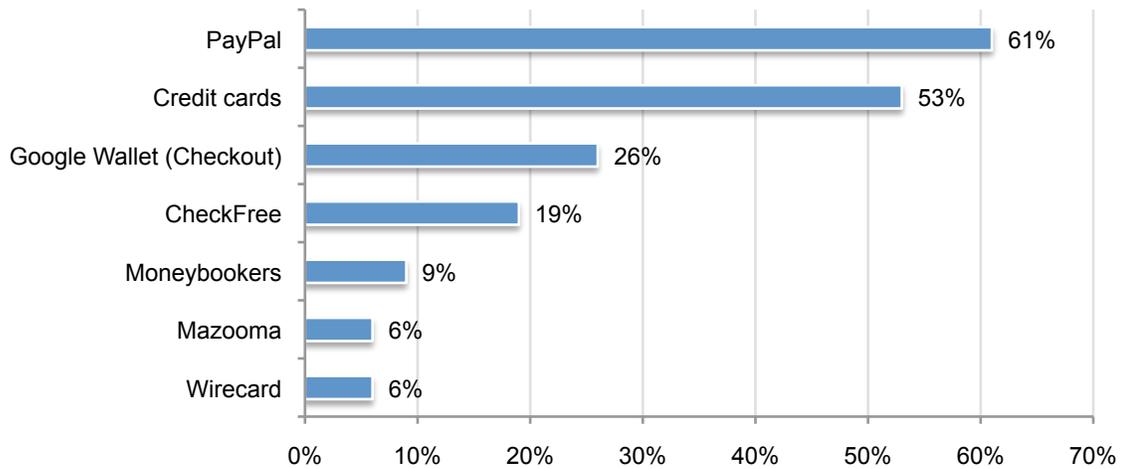


## Mobile Payments

**Commitment to protect consumers from online fraud is important.** Sixty-one percent of respondents in the study own a smartphone and 40 percent of these respondents pay bills using these devices.

According to Bar Chart 3, online services most often used to make payments are PayPal (61 percent) and credit cards (53 percent). Eighty-four percent say that a commitment to prevent fraud is either very important or important when selecting an online payment service provider.

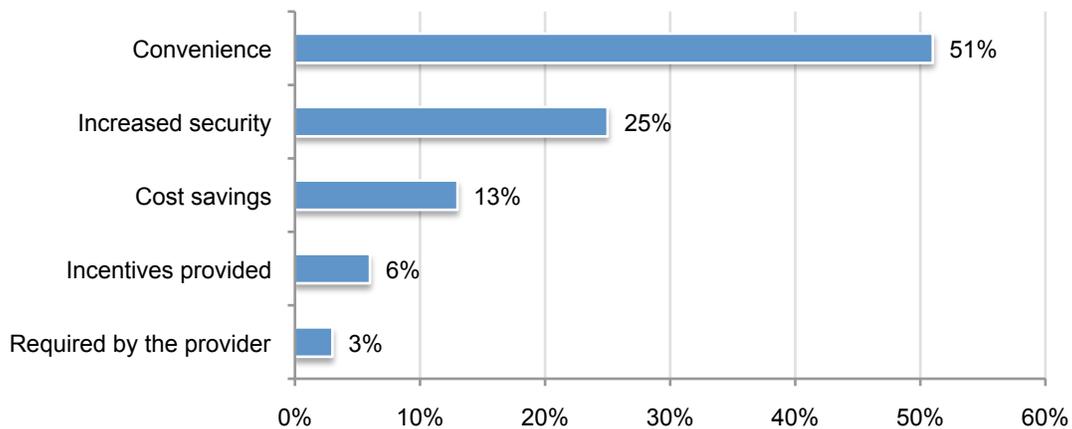
**Bar Chart 3: What online payment services do you normally use when you do a mobile payment or shop on the Internet?** The top two choices are indicated.



## Mobile Banking

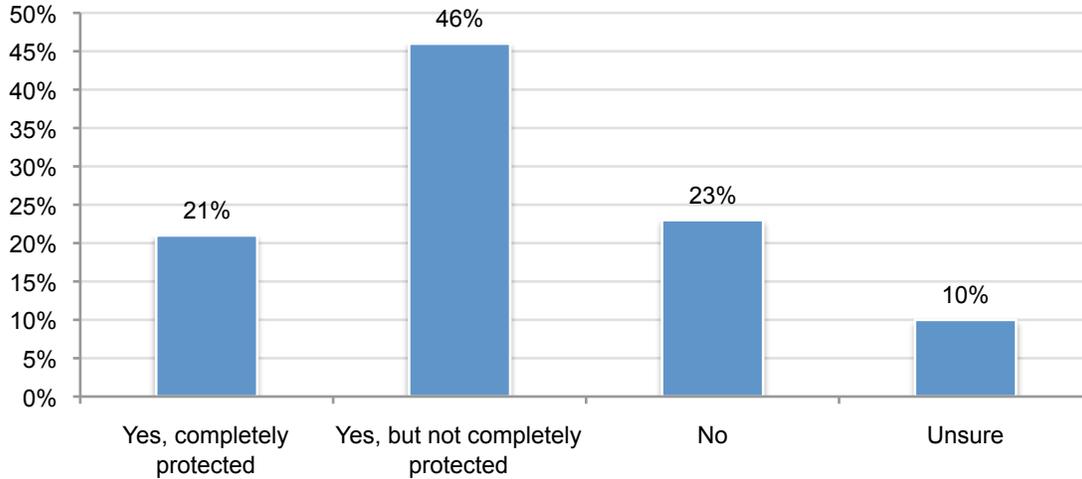
**Concerns about security are keeping consumers from mobile banking.** Only 29 percent of consumers in the study conduct mobile banking. However, Bar Chart 4 shows that those who use mobile banking say it is because of convenience (51 percent) and increased security (25 percent). On average, in the near future respondents plan to use mobile banking for approximately 40 percent of their online purchases. Those who do not engage in mobile banking say they are concerned about diminished security (51 percent).

**Bar Chart 4: What is the main reason why you do mobile banking?**



As shown in Bar Chart 5, when asked if they feel protected against fraudsters when doing mobile banking, 67 percent of consumers in the study say they feel completely or partially protected.

**Bar Chart 5: Do you feel protected against fraudsters when doing mobile banking?**



### eCommerce

**Consumers will be shopping both in stores and online during the coming Cyber Monday and Holiday season.** According to 67 percent of respondents (see Bar Chart 6), their online purchases on Cyber Monday and during the holiday season will either exceed in-store purchases (33 percent) or stay at the same level (34 percent).

**Bar Chart 6: What best describes your shopping plans this coming Cyber Monday and Holiday Season?**



The most popular devices used are desktop or laptop computers (49 percent) or smartphones such as Androids, iPhones or BlackBerry (37 percent). As shown in Table 1, the most popular purchases using a mobile payments option on a smartphone or tablet are music downloads (77 percent), online service subscriptions or memberships (75 percent) and apps for smartphone or

tablets (73 percent), according to survey results. Consumer electronics ranked slightly above clothing, at 48 percent and 43 percent, respectively.

Table 1. From the list below, please check all items that you would <b>purchase</b> using a mobile payments option on your smartphone or tablet computer.	Pct%
Music downloads	77%
Online service subscription or membership	75%
Apps for smartphone or tablet	73%
Gas for auto	69%
Video or game rental	65%
Travel including airlines, hotels and rental car	52%
Consumer electronics including computers	48%
Clothing	43%
Donations to a charity or religious organization	38%
Government services, fees or taxes	31%
Legal or tax services	25%
Medical services	23%
Home mortgage payments	22%
Education tuition or other fees	20%
Automobile purchase or loan payments	19%

More than half (51 percent) of respondents believe the fraud risk is the same on a smartphone, tablet, desktop and laptop computer. Only 19 percent say fraud risk is higher on a smartphone or tablet than on a desktop or laptop computer.

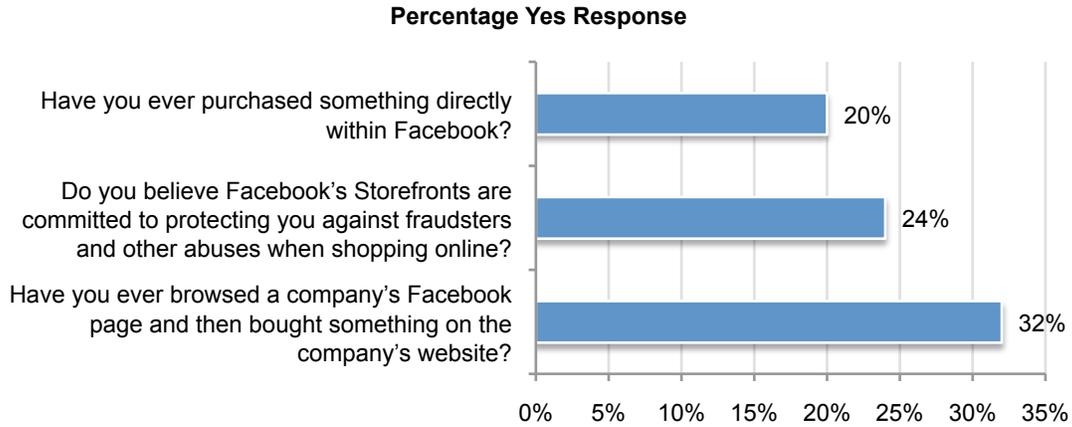
To protect themselves from online fraud and other abuses, Table 2 reports that 56 percent of respondents only use mobile banking applications that they trust, 55 percent know where their computer or mobile device is at all times, 52 percent only shop at websites that they know and trust and 50 percent only use a mobile device that is dependable and trusted.

Table 2. What precautions are you taking to protect yourself against online fraud and other abuses? Please select all that apply.	Pct%
I only use mobile banking applications that I trust	56%
I know where my computer or mobile device is at all times	55%
I only shop at websites that I know and trust	52%
I only use a mobile device that is dependable and trusted	50%
I choose a high privacy and security setting in my computer's browser	43%
I use anti-virus and anti-malware on my computer or mobile device	43%
I delete all cookies that I do not recognize	38%
I closely scan all bank statements for unusual transactions	38%
I limit the type of information shared with online companies	34%
I do not download free software from unknown sources	34%
I do not use insecure wireless connections	32%
I log-off or set my setting to a secure screen saver when it is not in use	29%
I encrypt data stored on my computer or mobile device	26%
I use and frequently change passwords only known to me	23%
I use a pseudonym rather than my real name	19%
I use an identity protection service	17%
I only shop at websites with a trust mark or seal indicating safe practices	16%

## Shopping on Social Networks

**Consumers seem reticent to shop on social networks.** Social networking shopping is lagging behind other online shopping venues. Only 32 percent of consumers surveyed have browsed a company’s Facebook page and then bought something on the company’s website. Only 20 percent have purchased something directly within Facebook. See Bar Chart 7.

**Bar Chart 7: Perceptions about Facebook as an online shopping venue.** Each bar represents the yes (affirmative) response to the question as stated.

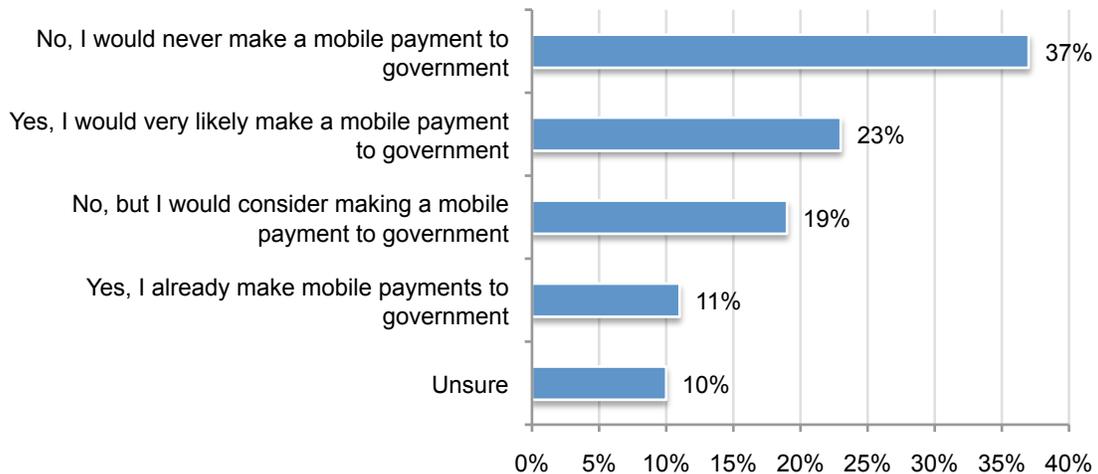


Security may be an issue when shopping online. Fifty-three percent of consumers do not seem to believe that Facebook’s storefronts are committed to protecting them against fraudsters and 23 percent are unsure. More than half (51 percent) say Google is more effective than Facebook at keeping them safe from online criminals.

## Government Payments

**Consumers prefer writing a check to making a mobile payment when paying the government.** Only 11 percent of respondents say they have made a mobile payment to the government, according to Bar Chart 8. Thirty-seven percent say they would never make a mobile payment to government and 10 percent are unsure.

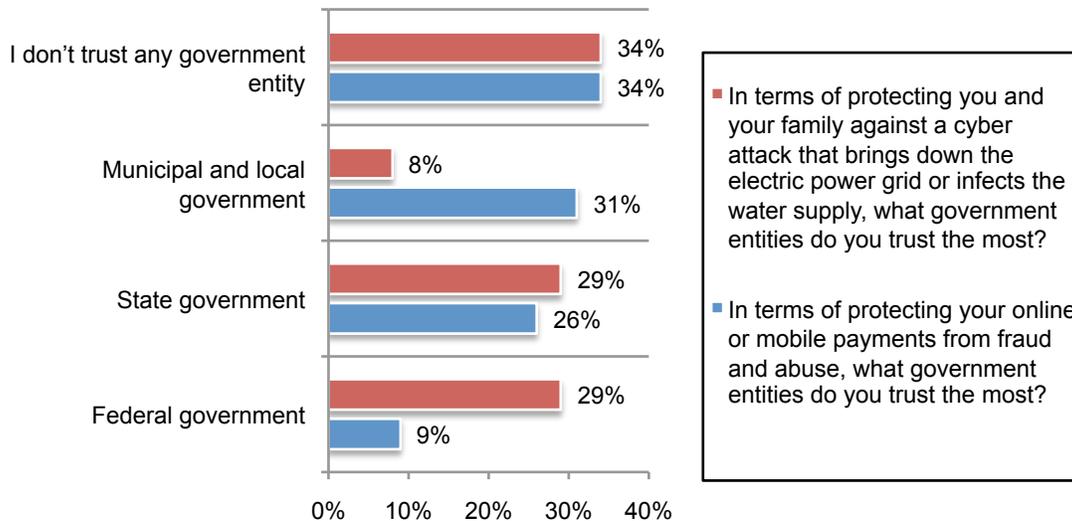
**Bar Chart 8: Would you ever make a mobile payment from your smartphone or tablet to remunerate fees to a government entity?**



The main reason is that most (63 percent) feel more comfortable making a traditional payment such as a written check and 61 percent say they like having written proof when making payments to the government. (Multiple responses were allowed).

**Consumers lack trust in the government's ability to protect them from online fraud and abuse.** As shown in Bar Chart 9, 34 percent of consumers surveyed do not trust government to protect them from fraud and abuse when online or making mobile payments. The federal government is least trusted (9 percent). Only 26 percent trust state government and 31 percent trust municipal and local government.

**Bar Chart 9: What government entities (if any) do you trust to protect you?**



Consumers have more trust in government's ability to protect them from the consequences of cyber warfare than online fraud. Twenty-nine percent trust the federal government and the same percentage say they trust state government. Thirty-four percent do not trust any government entity to protect them from online fraud and abuse.

### **Part 3. Differences between Elite vs. Mainstream Respondents**

We divided the respondents into two categories. The “elite” group of respondents spends more than 20 hours online and does at least two of the following online activities: blogging, paying bills or social media and eCommerce. In this category the elites are 219 respondents representing 30 percent of the total sample of respondents. In the category we refer to as “mainstream” users of the Internet are 503 respondents or 70 percent of the total sample.

In general, members of the elite subsample are younger, better educated and more likely to be gainfully employed than mainstream respondents. In addition, the elite subsample contains a higher proportion of female respondents. Following are the most salient differences between elites and mainstream respondents who participated in the study.

- Elites are less concerned about becoming a victim of fraud or feel more secure when shopping online than mainstream respondents.
- Elites are more likely than mainstream respondents to consider security when choosing an online bank, payment processor and commercial websites.
- Elites are more likely to own or use a smartphone or tablet computer. In addition, they are more likely to use their smartphone or tablet to make mobile payments than mainstream respondents.
- Elites are more likely to connect a personally owned mobile device such as a smartphone or tablet computer to their employer’s network or enterprise systems.
- Elites are more likely than mainstream respondents to choose an Internet payment service such as PayPal than use their credit or debit card when making mobile payments or when shopping online.
- Elites are more likely to feel fully or partially protected against fraudsters when doing mobile banking than mainstream respondents.
- Elites anticipate making more online purchases than conventional (in-store) purchases this coming Cyber Monday and during the Holiday season than mainstream respondents. In addition, elites are more likely to consummate their online purchases using a mobile payment feature contained on their smartphone.
- Elites are more likely to trust Facebook than Google. However, the margin of difference is narrower than for mainstream respondents.
- Location analysis revealed that respondents located in California, Massachusetts, Colorado, New York and Georgia have a higher proportion of elites than in other states.

#### Part 4. Methods

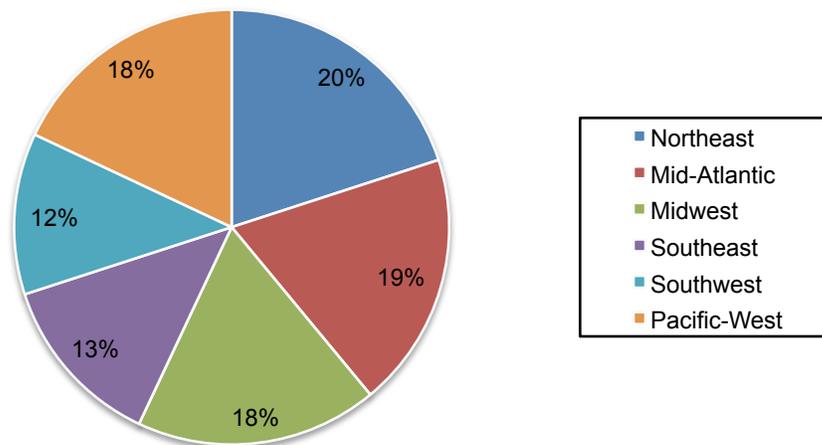
Table 3 summarizes the sample response for this study. Our sampling frame of adult-aged consumers consisted of 25,699 individuals located in all major regions of the United States. This resulted in 801 respondents completing the web-based survey of which 79 were rejected for reliability issues. Our final sample was 722 respondents (2.8 percent response rate).

Table 3. Sample response	Freq
U.S. consumer sample frame	25,699
Invitations sent	22,350
Total returns	801
Rejected surveys	79
Final sample	722
Response rate	2.8%

Forty-six percent of respondents say they are active users of social networks. Fifty-eight percent say they are the head of their household. Fifty-one percent of respondents are female and 49 percent are male.

Pie Chart 1 shows the distribution of respondents according to six regions in the United States. The Northeast is the largest region representing 20 percent of the total sample. The smallest region is the Southwest at 12 percent of the total sample.

**Pie Chart 1: Geographic distribution of respondents**



The following tables provide other key demographics about respondents in this study in a percentage frequency format.

Table 4. Mobile data-bearing devices respondents' regularly use	Pct%
iPod or similar MP3 player	69%
Desktop computer	65%
Laptop computer	63%
Smartphone	61%
Tablet computer	12%
Other	5%

Table 5. Respondents' employment status	Pct%
Full time employee	44%
Homemaker	16%
Unemployed	10%
Part time employee	8%
Business owner	8%
Retired	6%
Student	6%
Active military	2%
Total	100%

Table 6. Respondents' highest level of education	Pct%
University or College	39%
High School	29%
Vocational	24%
Post Graduate	6%
Doctorate	1%
Other	1%
Total	100%

Table 7. Respondents' age range	Pct%
18 to 25	22%
26 to 35	24%
36 to 45	18%
46 to 55	15%
56 to 65	11%
66 to 75	9%
75+	1%
Total	100%

## Part 5. Conclusion

This study offers some interesting results. Surprisingly, nearly one in three consumers believe the fraud risk to be lower on a smartphone or tablet than on a desktop or laptop computer. When asking the elite that number increased to 39 percent. In general, those consumers in the elite category often have different perceptions of online shopping and online fraud than those who are less frequent users. We learned that consumers who are mainstream and have a high propensity to use the Internet for shopping, banking, gaming, social media interactions, and other activities, appear to have a stronger sense of security online -- which is not exclusive only to desktops and laptops.<sup>2</sup>

Trust is important when shopping online. As we learned in a previous consumer study sponsored by Threatmetrix, online security is a major concern for consumers.<sup>3</sup> Forty-three percent say that perceptions about the security of an online bank or business website can affect their use of the site. In addition, when selecting an online payment service provider their commitment to protect consumers from fraud is very important or important for 84 percent of respondents. These findings demonstrate that spending on security is an important investment for online merchants.

### Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. The Ponemon Institute sent surveys to a representative sample of adult-aged consumers located in all major regions of the United States. Despite non-response tests, it is always possible that consumers who did not participate are substantially different in terms of underlying beliefs from those who completed the survey.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who use the Internet. We also acknowledge that responses from paper, interviews or telephone might result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from respondents. While certain checks and balances were incorporated into our survey evaluation process, there is always the possibility that certain respondents did not provide responses that reflect their true opinions.

---

<sup>2</sup>It is possible that consumers are lulled into a false sense of security as long as they do not experience fraud or other problems when online or in social networks.

<sup>3</sup>2011 Consumers' Reaction to Online Fraud (sponsored by ThreatMetrix) Ponemon Institute, April 2011.

## Appendix: Detailed Survey Findings

The following frequency tables provide all survey results for 722 consumers located in the United States. All survey results were gathered in September 2011.

### Part 1: Background

Q1. In an average week, about how much time do you spend on the Internet?	Pct%
Less than 1 hour	2%
Between 1 to 5 hours	4%
Between 6 to 10 hours	9%
Between 10 to 20 hours	33%
Between 20 to 40 hours	31%
More than 40 hours	21%
Total	100%

Q2. Which of the following online activities do you do in a typical week?	Pct%
Shopping	52%
Blogging	11%
Search & information gathering	69%
Banking & paying bills	35%
Entertainment such as music or gaming	39%
Emailing & communications	54%
Social networking	60%
Watching a video	45%
Total	365%

Q3. When was the last time you made an online purchase?	Pct%
Today	12%
Yesterday	13%
Last week	32%
Last month	25%
Last year	10%
Never (Go to Part 3)	3%
Can't recall	5%
Total	100%

Q4. Please choose the statement that best describes your degree of concern about fraud when you shop online:	Pct%
I have little or no concerns about fraud when I shop online.	21%
I have some concerns about fraud when I shop online.	53%
I have serious concerns about fraud when I shop online.	26%
Total	100%

Q5. In terms of the possibility of fraud and other abuses, how secure do you feel when you shop online?	Pct%
Very secure	23%
Secure	39%
Not secure	26%
Insecure	12%
Total	100%

Q6. Have you been the victim of online fraud?	Pct%
Yes	43%
No	57%
Total	100%

Q7. How concerned are you about becoming a victim of online fraud?	Pct%
Very concerned	30%
Concerned	42%
Not concerned	28%
Total	100%

Q8. Do your perceptions about the security of an online bank or business website affect your use that site?	Pct%
Yes	43%
No	38%
Unsure	19%
Total	100%

Q9. Do you use your mobile device to connect to your employer's network or enterprise systems? Computed only for respondents who are employed.	Pct%
Yes, frequently	40%
Yes, occasionally	36%
Never	24%
Total	100%

**Part 2: Mobile payments**

Q10. Do you own or use a smartphone?	Pct%
Yes	61%
No (Go to Part 3)	39%
Total	100%

Q11. Do you ever use your smartphone or tablet to make a mobile payment?	Pct%
Yes, frequently	11%
Yes, at least once	29%
No (Go to Part 3)	60%
Total	100%

Q12. What online payment services do you normally use when you do a mobile payment or shop on the Internet? Please check only your top two choices.	Pct%
PayPal	61%
CheckFree	19%
Google Wallet (Checkout)	26%
Wirecard	6%
Moneybookers	9%
Mazooma	6%
Credit cards	53%
Other (please specify)	2%
None of the above	9%
Total	191%

Q13. When selecting an online payment service provider, how important is their commitment to protect you from fraud and other abuses?	Pct%
Very important	55%
Important	29%
Not important	11%
Irrelevant	5%
Total	100%

### Part 3: Mobile Banking

Q14a. Do you conduct mobile banking?	Pct%
Yes	29%
No	71%
Total	100%

Q14b. If yes, why?	Pct%
Convenience	51%
Cost savings	13%
Increased security	25%
Incentives provided	6%
Required by the payment service provider	3%
Other (please specify)	0%
Don't know	2%
Total	100%

Q14c. If no, why not?	Pct%
Inconvenience	13%
Cost increases	6%
Diminished security	51%
Privacy concerns	23%
Other (please specify)	2%
Don't know	5%
Total	100%

Q15. Do you feel protected against fraudsters when doing mobile banking?	Pct%
Yes, completely protected	21%
Yes, but not completely protected	46%
No	23%
Unsure	10%
Total	100%

Q16. What statements best convey why you do mobile banking when shopping on the Internet? Select only your top two choices.	Pct%
Mobile banking provides better security	48%
Mobile banking provides greater convenience	71%
Mobile banking is more flexible	54%
Mobile banking provide better incentives	6%
Mobile banking is cheaper to use	11%
None of the above	10%
Total	200%

Q17. [Only for 14a = Yes response] What is the approximate percentage of online purchases you will make this year using mobile banking rather than traditional payments (by credit card, debit card or check)? Your best guess is welcome.	Pct%
None	6%
1 to 5%	11%
6 to 10%	9%
11 to 25%	15%
26 to 50%	20%
51 to 75%	23%
76 to 100%	16%
Total	100%

**Part 4: eCommerce**

Q18. From the list below, please check all items that you would <b>purchase</b> using a mobile payments option on your smartphone or tablet.	Pct%
Gas for auto	69%
Groceries	78%
Video or game rental	65%
Music downloads	77%
Online service subscription or membership	75%
Apps for smartphone or tablet	73%
Travel including airlines, hotels and rental car	52%
Consumer electronics including computers	48%
Clothing	43%
Medical services	23%
Legal or tax services	25%
Donations to a charity or religious organization	38%
Government services, fees or taxes	31%
Automobile purchase or loan payments	19%
Home mortgage payments	22%
Education tuition or other fees	20%
None of the above	19%

Q19. What best describes your shopping plans this coming Cyber Monday and Holiday Season?	Pct%
My online purchases will likely exceed in-store purchases	33%
My online and in-store purchases will likely be at about the same level	34%
My in-store purchases will likely exceed online purchases	17%
I'm not planning to shop online or in stores	16%
Total	100%

Q20. What device do you plan to use on Cyber Monday and this Holiday Season when shopping online? Please select only one top choice.	Pct%
Desktop or laptop computer	49%
Tablet computer (such as the iPad)	12%
Smartphone (such as an Android, iPhone or BlackBerry)	37%
Other (please specify)	2%
Total	100%

Q21. What precautions are you taking to protect yourself against online fraud and other abuses? Please select all that apply.	Pct%
I only use mobile banking applications that I trust	56%
I only use a mobile device that is dependable and trusted	50%
I choose a high privacy and security setting in my computer's browser	43%
I delete all cookies that I do not recognize	38%
I use a pseudonym rather than my real name	19%
I limit the type of information shared with online companies	34%
I only shop at websites that I know and trust	52%
I only shop at websites with a trust mark or seal indicating safe practices	16%
I use and frequently change passwords only known to me	23%
I encrypt data stored on my computer or mobile device	26%
I use anti-virus and anti-malware on my computer or mobile device	43%
I log-off or set my setting to a secure screen saver when it is not in use	29%
I know where my computer or mobile device is at all times	55%
I do not use insecure wireless connections	32%
I use an identity protection service	17%
I closely scan all bank statements for unusual transactions	38%
I do not download free software from unknown sources	34%
None of the above	23%

Q22. What statement best describes the risk of fraud on a mobile device such as a smartphone versus fraud risk using a desktop or laptop computer?	Pct%
Fraud risk is higher on a smartphone or tablet than on a desktop or laptop computer.	19%
Fraud risk is lower on a smartphone or tablet than on a desktop or laptop computer.	30%
Fraud risk is the same on a smartphone, tablet, desktop and laptop computer.	51%
Total	100%

**Part 5: Shopping on social networks**

Q23. Have you ever browsed a company's Facebook page and then bought something on the company's website?	Pct%
Yes	32%
No	68%
Total	100%

Q24. Have you ever purchased something directly within Facebook?	Pct%
Yes	20%
No	80%
Total	100%

Q25. Do you believe Facebook's Storefronts are committed to protecting you against fraudsters and other abuses when shopping online?	Pct%
Yes	24%
No	53%
Unsure	23%
Total	100%

Q26. Who do you believe is <b>more effective</b> at protecting you against fraudsters and other abuses when shopping online?	Pct%
Google	51%
Facebook	26%
Both are equal	13%
Undecided	10%
Total	100%

Q27. Have you bought (or do you plan to buy) a "virtual gift" for someone you know?	Pct%
Yes	9%
No	68%
Unsure (or don't know what a virtual gift is)	23%
Total	100%

**Part 6: Government payments**

Q28a. Would you ever make a mobile payment from your smartphone or tablet to remunerate fees to a government entity such as an income tax payment to the IRS, excise fees to your state DMV, local real estate taxes and so forth?	Pct%
Yes, I already make mobile payments to government	11%
Yes, I would very likely make a mobile payment to government	23%
No, but I would consider making a mobile payment to government	19%
No, I would never make a mobile payment to government	37%
Unsure	10%
Total	100%

Q28b. If no, why not? Please check all that apply.	Pct%
I don't want the government to have access to my bank accounts and other personal information	44%
I don't trust government with the information contained in my mobile phone app or mobile wallet	56%
I feel more comfortable making a traditional payment such as a written check	63%
I like having written proof when making payments to the government	61%
Other (please specify)	4%
Total	228%

Q29. In terms of protecting your online or mobile payments from fraud and abuse, what government entities do you trust the most? Please select only one choice.	Pct%
Federal government	9%
State government	26%
Municipal and local government	31%
I don't trust any of the above	34%
Total	100%

Q30. In terms of protecting you and your family against cyber warfare (such as a cyber attack that brings down the electric power grid or infects the water supply), what government entities do you trust the most? Please select only one choice.	Pct%
Federal government	29%
State government	29%
Municipal and local government	8%
I don't trust any of the above	34%
Total	100%

### Part 7: Demographics

D1. Please check the devices you regularly use:	Pct%
Smartphone	61%
Tablet (iPad)	12%
Laptop computer	63%
Desktop computer	65%
iPod or similar MP3 player	69%
Other (specify)	5%
Total	275%

D2. What is your present employment status?	Pct%
Full time employee	44%
Part time employee	8%
Homemaker	16%
Business owner	8%
Retired	6%
Student	6%
Active military	2%
Unemployed	10%
Total	100%

D3. Approximately, when did you start using the Internet or start doing email?	Pct%
Within the past 2 years	2%
3 to 5 years	5%
6 to 10 years	41%
More than 10 years	52%
Total	100%

D4. What is your highest level of education attained?	Pct%
High School	29%
Vocational	24%
University or College	39%
Post Graduate	6%
Doctorate	1%
Other	1%
Total	100%

D5. Please check your age range	Pct%
18 to 25	22%
26 to 35	24%
36 to 45	18%
46 to 55	15%
56 to 65	11%
66 to 75	9%
75+	1%
Total	100%

D6. Do you consider yourself an active user of social networks?	Pct%
Yes	51%
No	49%
Total	100%

D7. Are you the head of household?	Pct%
Yes	45%
No	55%
Total	100%

D8. Please check gender	Pct%
Female	51%
Male	49%
Total	100%

D9. Geographic region of the respondent	Pct%
Northeast	20%
Mid-Atlantic	19%
Midwest	18%
Southeast	13%
Southwest	12%
Pacific-West	18%
Total	100%

Please contact [research@ponemon.org](mailto:research@ponemon.org) or call the Institute at 800.877.3118 if you have any questions or comments about this research.

### **Ponemon Institute**

*Advancing Responsible Information Management*

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.