Ponemon INSTITUTE

2011 Privacy Trust Study for Retail Banking

Independently conducted by Ponemon Institute

Report dated: December 2011

2011 Privacy Trust Study for Retail Banking

Ponemon Institute December 2011

Part 1: Executive Summary

During the past year, a volatile global and domestic economy, new regulations and increasingly sophisticated threats to the security of sensitive and confidential information have tested the resiliency of the retail banking industry. While addressing these challenges, retail banks must also continually strive to maintain the trust and loyalty of their individual and business customers.

Customer trust and loyalty in retail banks is dependent upon the perception that the institution is taking every measure to protect their personal financial information. As revealed in this and past studies, a significant number of customers will abandon their relationship with the bank if their personal information is lost or stolen.

The 2011 study represents the ninth year Ponemon Institute has conducted its *Privacy Trust Study for Retail Banking.* As in past studies, this annual survey-based research series asks consumers to indicate how secure and confident they feel when sharing their personal information with their primary banking institutions. Despite financial woes in the economy, a majority of consumers in our study still see their primary banking institution as committed to protecting their personal information. This executive summary report provides the most salient findings from a national survey that included 5,571 adult-aged consumers representing all geographic regions within the United States.[1]

These findings are significant because trust has become increasingly important to creating customer loyalty and brand value in the U.S. retail banking industry. The perceived trustworthiness of retail banking organizations is even more important at a time of economic turmoil and decline as experienced by major financial institutions around the globe.

Our study reveals that even among banks with the highest level of consumer trust, it only takes one or two large data breaches to diminish a trusted relationship. Our findings show consumers expect their bank to have safeguards and procedures in place to protect them from identity theft, cyber crime and other harms resulting from lost or stolen data. If consumers lose confidence that their bank is not taking appropriate measures to protect their data from a breach, they may churn.

Our research asked consumers questions about their bank's privacy commitments. It asked questions concerning:

- Disclosure quality of privacy policies and other related notice
- Customer outreach activities for privacy and data security
- Online experience with special focus on privacy and data security
- Response (if any) to data breach incidents
- Perceptions about advertising, promotions and marketing
- Overall perceptions about the bank's services, especially customer contact experience

Overall, privacy trust scores for banks decreased from 2010 possibly because of poor economic conditions and new consumer regulations in the U.S. financial services industry. The factors that build trust in the bank's privacy and data protection commitments are:

- The perceived financial stability (relative to other banks).
- The overall service quality, especially experience with customer services.
- Disclosure about its privacy and data security practices, especially when banking online.

[1] A detailed research report is available for purchase. The full report provides detailed responses to all survey questions that relate to privacy, data protection and related business practices.

- The bank's advertising, promotion and customer outreach (was it viewed as respectful and did the customer have the opportunity to easily opt-out).
- The bank's online identity and authentication procedures, when they are viewed as rigorous and difficult.
- Stated or implied commitment to stand behind the customer in the event of identity theft or other related crimes resulting from lost or stolen personal data.

The factors that appear to erode trust in the bank's privacy commitments are:

- Financial instability (relative to other banks).
- Data breaches – the notification of a data breach has the most negative impact on overall trust perceptions about the bank.
- Irrelevant or annoying advertising campaigns – including aggressive promotions for credit cards, home mortgages and other product offers that are mailed, emailed or telephoned.
- Difficult to use or poorly designed web site that is inconvenient for various online banking functions.
- The bank's aggressive use and sharing of their personal information, especially when the sharing involves an outsourcer in an offshore location.
- Rumors about the bank's negligence or inability to protect customer information.

Part 2: Survey Methods

As in earlier studies conducted over the past nine years, the primary purpose of this research series is to advance our understanding about how consumers feel when sharing their personal information online with institutions they regularly bank with. Respondents were asked to refer to the following definitions when framing responses to survey questions:

- Personal information – information about yourself and your family. This information includes name, address, telephone numbers, e-mail address, Social Security number, other personal identification numbers, access codes, age, gender, income, account activity and many other types of data about you.

- Privacy commitment – an obligation by the bank to keep your personal information safe and secure. This includes the commitment not to share your personal information without a just cause or without obtaining your consent to do so.

The survey instrument listed 20 major retail banking institutions in the United States selected according to approximate deposit size as reported by the U.S. Federal Reserve and the number of branch locations. The survey also permitted respondents to write-in the name of a banking institution (such as a community bank) not listed on the survey form.

Respondents were asked to indicate only one primary institution that they currently use for retail banking services, and then expressed their opinions on how secure and confident they are about their bank's privacy commitment.

Following is the adjective scale used by subjects to compile a PTS for U.S. retail banking institutions listed within our survey instrument.

- Strongly agree that the bank is committed to protecting the privacy of my personal information.
- Agree that the bank is committed to protecting the privacy of my personal information.
- Unsure that the bank is committed to protecting the privacy of my personal information.
- Disagree that the bank is committed to protecting the privacy of my personal information.
- Strongly disagree that the bank is committed to protecting the privacy of my personal information.

This year our survey instrument captured one primary opinion rating described above and 24 individuated questions. Survey items were used in prior banking studies, thus allowing us to compare results over time. As explained above, the primary task required all respondents to provide an opinion about each bank in which they have an account. Then respondents were required to choose the one bank that they consider as their primary banking institution. The remaining survey items required subjects to respond to questions about the privacy and data protection practices of their primary banking institution.

Part 3: Sample

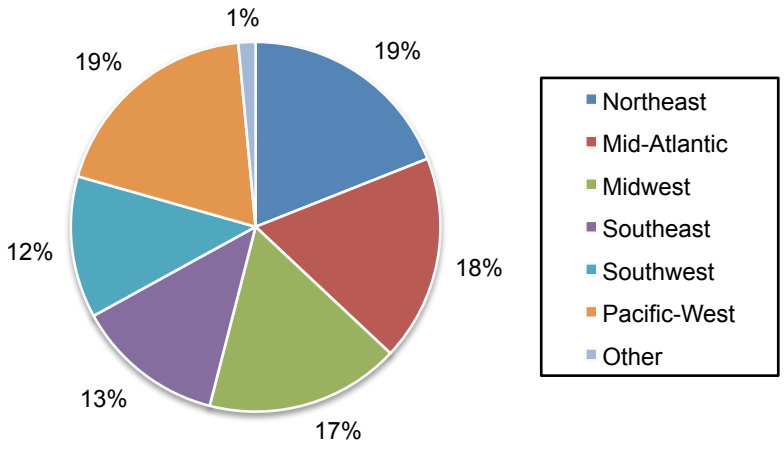
Table 1 reports sample response statistics. Nearly 140,000 adult-aged consumers were invited to participate in this year's study.[2] Our sampling method used both Web and paper form surveys. While most responses were collected on a proprietary survey site, 326 responses were completed manually and returned in a prepaid return envelope.[3]

A total of 5,571 individuals responded. Of these returns, 427 were excluded because of reliability testing. The final sample involves 5,571 individuals with a response rate of 4 percent. These respondents provided a total of 8,529 discernible bank ratings or an average of 1.54 per individual respondent. Approximately 51 percent of respondents are female and 49 percent male. The average age of respondents (based on a self-reported range variable) is 31.6 years.

Table 1. Sample Characteristics	Freq.	Pct%
Sample Frame	139,885	100.0%
Total Responses	5,998	4.3%
Total Rejections	427	0.3%
Sample Size	5,571	4.0%
Total bank ratings	8,529	
Average ratings per respondent	1.54	

All regions of the nation are represented in this study. In total, respondents in 48 U.S. states and two U.S. territories (labeled other) are included in this research. Pie Chart 1 reports the geographic distribution of respondents according to major U.S. region.

Pie Chart 1: Distribution of respondents by U.S. Region



[2]As in prior years, our sample frame is created from consumer contact lists that were designed to be statistically representative of the U.S. adult aged population in terms of gender, age, household income and education based on U.S. Census data. Please note that respondents were provided nominal compensated for their full participation.

[3] We deployed parametric tests on an item-by-item basis to determine possible response differences between Web and paper surveys. No significant difference at or above the $p < .05$ level was found on any one of the survey items.

Part 4: Survey results

The retail banks achieving the highest Privacy Trust Scores (PTS) in over four years of study are listed by year in ascending trust ranking. Table 2 shows U.S. Bank in first place, followed by Fifth Third and PNC. It is important to note that some of the banking institutions earning top five ranks were acquired and, hence, consolidated in the overall total score. Specifically, National City is now included in PNC Bank (ranked second) and Wachovia is included in Wells Fargo.

The sample size (number of ratings) and privacy trust score compiled from respondents' ratings appears next to each bank. Our computational method limits the PTS score to a numerical value between ± 2. A high PTS score suggests that consumers view their bank as having superior privacy and data protection practices, and a low PTS score suggests just the opposite.

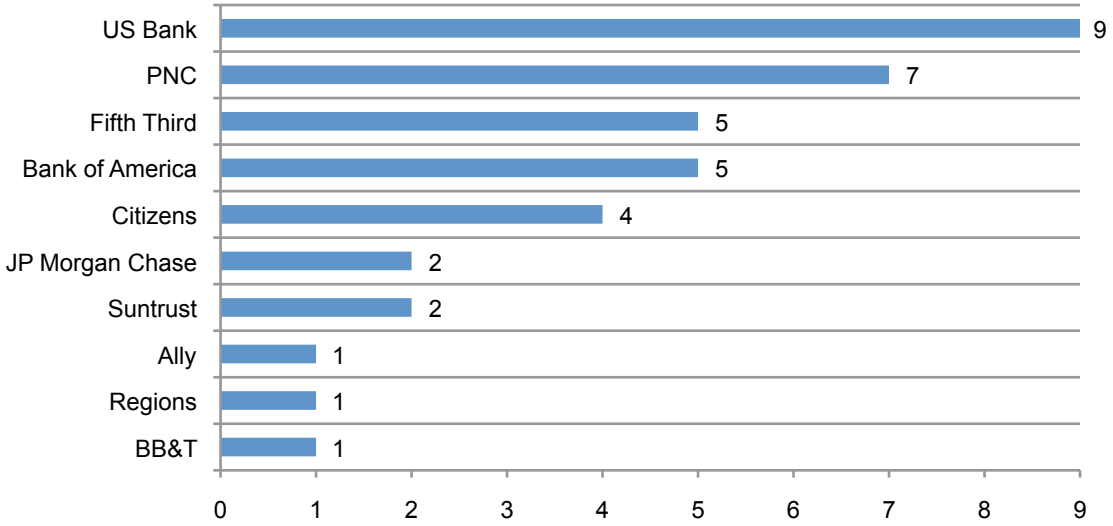
Table 2: The Top Five Most Trusted Banks Over Four Years

2011 Most Trusted for Privacy	2011 Rank	Sample size	PTS
US Bank (Minneapolis)	1	356	1.55
Fifth Third Bank (Cincinnati)	2	209	1.41
PNC Bank (Pittsburgh)	3	167	1.33
Citizens (Providence)	4	152	1.29
BB&T (Winston-Salem)	5	191	1.26
Ally Bank (Detroit)	5	100	1.26
Total/Average		1,790	1.35
2010 Most Trusted for Privacy	2010 Rank	Sample size	PTS
US Bank (Minneapolis)	1	323	1.51
Regions Bank (Birmingham)	2	208	1.42
PNC Bank (Pittsburgh)	3	189	1.34
Citizens (Providence)	4	159	1.31
JP Morgan Chase (New York)	5	911	1.3
Total/Average		1,790	1.38
2009 Most Trusted for Privacy	2009 Rank	Sample size	PTS
US Bank (Minneapolis)	1	312	1.5
PNC Bank (Pittsburgh)	2	186	1.45
Suntrust (Atlanta)	3	185	1.38
Citizens (Providence)	4	140	1.34
Bank of America (Charlotte)	5	812	1.31
Fifth Third Bank (Cincinnati)	5	127	1.31
Total/Average		1,762	1.38
2008 Most Trusted for Privacy	2008 Rank	Sample size	PTS
US Bank (Minneapolis)	1	305	1.48
National City (Cleveland)	2	142	1.42
Suntrust (Atlanta)	3	191	1.37
Citizens (Providence)	4	137	1.3
PNC Bank (Pittsburgh)	4	134	1.3
Wachovia (Charlotte)	5	341	1.26
Total/Average		1,250	1.36

Bar Chart 1 summarizes the ranking of the top five banks over the past nine years. Please note that this figure does not contain the names of banks that have been acquired over the study period. As shown, only US Bank has earned a top five rating for all nine consecutive years. PNC Bank has been ranked as a top five bank for seven consecutive years. Fifth Third and Bank of America has been ranked five times and Citizens has been ranked four times. JP Morgan Chase

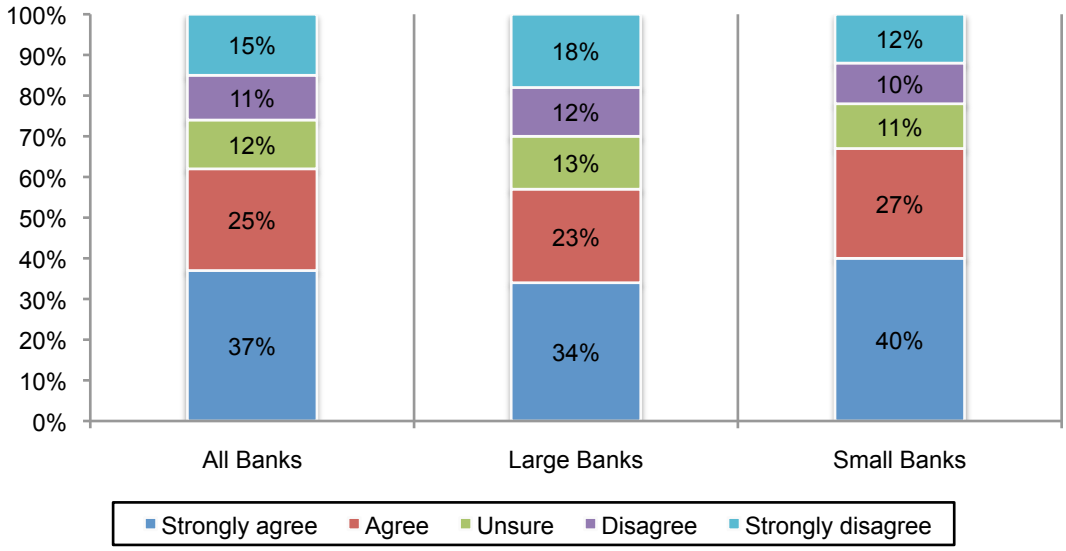
and Suntrust have been ranked twice. Finally, Ally Bank enters the top five this year (tied with BB&T for fifth place).

Bar Chart 1: Banks Listed in Top Five Over Nine Years
Bank rankings are based on the annual Privacy Trust Score



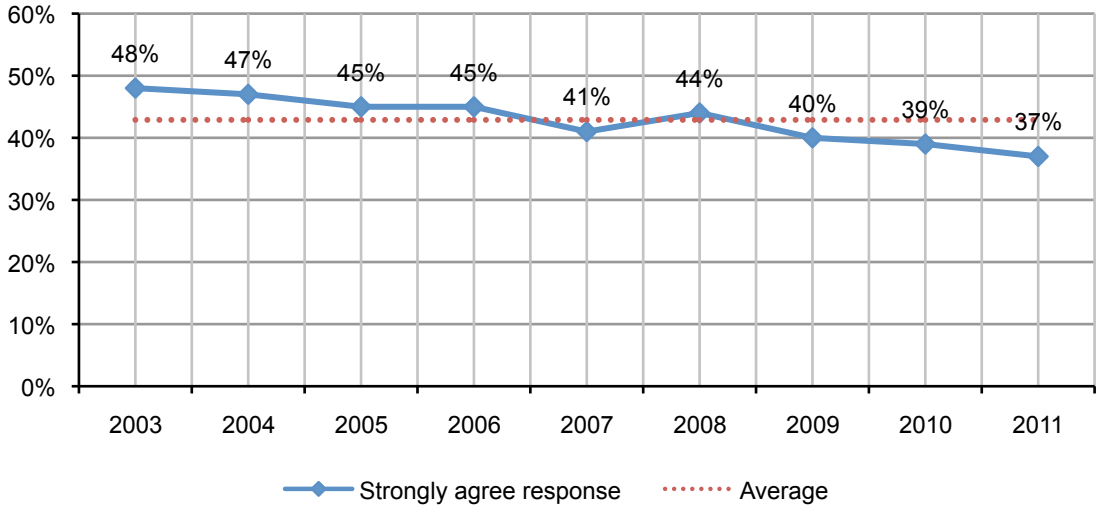
Bar Chart 2 summarizes the distribution of trust ratings according a five-point adjective scale from strongly agree to strongly disagree that the rated bank is committed to protecting the privacy of consumers' personal information. As reported, strongly agree and agree choices are the most frequently selected responses for both large and small (community) banks. It is also interesting to see that smaller-sized banks enjoy more favorable trust rating than larger banks.

Bar Chart 2: Summary of attribution ratings for large and small banks
My bank is committed to protecting the privacy of my personal information



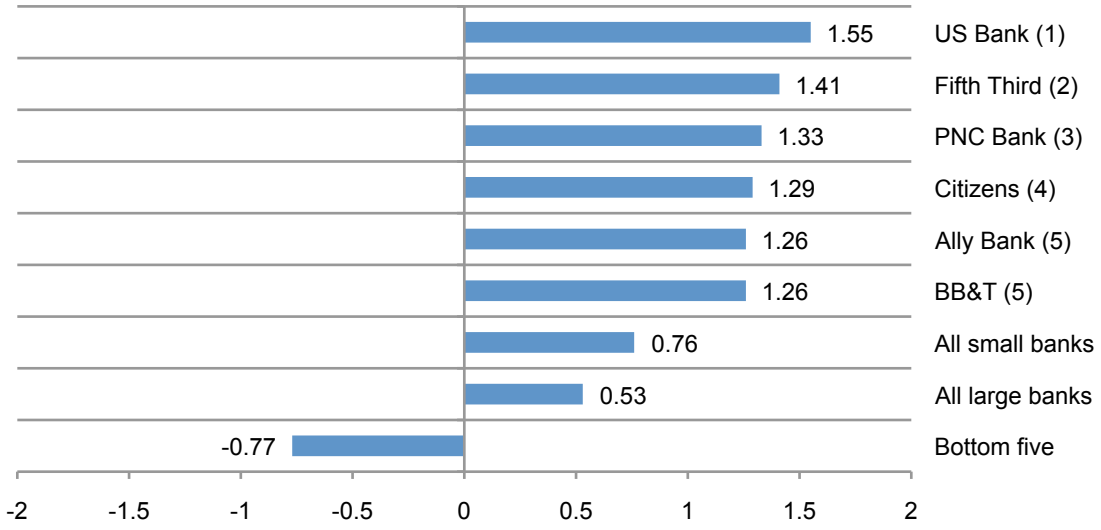
Line Graph 1 plots the strongly agree response trend over nine years. This pattern of results suggest a downward sloping trend, which indicates respondents are losing confidence in their bank's ability to protect the privacy of their personal information.

Graph 1: Strongly agree response for all banks over nine years
Q. My bank is committed to protecting the privacy of my personal information.



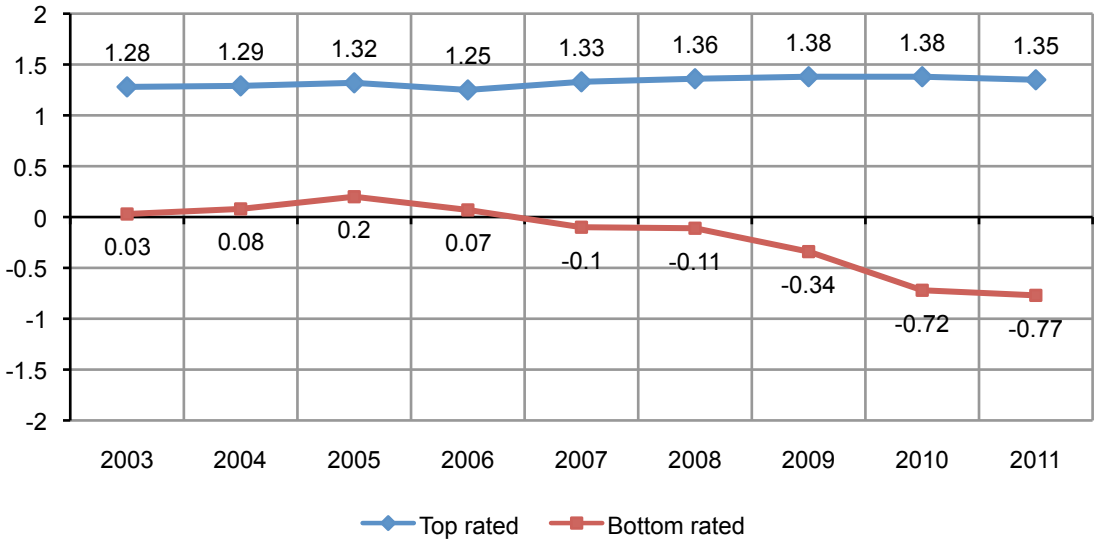
Bar Chart 3 summarizes the 2011 privacy trust results, showing US Bank is in first place with a PTS of 1.55. The average privacy trust score for larger-sized banks is .53 (down from .58 last year). The average privacy trust score for smaller-sized banks is .76 (down from 79 last year). The negative PTS score of -.77 represents a combined average PTS score for the bottom five performing banks combined (down from -.72 last year).

Bar Chart 3: Summary of the 2011 Privacy Trust Scores
PTS ranges from a low of -2 to a high of +2



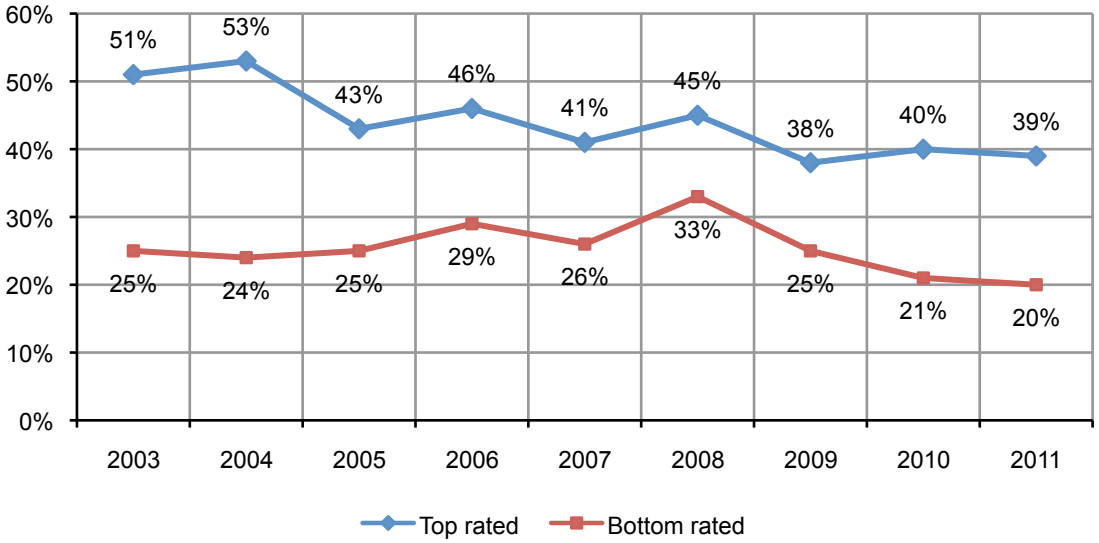
Line Graph 2 plots the average PTS score for top ranked, larger banks, smaller (community) banks and the bottom five banks in terms of compiled privacy trust scores over the past nine years. As can be seen, smaller-sized banks consistently outperform larger (national) banks on trust scores. It is interesting to see that the bottom five banks have steadily declined over the past series, suggesting consumers may be losing confidence in the privacy practices of certain banking organizations that they routinely deal with.

Graph 2: Nine year trend on privacy trust scores for the top rated and bottom rated banks
PTS ranges from a low of -2 to a high of +2



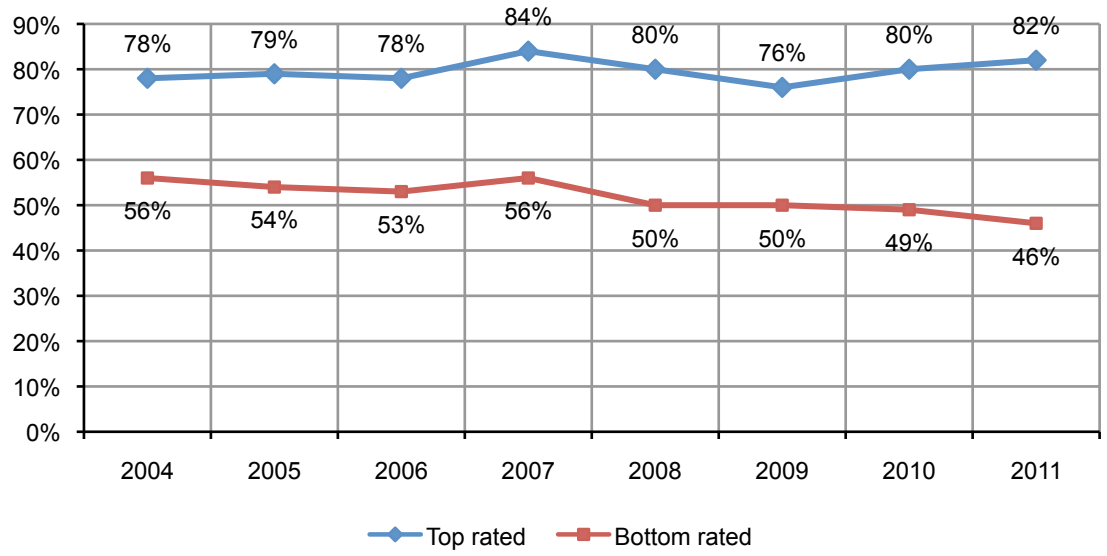
Line Graph 3 provides a seven year time series to the question, "How safe is your bank in making sure your personal information is secure, such as account data, credit card numbers, access codes, Social Security number and so forth?" This series is trending downward suggesting consumers feel less safe in terms of privacy protections over nine years. This graph also shows that the top five banks outperform the overall and bottom five in terms of providing a sense of safety and security for their customers.

Graph 3: How safe is your bank in making sure your personal information is secure?
Each point represents a combined very safe and safe response.



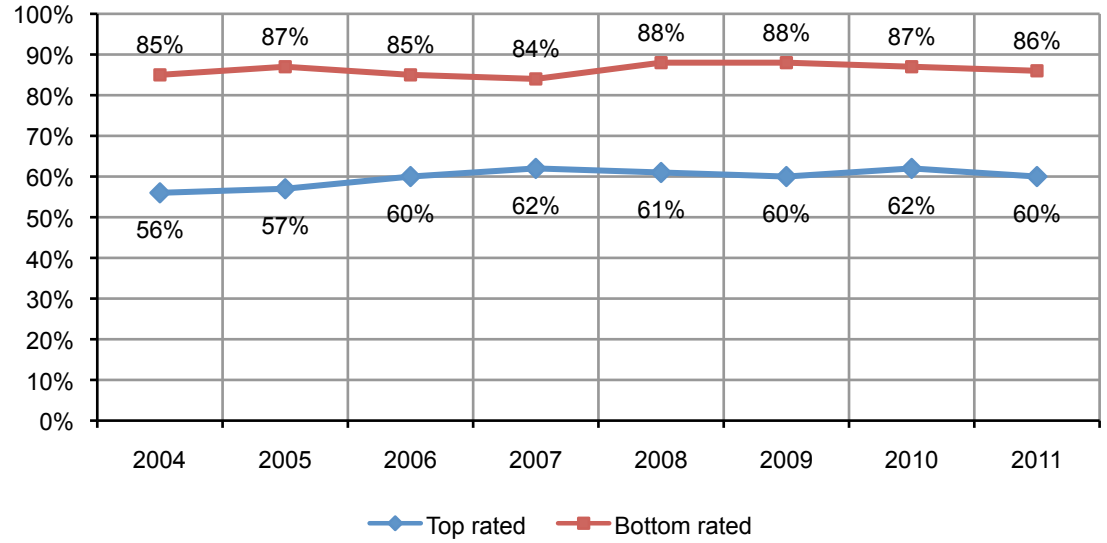
Line Graph 4 provides the yes response over eight years to the question, "If your bank had a privacy breach that resulted in the loss or theft of your personal information, do you believe it would let you know about the incident?" As can be seen, the top five performing banks are viewed as more honorable in reporting data breaches to customers than bottom performers.

Graph 4. If your bank had a privacy breach that resulted in the loss or theft of your personal information, do you believe it would let you know about the incident?
Each point represents the Yes response
This question was not asked in FY 2003



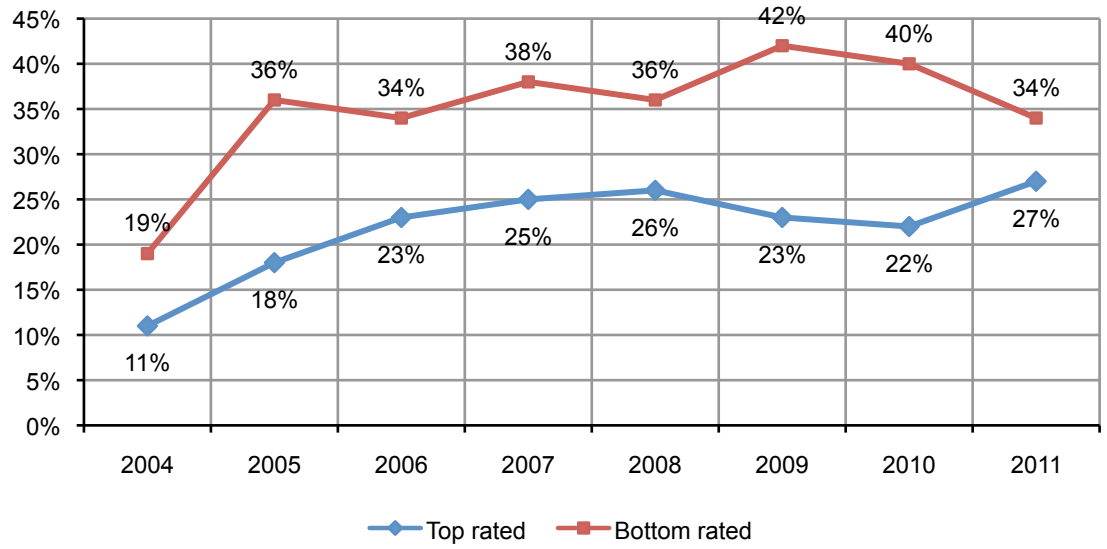
Line Graph 5 summarizes the number of data breaches noticed from the bank before it would cause a meltdown in their confidence in the bank's ability to secure data. The response for one and two times is reflected here. In comparison to the bottom five banks, the top five performing banks are less likely to experience a diminished level of confidence after one or two breaches.

Graph 5: How many notices of a data breach would it take before you lost confidence in your bank's ability to keep your personal information secure?
Each point represents the combined response for one and two data breach notices received
This question was not asked in FY 2003



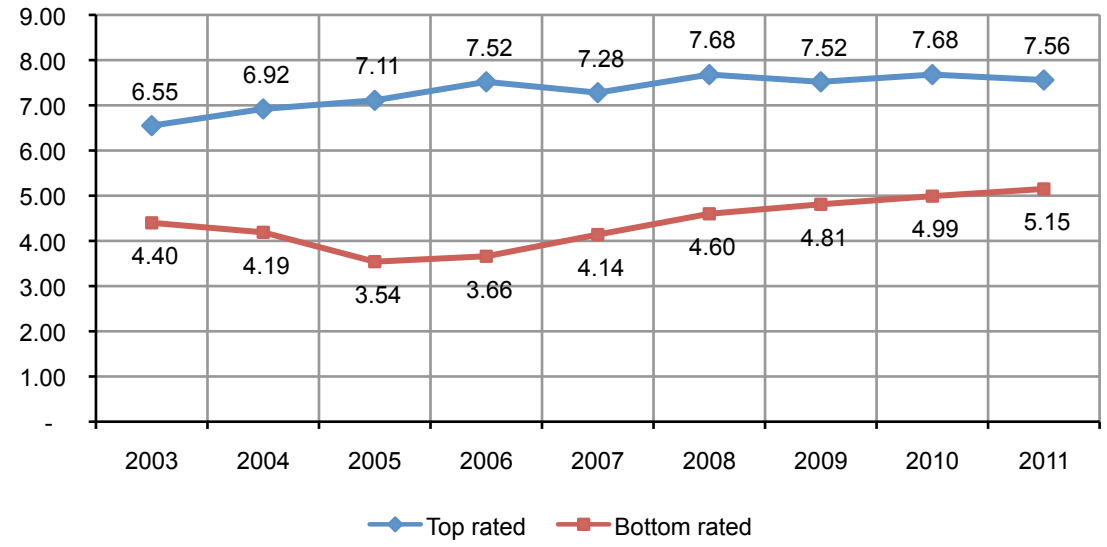
Line Graph 6 plots the churn intention of bank customers after learning about a data breach. As shown, the series appears to be increasing over eight years, suggesting a growing number of consumers are likely to move their accounts to other, more trusted, banking institutions if they experience a data breach.

Graph 6: If your bank had a data breach would you leave?
Each point represents the Yes response
This question was not asked in FY 2003



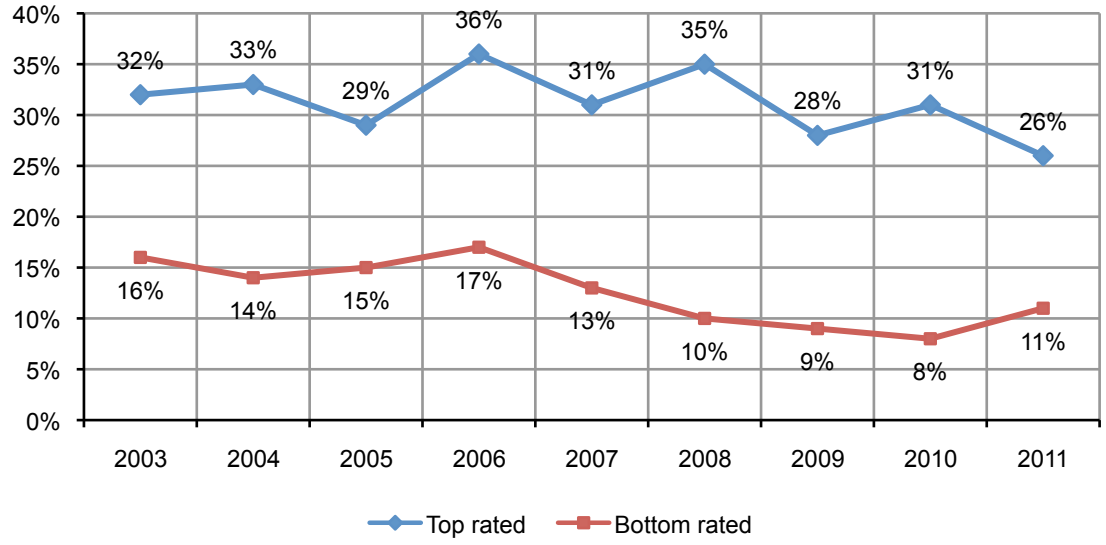
Line Graph 7 reports the average years that respondents say they have been a customer of their chosen primary banking institution. As reported, the top five banks appear to have a higher level of customer tenure than low performing banks.

Graph 7: Average (mean years) customer tenure



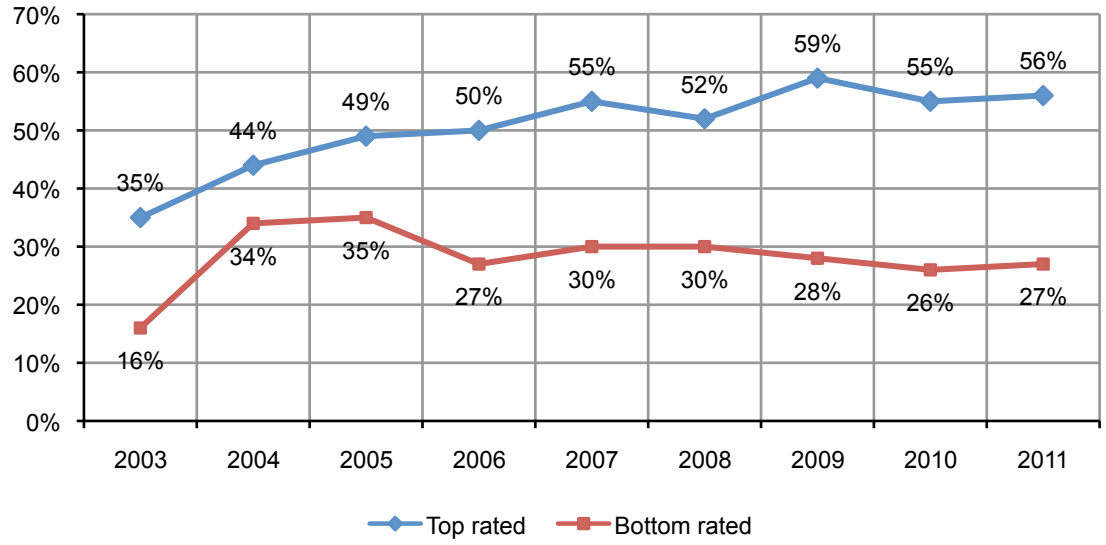
Line Graph 8 reports respondents' perceptions about the marketing communications they receive from their bank. It is clear that the top performing banks are perceived as having a more respectful or less intrusive approach to marketing communications than bottom performers for all nine years.

Graph 8: How relevant is the bank's marketing communication to you?
Always relevant and relevant most of the time response combined.



Line Graph 9 reports the perception of consumers about the privacy disclosure and notice practices of their bank. Again, we compare the top five and bottom five banks. It is clear that consumers of the top performing banks hold a more favorable perception than the bottom performers in terms of their privacy disclosures.

Graph 9: How do you rate the privacy disclosure and notice provided by your bank?
Each point shows the combined good, very good and excellent response combined



Part 5. Recommendations & Limitations

As we have noted above, regulations, cyber threats and customers' concerns about the privacy and security of their financial information is increasing the importance of having a strategic approach to achieving a high level of privacy trust among key stakeholders. Accordingly, we recommend the following actions:

- Assign executive-level authority for protecting information assets such as a chief privacy offer or an equivalent role. As reported in the *2011 Cost of a Data Breach Study*, the presence of a high-level leader benefits organizations through fewer data breach incidents as well as lower costs when a data breach occurs.[4]
- As part of the bank's commitment to quality service, communicate that it will stand behind the customer in the event of identity theft or other related crimes that result from lost or stolen personal information.
- Address the insider threat to sensitive and confidential information through the development of security and privacy policies for the protection of customer information. In addition, carefully implement employee training and awareness programs that stress the importance of safeguarding such information.
- Use encryption, data leak prevention, access management, and other information security technologies that reduce the risk of information loss or theft whenever feasible.
- In the event of a data breach, have a crisis management plan to ensure the source of the breach is determined as quickly as possible and the appropriate victims are notified.
- Ensure marketing communications are relevant to the customer. This is especially the case with use of online digital media and behavioral targeted ads. Overly annoying or irrelevant ads have been shown to diminish customer confidence in their bank's privacy commitment.

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 surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of adult-aged U.S. consumers, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who bank with U.S. financial service institutions. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would 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 subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

[4] See 2011 U.S. Cost of Data Breach Study, Ponemon Institute, January 2012.

If you have questions or comments about this executive summary or you would like to obtain a full report, please contact us by letter, phone call or email:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686 USA
1.800.877.3118
research@ponemon.org

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 company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.