

2014 LexisNexis® Data Minimization

Balancing Business Needs with Consumer
Expectations

October 2014

Table of contents

Objectives And Methodology	4
Executive Summary	5
Key Findings by Industry	5
Financial Services Industry	5
Health-Care Industry	6
Retail Industry	6
Government	7
Recommendations	8
Data Breaches, ID Theft, and the Willingness to Share Sensitive Data	9
Detailed Findings: Financial Services Industry	12
Industry Overview	12
Types and Use of PII Collected	13
General Consumer Data-Sharing Behaviors	14
Consumer Group Profiles	17
PII Collection in the Future	20
Detailed Findings: Health-Care Industry	22
Overview	22
Types and Use of PII Collected	23
General Consumer Data-Sharing Behaviors	24
Consumer Group Profiles	26
PII Collection in the Future	28
Detailed Findings: Retail Industry	31
Overview	31
Types and Use of PII Collected	32
General Consumer Data-Sharing Behaviors	33
Consumer Group Profiles	36
PII Collection in the Future	38
Detailed Findings: Government	40
Overview	40
Types and Use of PII Collected	40
General Consumer Data-Sharing Behaviors	41
Consumer Group Profiles	44
PII Collection in the Future	46
Appendix	47

Table of figures

Figure 1: Low-, Medium-, and High-Risk Scenarios by Industry.....	4
Figure 2: Lifetime Identity Theft and Data Breach Incidence Among All Consumers	9
Figure 3: Level of Concern Over Identity Theft Among Consumers	10
Figure 4: Consumers' Willingness to Share PII by Degree of Sensitivity	11
Figure 5: Federal Laws and Regulations Governing the Treatment of PII in the Financial Services Industry.....	12
Figure 6: Consumers' Reported Trust in Various Institutions.....	14
Figure 7: Consumers' Willingness to Share PII When Opening a New Account.....	15
Figure 8: Consumers' Willingness to Share PII for Online Mortgage Calculators	16
Figure 9: Consumer Group Profiles for the Financial Industry	17
Figure 10: Financial Services Industry Key Takeaways	21
Figure 11: Federal Laws and Regulations Governing the Treatment of PII in the Health-Care Industry	22
Figure 12: PII Consumers Are Most Likely to Share With Health-Care Providers.....	24
Figure 13: PII Consumers Are Least Likely to Share With Health-care Providers	25
Figure 14: Patient Group Profiles for the Health-Care Industry.....	26
Figure 15: Health-Care Industry Key Takeaways.....	30
Figure 16: Areas of PII Collection in the Retail Industry	32
Figure 17: Consumers' Willingness to Share PII When Registering to Receive Coupons and Rewards	33
Figure 18: Consumers' Willingness to Share PII for Returning a Purchase for a Refund	34
Figure 19: Consumer Group Profiles for the Retail Industry	36
Figure 20: Retail Industry Key Takeaways	39
Figure 21: Consumers' Willingness to Share PII With Government Agencies When Registering to Receive Program Details or Benefits.....	41
Figure 22: Consumers' Willingness to Share PII With Government Agencies When Filing a Tax Return	42
Figure 23: Perception of Security Risk Based on Risk Scenarios	43
Figure 24: Consumer Group Profiles for the Government	44
Figure 25: Government Agencies Key Takeaways	47
Figure 26: Heat map of Financial Industry Consumer Information-Sharing Profiles	48
Figure 27: Heat map of Health-Care Industry Consumer Information-Sharing Profiles.....	49
Figure 28: Heat Map of Retail Industry Consumer Information-Sharing Profiles.....	50
Figure 29: Heat Map of Government Group Consumer Information-Sharing Profiles.....	51

Objectives and methodology

This white paper explores the current use of consumers' personally identifiable information (PII) for identity verification among key industry groups as well as consumers' willingness and perceptions involving the sharing of PII. Based on these findings, it aims to provide insight on future industry trends, specifically those involving opportunities to reduce the amount of sensitive data being collected and retained (data minimization).

Industry data cited in this white paper is primarily based on in-depth Interviews with 22 industry experts working in financial services (banking industry), health care, government, and retail.

Consumer data is based on a 20-minute online survey conducted in December 2013 among 3,018 U.S. adult consumers. Respondents were presented with questions to determine their willingness to share various PII under different scenarios, by industry. Each of the respective scenarios, in which the identity of the consumer must be verified, represents different overall levels of risk (i.e., compliance and fraud risk) to organizations in each industry. (See Figure 1).

Figure 1. Low-, Medium-, and High-Risk Scenarios by Industry

Vertical	Low Risk	Medium Risk	High Risk
Financial services	Using an online mortgage calculator	Opening a bank checking or savings account	Applying for an automobile loan
Health care	Making an online appointment with a new dentist or a new doctor	Applying for health insurance via a state or federal online health insurance exchange	Opening an account with a health-care provider or retail pharmacy to review your medical records, lab results or prescription history online
Retail	A retail or consumer goods company to receive coupons or promotions	Returning an online purchase for a refund	Purchasing an age-restricted product like tobacco products or lottery tickets
Government	Registering to receive general program or benefit details	Requesting a copy of your birth certificate	Filing your federal tax return to receive a tax refund

Consumer profiles

In order to characterize consumer sentiment with regards to sharing personal information and identify key demographic and behavioral drivers, a cluster analysis was performed for each of the four key industries. Consumers were segmented based on their willingness to provide each of 16 types of PII in all three risk scenarios. For each industry, the emerging consumer segments were analyzed for key differentiators, and recommendations were made for the treatment of each segment in the industry context.

Executive summary

Today millions of U.S. consumers regularly provide their personally identifiable information (PII) to organizations such as retailers, financial institutions, government entities, and health-care organizations. Data collection of personal information most commonly occurs during the account registration or customer onboarding process, but can occur throughout the customer lifecycle. Requesting personal information for identity verification, future communications or account maintenance represents a dynamic interplay between consumers' trust and the organization's PII data requirements. In turn, the organization's data requirements are shaped by factors including industry regulations, fraud mitigation and data security concerns, unique identity verification needs, and vendor stipulations and marketing needs. The role and influence of each of these factors are far from constant as they often shift weight, shape, and form by industry. As a result, the PII collection process and experience vary greatly across industries, affecting both the consumers and the industry stakeholders in diverse ways. Every industry expert interviewed for this research expressed a perceived duty to protect consumers and if presented with an alternative to how their respective organizations currently collect data, most would take advantage.

Key findings by industry

Financial services industry

Current PII collection practices in the financial services industry are heavily bound by federal and state regulations that require extensive PII. Key acts and guidelines governing this industry include KYC guidelines, the Patriot Act, and the Bank Secrecy Act. This industry currently collects extensive PII on consumers including name, address, phone number, email address, driver's license number, mother's maiden name, date of birth, and Social Security number (SSN).

Despite their view that more data is better for security, many banking experts hope to reduce the amount of PII they must collect and subsequently store. There is a perception that integrating new technology with the existing identity verification framework would make the industry less dependent on the collection of "sensitive" PII to improve identification and reduce chances of aggravating customers. Some experts specifically believe that using answers to dynamic knowledge-based questions in place of sensitive PII might be part of the solution.

The financial industry benefits from a high level of consumer trust, but even that has its limits. From the consumers' perspective, trust in FIs is fairly high with 60% of consumers stating they are very willing to share their PII. Consumers are willing to sharing their PII for purposes such as a new financial account, where they may be more accustomed to providing such information and understand its purpose. However, their willingness declines when consumers are faced with informational activities, such as using an online mortgage calculator, where they may not understand or appreciate a request for more sensitive PII.

Nearly half of consumers display a tendency to overshare PII during a financial services interaction, which may increase their identity theft related risks. Among the three distinct financial services consumer groups, the cohort that is the most willing to share PII represents nearly half of all consumers (47%). Possibly contributing to their increased likelihood of being an identity theft victim, this segment will share PII with relatively minimal regard to circumstance or the sensitivity of the information requested which increases the chances that it will be exposed to compromise during storage or transmission between them and their bank or credit union.

Health-care industry

Sensitive data collection in the health-care industry is heavily driven by regulations, privacy act guidelines, and software requirements. The Affordable Care Act (ACA) and Health Insurance Portability and Accountability Act (HIPAA) are two main acts regulating the health-care industry. Regulations in this industry are more focused on protecting the storage and use of PII, than dictating the type of PII collected. Health-care industry experts acknowledge that their collection of SSNs is being driven by the requirements of patient record management systems, rather than compliance with industry regulations.

While industry experts are satisfied with the amount of PII being collected, the volume of PII health-care organizations are required to collect presents challenges. Current verification systems which collect name, address, email address, SSN, driver's license numbers, date of birth, phone numbers, insurance information, and some form of medical history for health care transactions are deemed effective. However, there is an ongoing struggle in the industry on how to manage and protect the vast amounts of information collected by both providers and payers.

Linking patients' identity to their medical records is fast developing as a crisis in the health-care industry. The industry currently lacks an easy, uniform way to identify patients and link them to their health data, doctors, hospitals, pharmacies, and insurance plans, which is creating a wall of unrelated patient-identity numbers bogging down the medical records system.¹ Despite the risks of sharing and storing SSNs, this has created some reliance by health-care organizations on their use for patient identification. In the place of collecting such sensitive PII, industry experts remain hopeful of possible streamlining in the future through the use of tools such as a universal health-care ID.

Balancing fraud mitigation and privacy concerns are proving difficult. Health-care organizations must collect and secure sensitive PII from their patients, some of whom do not wish to share this information in the first place, increasing liability in the case of a data breach. Yet, limiting the data utilized for identity verification to less sensitive PII such as name and address will likely not appeal to payers or providers either, as fraudsters could easily gain this information from secondary sources and circumvent the verification process.

At first glance patients appear generally unwilling to share more sensitive PII with health-care organizations, but upon closer examination there is a clear divide among groups of patients. Patients overall are more willing to share "low sensitivity" PII such as gender, age, name, and address regardless of context but remain hesitant to share "high sensitive" information, specifically SSN. Yet when broken into groups based on their behaviors, nearly half of patients display flexibility – willing to share most PII and hesitating only slightly when the data is of the most sensitive in nature.

Retail industry

Sensitive data collection in the retail industry is driven by marketing, fraud mitigation, and regulatory compliance. PII collection is a more complex and diverse structure here compared with other industries, due to the variety of circumstances where PII is utilized. Retailers collect largely "low sensitivity" PII such as name, telephone number, and email address for online transactions and loyalty programs. However, PII collection gets more intense for retailers managing credit card portfolios, as they must meet some of the same regulatory requirements as financial institutions.

With the growing threat of cyberfraud there is a greater need for effective, low-friction ID verification. Retailers are facing increased pressure to balance customer convenience and ID verification, especially for the online and mobile channels. Identity verification for ecommerce and mcommerce require a low-friction experience to mitigate "cart abandonment", yet criminals rely on the anonymity afforded these by these channels to successfully complete fraudulent transactions.²

Increased public focus on the issue of data breaches is motivating data minimization efforts among retailers.

Although industry experts are fairly satisfied with the current data collection process, large-scale data breaches and growing attention from the media are raising concerns about the protection and use of PII. This is creating a reliance on vendors and third parties for collecting and managing consumer data.

Due to data security and fraud concerns, consumers express the least willingness to share PII with retailers. Some industry experts believe the proliferation of data breaches and recent revelations about the compromise of online privacy have decreased willingness among consumers to share PII. Data breaches have been closely linked with identity theft,³ and while 26% of consumers have been victims of identity theft, more than half (54%) are concerned that they will be victims in the future. Only 17% of consumers state they are very willing to share PII with this industry (see Figure 1). Consumers especially express deep reluctance to share “high sensitivity” PII such as SSNs and historical identifiers (e.g., mother’s maiden name). However, they are open to sharing the more “low sensitivity” PII such as gender, age, and address.

One in four consumers effectively abstains from sharing PII with retailers. While the respective groups of consumers are not overly polarized with the greatest proportion of the population in the relatively generous group 1 (40%), at least one in four consumers is hesitant to share any type of PII with retailers (group 3, 25%). Whether due to customer conditioning or the recent slate of retailer data breaches, this industry faces the greatest challenge among businesses in all examined sectors when soliciting PII from consumers.

Government

The government has the most intensive and intrusive levels of data collection among all industries. Sensitive data collection requirements are heavily mandated by policies enforced by federal and state funding agencies. Personally identifiable information collected by government agencies include SSN, date of birth, mother’s maiden name, place of birth, income, and legal status. Some federal programs, such as those provided by the Department of Housing and Urban Development, also request the collection of demographic data including race, ethnicity, and gender.

The collection of PII is driven by regulatory compliance needs, yet data security is recognized as a significant challenge. Government officials express satisfaction with the current process as they are collecting all of the data required by applicable guidelines and regulations, although with the growing threat of data breaches and cyberattacks, there are also increasing concerns regarding the protection and privacy of the stored information.⁴

Government agencies collect extensive PII, and they expect the collection and use of this information to become more stringent in the future. Given recent data breaches and the rising threat of ID theft, industry experts expect the PII collection process to get even more stringent with state and federal regulations levying additional requirements as to which types of PII must be collected and how it should be maintained.

Despite the media attention on data breaches, consumers place a high amount of trust in government when it comes to sharing PII. This is the only industry in which consumers express a high level of willingness to share their SSNs – particularly in high-risk scenarios. Likely due to having been conditioned to expect to provide this information while filing their federal tax returns, 71% of consumers report they are very willing to share their SSN in this scenario.

While nearly half of consumers will freely share most PII with government agencies, a small but demographically similar group refuses to let the government know much more than their name. Representing more than half of all consumers and very different perspectives on sharing PII, these two groups are barely differentiated from each other demographically, and are only differentiated from the general population by their employment status. This makes distinguishing between them, and consistently verifying their identity through PII a considerable challenge.

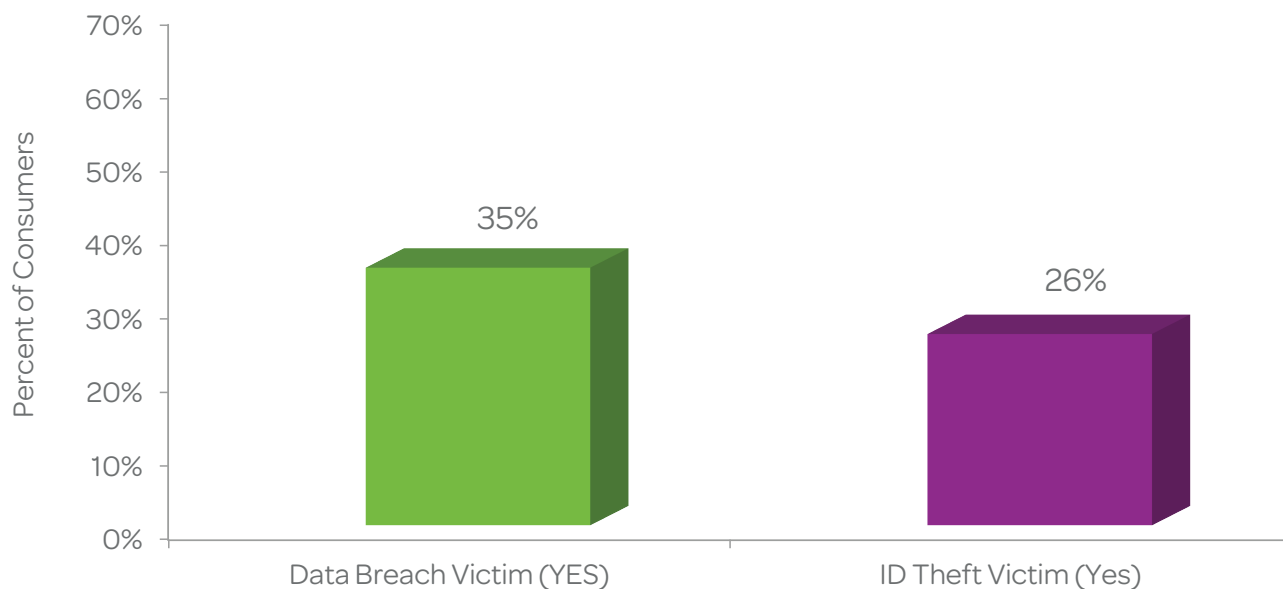
Recommendations

- **Reduce risks associated with data theft by streamlining the collection of PII where possible.** Streamlining the data collection process, or limiting the collection of PII to only that which is necessary to establish identity, can reduce the risk to the organization and consumers in the event of a breach while also minimizing the burden on consumers when the PII is being collected.
- **Assess the drivers of your data collection process when streamlining, especially when there are regulatory considerations.** In the financial services, health-care, and government sectors, the need to comply with regulations can severely curtail any efforts to reduce the amount of data collected. Before attempting a data minimization effort, it is critical to distinguish between PII that must be collected due to regulations and that which is being collected for business needs so as to avoid falling out of compliance.
- **Use data collection technology and systems that suit the organization's needs, not vice versa.** Health-care organizations in particular expressed that they were often collecting sensitive PII only because it was a required field within the patient management software. Avoid inconveniencing the consumer unnecessarily by ensuring that the solutions in use to collect and store PII can be customized to the needs of the organization.
- **Understand the preferences of consumers specifically served by the organization before deciding on a data collection policy.** It is commonly understood that consumers as a whole express certain preferences as to the type of PII they are willing to share under different circumstances. Yet after examining discernable patterns of behavior among consumers, distinct groups can be identified, each of which can feel differently about sharing PII in the same scenario. Knowing how the population served by the organization aligns with these distinct groups will allow for a more effective and well-received data collection policy.
- **To further minimize data collection and the burden on consumers, balance the use of consumer-sourced and third-party PII.** In addition to data minimization benefits, supplementing data collected from consumers with that from alternative sources can mitigate the need to collect PII that might be considered impractical or unwelcomed by consumers.
- **Determine which data is the most effective for positively identifying consumers without being burdensome, to maximize the overall success of data collection efforts.** The most sensitive pieces of PII are valued for their uniqueness, in that they more closely correlate with a single individual than other types of data. Understanding how to balance the accuracy of a piece of PII or different combinations of PII are for identity verification is critical to meeting internal needs while also minimizing inconvenience for consumers.

Data breaches, ID theft, and the willingness to share sensitive data

Organizations should be cognizant of how consumers' fears and experiences affect their willingness to share sensitive data. Data breaches and identity theft have become pervasive threats to consumer trust, especially due to the growing media attention on data breaches. In the U.S., over 1 in 4 consumers have experienced ID theft, while more than 1 in 3 consumers have been notified that their information was compromised in a data breach in their lifetimes (see Figure 2).

Figure 2. Lifetime Identity Theft and Data Breach Incidence Among All Consumers

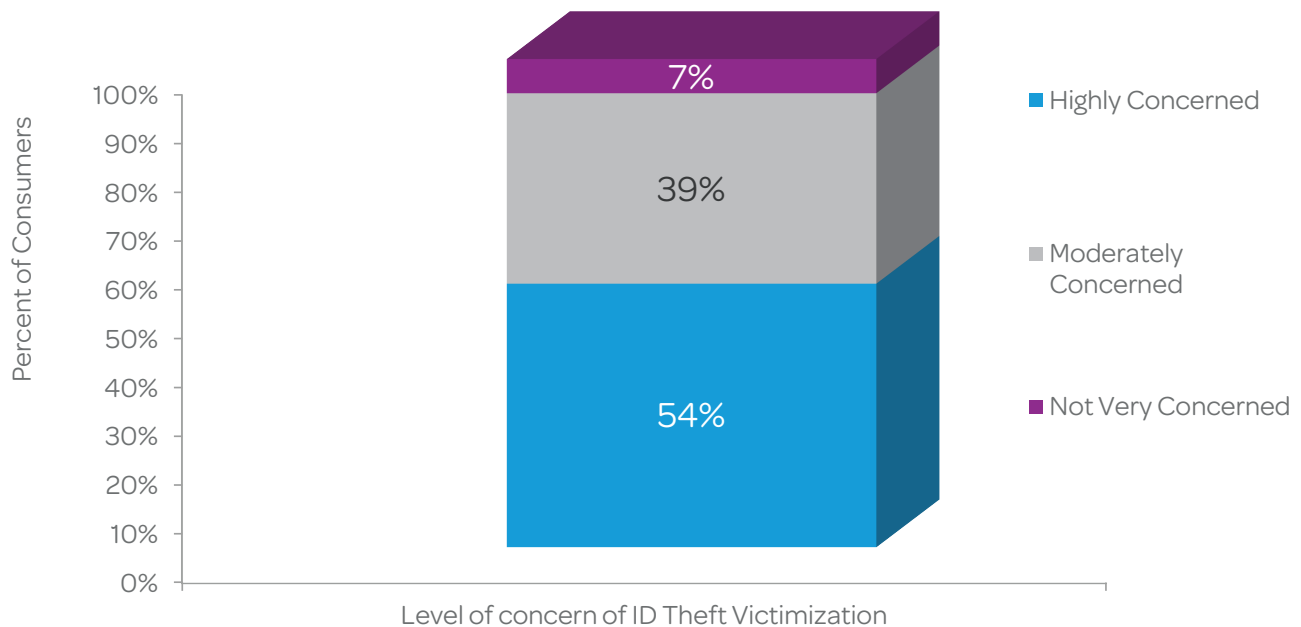


Q: Have you EVER been notified by a business or other institution that your personal or financial information has been lost, stolen or compromised in a data breach?
Q: Have you EVER been a victim of identity theft?

December 2013, n = 3,018.
Base: All consumers.

Unsurprisingly, more than half of consumers (54%) are concerned about ID theft victimization in the future (see Figure 3). The compromise of PII from businesses and government organizations is as a major contributing factor to identity theft and fraud. Both protecting and minimizing the collection of sensitive data are critical steps forward for every organization to prevent consumer PII from being compromised and misused.

Figure 3. Level of Concern Over Identity Theft Among Consumers

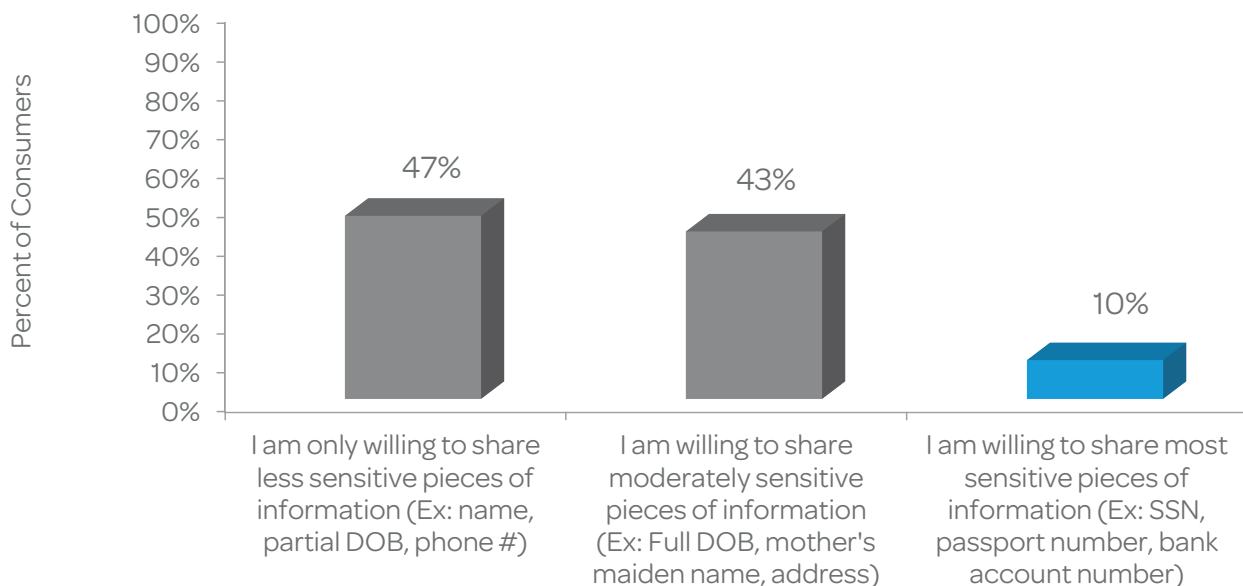


Q: Please indicate your level of concern about being a victim of ID fraud where your personal or financial information may be compromised and misused from different accounts you may have. Please rate on a scale of 1 to 10, where 1 means 'Not At All Concerned' and 10 means 'Extremely Concerned'.

December 2013, n = 3,018.
Base: All consumers.

Consumer willingness to share certain types of sensitive data further supports the need for data minimization efforts to become common practice. Concern over the issue of identity theft, whether shaped by experience or public perception around data breaches, undoubtedly affects consumers. With only 10% willing to share the most sensitive types of PII (see Figure 4) and the seemingly unrelenting pace at which breaches continue to occur, the use of alternative data to positively identify consumers is a necessity.

Figure 4. Consumers' Willingness to Share PII by Degree of Sensitivity



Q: While opening an account, or signing up for coupons from a retailer or registering to receive government benefits materials, you may need to provide several personal identifying information to the organization for them to create your identity with them. With regards to sharing such personal identifying information please, select the statement below that best describes you.

December 2013, n = 3,018.
Base: All consumers.

When crafting data minimization strategies, organizations in the financial services, health-care, government, and retail sectors must consider the identity theft and data breach experiences of consumers. Levels of willingness to share PII with these organizations will decline in tandem with the compromise and misuse of consumer data resulting from data breaches. These organizations can best prepare for the growing reluctance of consumers to share PII by limiting their requests for this information to only that which is absolutely necessary and cannot be sourced elsewhere. Minimizing data collection is necessary to secure not only the integrity of consumer data, but also the reputations of organizations in these industries.

Detailed findings: Financial services industry

Industry overview

The U.S. banking industry currently represents 6,730 banks and credit unions with approximately \$14.9 trillion in assets.⁵ The stakes are high, and as the industry moves toward increased use of web apps for access to banking services and new product enrollment, end-users expect financial service providers to protect their assets and sensitive information from unauthorized disclosure or access. U.S. banks have a critical need to balance customer convenience and acceptance of privacy intrusions vs. collecting adequate PII to facilitate identity verification.

Experts in the banking industry point to tough industry regulations and compliance requirements as the leading drivers for their PII collection policies. Focusing on anti-money-laundering and fraud mitigation, the key regulations governing these efforts include Know Your Customer (KYC) guidelines, the Bank Secrecy Act, and the Patriot Act.

Currently, information collection among financial institutions is driven by security and anti-fraud and anti-money-laundering needs, rather than marketing purposes.

Figure 5. Federal Laws and Regulations Governing the Treatment of PII in the Financial Services Industry

KYC guidelines	Know Your Customer (KYC) is a blanket term referring to the set of programs and policies required of, but not limited to, financial institutions to collect and verify the validity of personal information collected from their clients. These guidelines are the result of Title III of the USA Patriot Act, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 requirements for identity verification when opening new accounts at financial institutions. Typical KYC information requirements include full name, address, phone number, SSN, and at least two valid forms of identification. These requirements can vary by state.
The Patriot Act	The USA Patriot Act was signed into law by President George W. Bush on October 26, 2001. Title III of this act amends the Bank Secrecy Act of 1970 by expanding the reporting requirements of financial institutions, requiring the implementation and oversight of customer identification and anti-money-laundering programs, and prescribing regulations establishing minimum standards for financial institutions to verify their customers' identity when opening a new account. ⁶
Bank Secrecy Act	The Bank Secrecy Act (BSA) of 1970 (aka the Currency and Foreign Transactions Reporting Act) established requirements for record-keeping and reporting by private individuals, banks, and other financial institutions. Specifically, the act requires financial institutions to keep records and file reports of cash purchases of financial instruments and legally required financial institutions to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. ⁷

Types and use of PII collected

Financial services industry (banking) experts are almost uniform as to the types of PII that they currently collect from their customers. Information collected from new customers, or customers opening new accounts, includes name, address, phone number, email address, driver's license number, mother's maiden name, date of birth, and SSN. For additional products such as loans or lines of credit, the financial institution may also collect additional information to determine creditworthiness such as personal income, household income, credit cards, loans, retirement accounts, and other lines of credit.

To meet KYC guidelines, banks additionally require their customers to validate the information collected. If customers go to the branch to open a new account, they are required to show two forms of photo ID (driver's license, passport, government ID card, etc.). If the application is received online or through a call center, knowledge-based authentication (KBA) is trusted to replace at least one of the ID requirements.

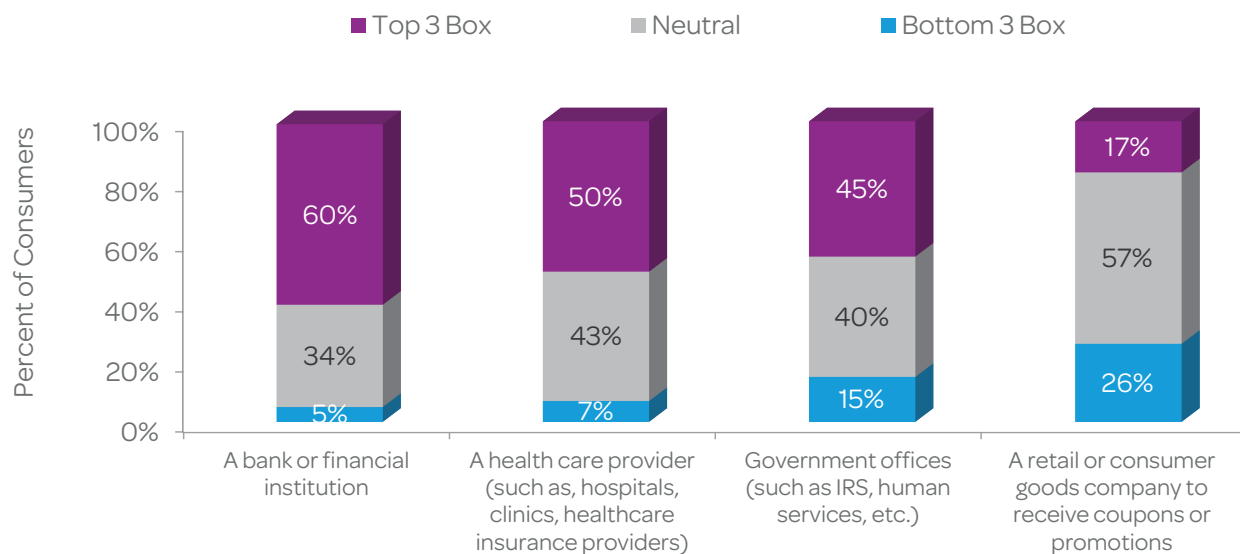
During interviews, banking experts asserted that marketing plays only a supplemental role in the PII requirement process. New customers' email address and/or phone numbers are used for internal marketing purpose, and can be used in combination with other demographic factors, but none of this information is expressly collected with marketing in mind. Instead, the bulk of the information collected is driven by regulatory requirements (such as the Bank Secrecy Act and USA Patriot Act) and used as part of fraud mitigation programs, anti-money laundering (AML) measures, or static KBA.

General consumer data-sharing behaviors

Considering all of the information collected when consumers open new accounts with FIs, finding the balance of convenience and privacy is a constant struggle for bankers. The burden placed on consumers to provide increasing amounts of PII can bog down the account opening process and raise the possibility of application abandonment.⁸ However, banking experts believe consumers are still willing to share their PII, even though they might not fully comprehend the reason why all the information is being collected.

The confidence expressed by banking experts is validated by consumers. Consumers reported high levels of confidence toward FIs as nearly 3 in 5 consumers are willing to trust FIs with their personal information (see Figure 6).

Figure 6. Consumers' Reported Trust in Various Institutions

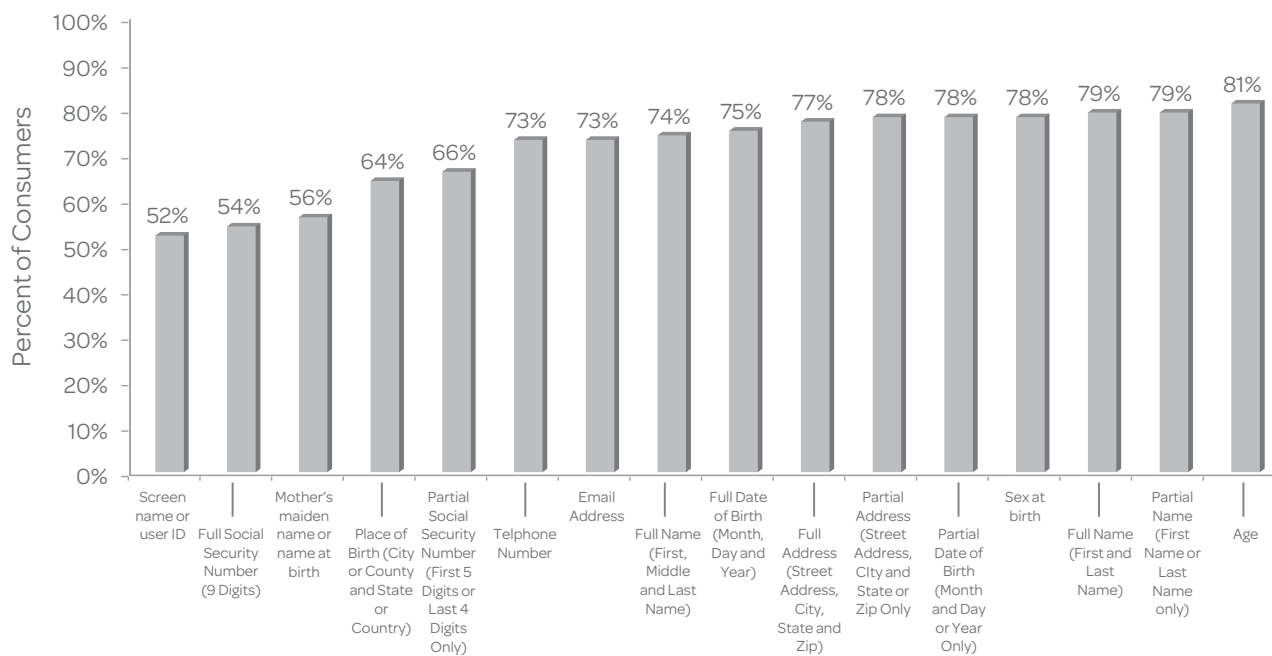


Q: Which of the following types of companies or organizations would you trust with your personal identifying information if you were to open and maintain an account with them?

December 2013, n = 3,018.
Base: All consumers.

Consumers' willingness to share PII with their FI is not a blanket phenomenon. Consumers are most willing to share PII when engaged in a critical yet familiar activity such as opening a new account. More than 70% of consumers are willing to share their age, name, address, email address, and phone numbers when opening accounts (see Figure 7). However, consumers' willingness to share information drops for more sensitive forms of PII such as SSN, place of birth, and mother's maiden name.

Figure 7. Consumers' Willingness to Share PII When Opening a New Account

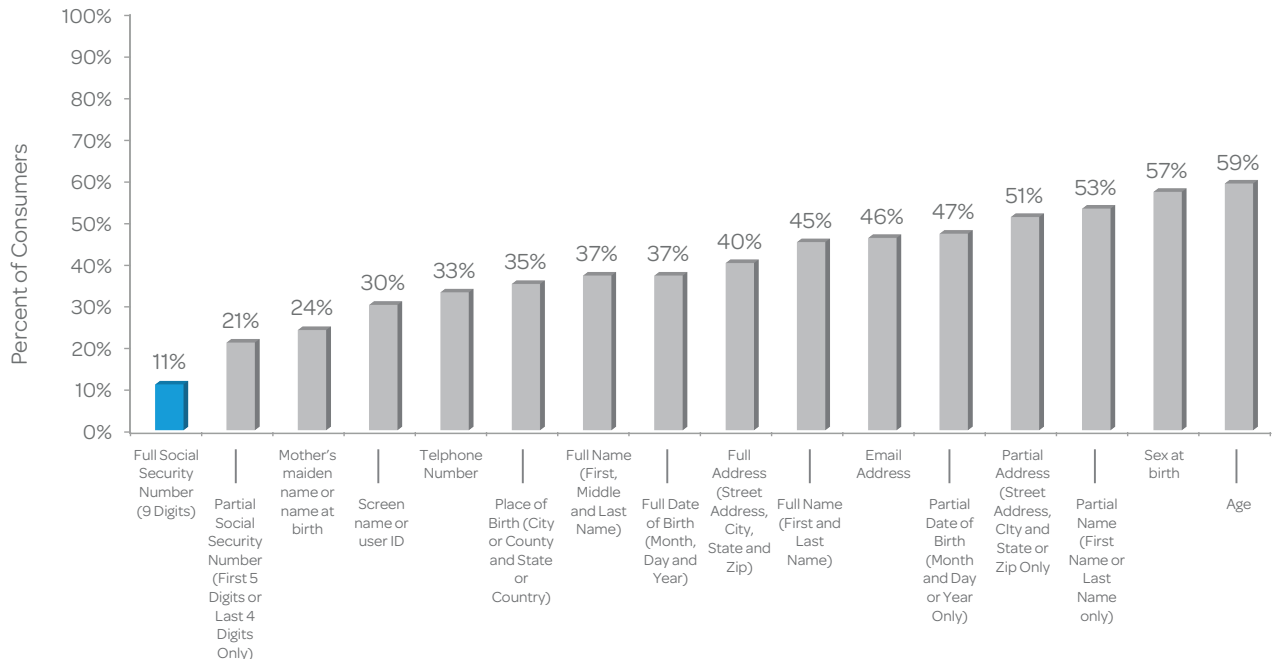


Q: You are opening a bank checking or savings account (either at a branch or online over the internet). For each of these personal identifying information, please answer how willingly you will share the information in this scenario. Please rate on a scale of 1 to 10 where 1 means 'Not At All Willing' and 10 means 'Totally Willing'. TOP 3 BOX SHOWN

December 2013, n = 606.
Base: Consumers assigned to Financial Services Group.

Consumers' overall willingness to share PII dips significantly when the service requested does not require access to a private account or can be received anonymously, such as providing information for an online mortgage calculator. Only 59% are willing to share even age as a PII for this purpose, revealing some reluctance among consumers to give information for services that do not result in completing a transaction or demonstrate a perceived need for the more sensitive data (see Figure 8). Yet, despite consistently lower levels of willingness to provide any information for this type of service, it is still surprising that more than 1 in 10 indicated a willingness to provide their SSN in this scenario. This could indicate that a portion of the population either is indifferent to providing sensitive data regardless of circumstance or has no expectations regarding the sensitivity of data being collected.

Figure 8. Consumers' Willingness to Share PII for Online Mortgage Calculators



Q: You are using an online mortgage calculator. For each of these personal identifying information, please answer how willingly you will share the information in this scenario. Please rate on a scale of 1 to 10 where 1 means 'Not At All Willing' and 10 means 'Totally Willing'. TOP 3 BOX SHOWN

December 2013, n = 606.
Base: Consumers assigned to Financial Services Group.

FIs are generally in tune with the preferences of consumers as a whole.

"I think they'd want to provide as little as possible [when using a mortgage calculator], because they realize that this is not a financial product, it's a calculator."

– Vice President, Large Regional Bank

"Consumers expect to have to give up personal information to open up a financial account, and so they'll be willing to give what they would consider in their minds to be kind of the standard information of name, address, Social Security number, telephone number, etc."

– Senior Privacy Officer, Large National Bank

Consumer group profiles

Overall consumer willingness to share PII with financial institutions grows in tandem with the risk of the scenario. Yet all consumers have not been conditioned to react to these requests in the same manner, and not all consumers interact with FIs through the same channels. Upon closer examination there are underlying group behaviors related to sharing PII that can be identified within the overall population of consumers. Understanding who these groups are composed of and the circumstances under which they are willing to share PII will prepare FIs for verifying identities through in-person and digital channels while maintaining a positive experience for existing and potential accountholders.

Consumers within each of these groups share one of three unique sets of behaviors when it comes to providing their PII. The most willing of these groups to share PII (the Ready and Willing group) represents nearly half of all consumers (47%), while the other two groups (the Data Sharing Skeptics group and the Cautious yet Flexible group), are of nearly equal proportions (26% and 28%, respectively) yet they assess whether or not to share PII by somewhat different criteria (see figure 9).

Figure 9. Consumer Group Profiles for the Financial Industry

Financial Industry Consumer Groups			
Likelihood that consumers in this group are ...	Group 1. Data-sharing skeptics, lowest willingness (26% of consumers)	Group 2. Cautious, yet flexible, medium-willingness (28% of consumers)	Group 3. Ready and willing, highest willingness (47% of consumers)
Female	↑	↓	↓
Male	↓	↑	↑
Aged 25 to 34 years	↑	↓	--
Aged 55 to 64 years	↓	↑	--
Earn > \$100k annually	↓	--	↑
Fraud victims (ever in lifetime)	↓	--	↑
City-dwellers	↑	↓	↑
Early adopters of new technology	--	↓	↑
Smartphone owners	↓	↑	↑
Broadband-enabled	↓	↑	↑

Group 1: “Data Sharing Skeptics” (26% of consumers)

Decides to share PII based on: The sensitivity of PII requested

Overall willingness to share PII: Low

They are more likely to be:

- Female (62%)
- Between 25 to 34 years of age (22%)
- City-dwellers (36%)

They are less likely to be:

- Between 55 and 64 years of age (14%)
- Individuals with a household income over \$100k (17%)
- Previous identity theft victims (22%)
- Individuals with broadband access (79%) or a smartphone (53%)

Synopsis:

This group is generally less willing to share PII than other segments, regardless of the scenario. They are only moderately willing to share sensitive PII during medium risk and high risk scenarios, and when the scenario is low risk their willingness declines further. Displaying a heightened need to maintain the privacy of their PII, bankers that do business with consumers in this group can expect to collect fewer pieces of PII directly from them.

Key takeaway:

To secure business from this group, bankers must clearly articulate the reasons behind requesting sensitive PII in higher risk scenarios. In lower risk scenarios, bankers should determine the optimal mix of less sensitive data that they can solicit from the consumer which can be supplemented with information from alternative sources.

Group 2: “Cautious yet Flexible” (28% of consumers)

Decides to share PII based on: The sensitivity of PII requested and the riskiness of the situation

Overall willingness to share PII: Medium

They are more likely to be:

- Male (54%)
- Between 55 to 64 years of age (21%)
- Individuals with broadband access (92%) or a smartphone (65%)

They are less likely to be:

- Between 25 and 34 years of age (13%)
- City-dwellers (24%)
- Early-adopters of new technology (17%)

Synopsis:

This group weighs both the risk of the scenario and the sensitivity of the PII requested when deciding on whether or not to relinquish their PII. They display a relatively moderate willingness to share PII when compared to other segments. More specifically, they exhibit a greater propensity to share less sensitive PII in a medium risk scenario, such as when applying for an auto loan or in a high-risk scenario, such as when opening a new account. Displaying an acute awareness of the circumstance, they are generally less willing to share any type of PII in low-risk scenarios, such as when using a mortgage calculator.

Key takeaway:

Relatively flexible, but still exhibiting a degree of caution, bankers can scale their data collection requests to reasonably align with compliance and internal business needs without excessive pushback from this group.

Group 3: “Ready and Willing”

Decides to share PII based on: The sensitivity of PII requested

Overall willingness to share PII: High

They are more likely to be:

- Male (49%)
- City-dwellers (36%)
- Individuals with a household income over \$100k (25%)
- Previous identity theft victims (33%)
- Early-adopters of new technology (29%)
- Individuals with broadband access (89%) or a smartphone (64%)

Synopsis:

Possibly contributing to their increased likelihood of being an identity theft victim, this group will share PII with relatively minimal regard to circumstance or the sensitivity of the information requested. This group will share PII of all types uniformly in both medium and high risk scenarios, while only demurring slightly in their willingness to share the most sensitive PII in low risk scenarios. Financial service providers face a substantial challenge with this group as the ease with which they share PII increases the chance that illicit attempts to glean information from these consumers or their devices will be successful.

Key takeaway:

Rather than taking advantage of their seeming indifference to share PII, bankers should collect the data necessary for their needs while also conditioning and educating this group on data sharing best practices.

PII collection in the future

Experts believe they have successfully streamlined the application process and are already collecting the minimum required to meet regulatory standards.

“At this point, I’m not sure there is anything different that we would do based on what we see our competitors doing. I think we’re pretty much (at the) minimum necessary information gathered.”

– Senior Privacy Officer, Large National Bank

There is also a perception that having access to larger quantities of PII provides greater security for the FI and their customers. Feelings of adequacy and security are higher in FIs that collect more information, rather than less.

“The simple answer to your question is yes. The less information you collect the harder it is to get a true picture – a picture of the true customer.”

– Senior Privacy Officer, Large National Bank

In terms of the types of data collected, if the current regulations’ requirements were to be changed, there is a perception that better security solutions would come from shifting away from credit bureaus to more accurate, effective tools such as dynamic KBA as the authoritative source for identification.

“As private as people want to keep their Social Security number and everything else, it’s based on static information. Even the [static] knowledge-based authentication questions we use, they’re not good. ... The committed fraudster generally gets [the information]. Given that the information is static, fraudsters can build identities very quickly.”

– Director, Large International Bank

There is also a perception that integrating new technology with the existing identity verification framework would make the industry less dependent on the collection of “sensitive” PII to improve identification and reduce chances of aggravating customers.

“We need to marry our current identity verification, fraud prevention strategies and technology better to the PII that we ask on our application. I think that things are changing faster than our applications, and our process is changing.”

– Director, Large International Bank

Figure 10. Financial Services Industry Key Takeaways

Key Takeaways: Financial Services Industry	
Industry Practices and Perspectives	
	• The data collection processes and procedures of the financial services industry are bound tightly by state and federal regulations, making it difficult for the financial institutions to move away from collecting sensitive PII to validate their customers' identities.
	• Some banking experts believe their current data collection process is already streamlined and more PII is equal to better security.
	• FIs are in tune with their customers' perceptions and correctly surmise consumers' unwillingness to share PII for less critical purposes such as online mortgage calculators.
	• Experts believe PII collection will move in the direction of using more dynamic verification enabled by the increasing adoption and evolution of mobile devices.
	• Despite their view that more data is better for security, many banking experts hope to see future products that are effective for identity verification yet will reduce the amount of PII they must collect and subsequently store.
Consumer Perceptions	
	• Despite a recent surge in public concern about data privacy (the result of fallout from data breaches of national retailers and publicized details on government data collection programs); consumers continue to trust FIs with their personal information.
	• Consumers are used to and comfortable sharing sensitive PII for purposes such as opening new accounts, while they are hesitant to share the same information for lower-risk scenarios such as an online mortgage calculator.
	• Consumers are most sensitive about sharing SSN and least sensitive about age, address, gender, and telephone number.
	• Nearly half of consumers display a tendency to overshare PII during a financial services interaction, which may be exposing them to identity theft should the data be compromised during storage or transmission between them and a financial service provider.

Detailed findings: Health-care industry

Overview

Similar to the financial services industry, PII data collection in the health-care industry is driven heavily by regulations. However, unlike the financial services industry, regulations are more focused on ensuring patient privacy rather than deterring fraud or illegal activities. The Affordable Care Act (ACA) And Health Insurance Portability and Accountability Act (HIPAA) are the leading regulatory statutes driving privacy in this industry. Therefore, PII information collected by institutions serves a dual role in the health-care industry. It helps payers and providers meet HIPAA guidelines for protecting patient privacy while making it more difficult for fraudsters to commit insurance fraud and increase risk.

Figure 11. Federal Laws and Regulations Governing the Treatment of PII in the Health-Care Industry

HIPAA ⁹	The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information. Critically, the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification after a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.
ACA ¹⁰	On March 23, 2010, President Barack Obama signed the Affordable Care Act into law. The law puts in place comprehensive health insurance reforms in the United States that will roll out over four years and beyond. As part of this new package of reforms, the ACA established requirements and standards for operating rules requiring health-care organizations to transition record-keeping and data collection toward electronic systems in an effort to improve record-keeping systems, reduce system errors, and mitigate fraud and abuse risks.

Apart from regulations, PII collection in the health-care industry is significantly influenced by vendor requirements. Vendors, also looking to meet HIPAA and ACA requirements, play a major role in patient identification, as mandates for data efficiency and security from the ACA and HIPAA are pushing vendors, payers, and providers toward building and maintaining more electronic health records.

“The regulatory environment is a key driver. Other drivers are the enforcement landscape, reputational risk, and vendor contractual requirements ... [which] come out of the regulatory environment as well.”

— Director Of Risk And Fraud Security, National Health Plan Provider

Additionally, internal requirements for patient identification, in an effort to prevent medical mistakes and the corresponding legal ramifications, are driving many health-care providers to expand their data collection processes.

Types and use of PII collected

In the health-care industry, there is no uniform code or standard regulating the types of PII to be collected. Existing industry regulations are instead focused on protecting patient privacy and regulating how the collected PII is stored and used. These regulatory restrictions place health-care organizations in a unique role in which they must collect a large quantity of information as part of their operations but are limited in the use of this data.

Health-care organizations currently collect a diverse range of information from patients as part of their enrollment or intake process. Data collected by providers and payers is quite comprehensive. It includes name, address, email address, SSN, driver's license number, date of birth, phone numbers, insurance information, and usually some form of medical history.

However, from the provider's perspective, not all of these pieces of information are required for verification purposes. Photo ID is the main course of ID verification at the time of check-in for most providers. Provider experts indicated that a photo ID and a health insurance card are typically all that is used to verify a person's identity, even during enrollment. Like experts in the financial services industry, some experts in the health-care industry pointed out that just relying on photo ID is not foolproof, and that they are not confident in the efficacy of relying on this method of verification.

"Providers are now trying to ask for a driver's license or some ID card in order to validate [identity], but I would not rank that as a very high confidence."

— Director Of Risk And Fraud Security, National Health Plan Provider

Unlike with providers, SSNs and driver's license numbers are used most often by health-care payers for ID verification at the time of enrollment in health plans. Most of the other information collected helps to deepen verification capabilities and/or to meet payers' or other vendor/third party's software and information requirements.

"So as a [health-care] payer, information is collected on individuals. We collect everything from demographic information, name, address, age, Social Security number, birth date, to their entire health history. It's very comprehensive."

— Director Of Risk And Fraud Security, National Health Plan Provider

Some providers reported using an electronic medical record system to check "real-time eligibility" with health plans and their own organization, but this system is not standard across all providers.

General patient data-sharing behaviors

Overall, experts at health-care institutions believe the effect of the data collection and verification process on consumers is minimal. Experts indicated that patients/customers are inconvenienced by the amount of data they have to provide, but that they are willing to cooperate to prevent fraud or ID theft and improve their overall care. Providers report patients might complain about the length of the application but are largely willing to share their PII.

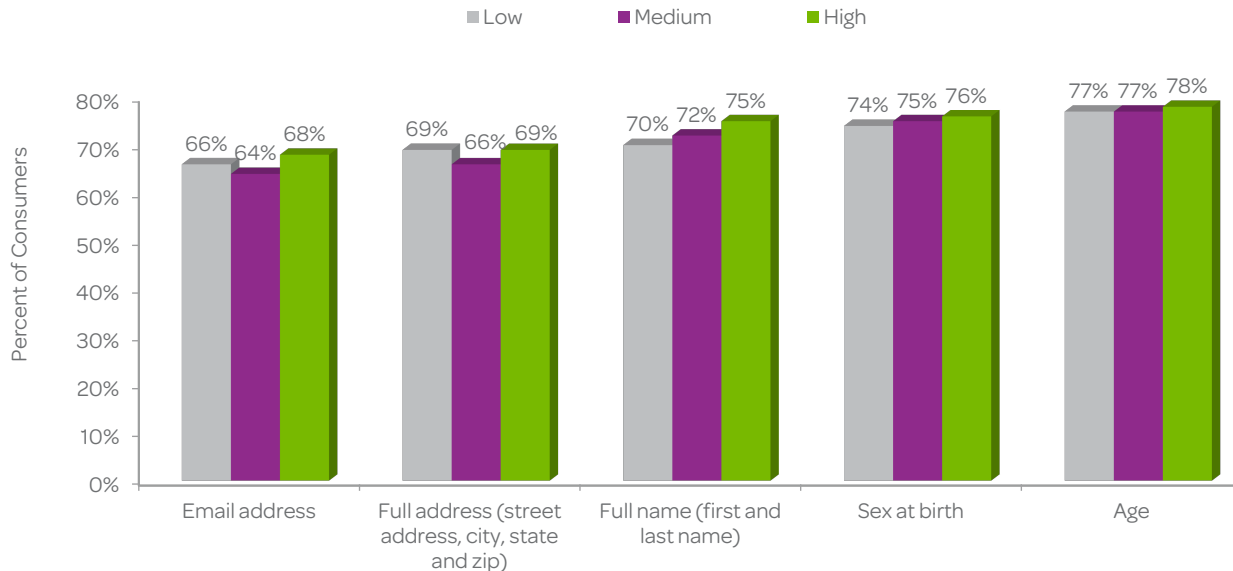
“It’s a national problem where many people are afraid of identity theft. So the vast majority of patients, while even though they consider it time-consuming, at the end of the day they’re grateful for it, because we’re helping to protect their identity and protect their health.”

– Director Of Operations, Regional Health-Care Provider

Reflective of this belief, 50% of consumers reported that they are most willing to share their PII with health-care organizations (see Figure 6). Though second behind the financial services industry, the very personal nature of health care in the U.S. leads many consumers to place greater trust in health care than government, or retail industries.

Consumers are largely willing to share basic information such as their age, name, date of birth, and phone number with health-care organizations. More than 6 in 10 consumers are willing to share this information regardless of context: their willingness to share remains similar regardless of whether it’s a low-risk situation such as making an appointment online with a doctor or higher-risk situations such as applying for health insurance online or opening an account with a health-care provider/pharmacy (see Figure 12). This contrasts sharply with the financial industry, where the willingness to share information differs based on the riskiness of the scenario (see Financial Industry section, pg. 12), as well as with retailers, where willingness to share PII remains comparatively low regardless of the scenario (see Retail Industry section, pg. 31).

Figure 12. PII Consumers Are Most Likely to Share With Health-Care Providers

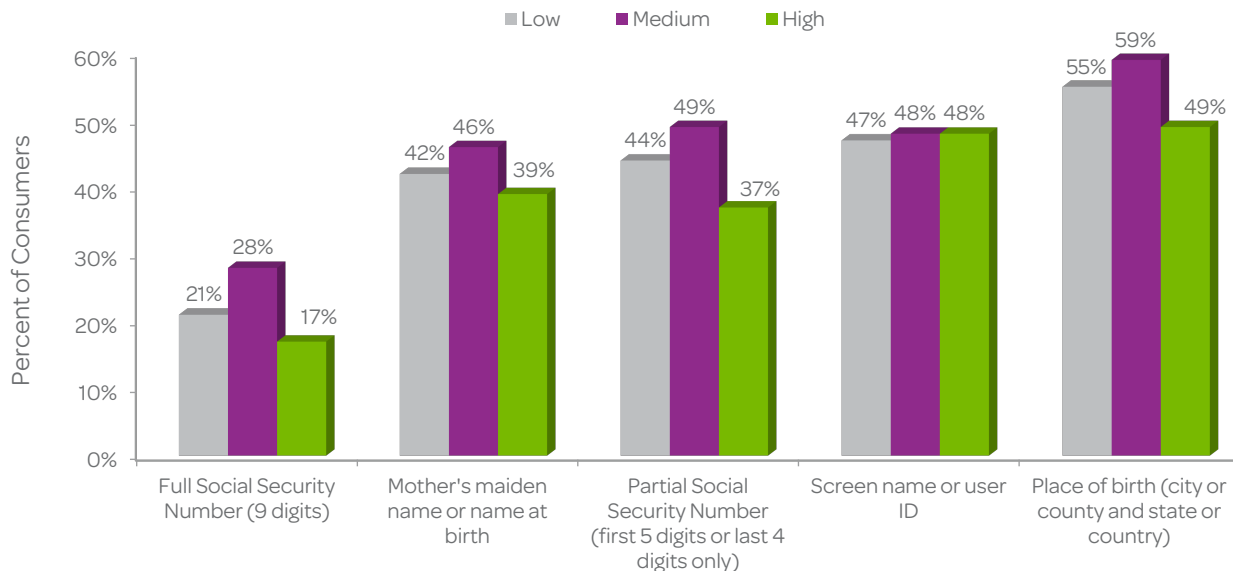


Q: You are opening an account with a healthcare provider or retail pharmacy to review your medical records, lab results, or prescription history online. Please answer how willingly you will share the information in this scenario. Please rate on a scale of 1 to 10, where 1 means “not at all willing” and 10 means “totally willing.” Top 3 box shown.

December 2013, n = 605
Base: Consumers assigned to healthcare group.
© 2014 Javelin Strategy & Research

Despite the overall level of trust for health-care organizations among patients, consumers are generally hesitant when it comes to sharing their SSN, mother's maiden name, place of birth, and screen name – with the greatest sensitivity displayed toward sharing their full SSN. Fewer than 3 in 10 consumers are willing to share their full SSN with health-care providers (see Figure 13). Again, this perception remains constant regardless of the type of activity within the health-care landscape.

Figure 13. PII Consumers Are Least Likely to Share With Health-care Providers



Q: You are opening an account with a healthcare provider or retail pharmacy to review your medical records, lab results, or prescription history online. Please answer how willingly you will share the information in this scenario. Please rate on a scale of 1 to 10, where 1 means "not at all willing" and 10 means "totally willing." Top 3 box shown.

December 2013, n = 605
Base: Consumers assigned to healthcare group.
© 2014 Javelin Strategy & Research

Health-care providers experience consumer pushback when requiring more sensitive pieces of information from their patients. Some health-care industry experts pointed out that their collection of SSN is not driven by internal or regulatory policies but is instead dictated by the software tools they use. From a privacy perspective, this puts some health-care organizations in a difficult position. They must collect and secure sensitive PII from their patients (some of whom do not wish to share this information in the first place), increasing their information liability in the case of a data breach while not adding additional strength to their ID verification processes.

"Our electronic medical records system here is designed so that you can't get past the system unless you have their Social Security number in that field. It's a required field – not an option. But this is not for compliance, it is a matter of software design."

– Compliance Officer, Regional Health-Care Provider

Patient group profiles

Patient willingness to share PII is barely affected by the risk level of the scenario. The overall patient population is fairly well conditioned to healthcare organizations' broad requests for data. Patients instead express more hesitation to share PII as the sensitivity of that PII grows. By understanding the degree to which their patients resist sharing different types of PII, healthcare organizations can better hone their data minimization efforts.

When examining the data sharing behaviors of different groups of patients, their degree of willingness is unaffected by the scenario; instead they are influenced by the sensitivity of the PII being requested. Highly polarized, patients are more likely to fall into either group 1 (the Extremely Private group) (40%) or group 3 (the Practically Carefree group) (48%), than group 2 (the Tempered Responder group) (12%).

Figure 14. Patient Group Profiles for the Health-Care Industry

Healthcare Industry Consumer Groups			
Likelihood that consumers in this group are ...	Group 1. Extremely private, lowest willingness (40% of consumers)	Group 2. Tempered responder, medium willingness (12% of consumers)	Group 3. Practically carefree, highest willingness (48% of consumers)
Female	↑	--	↓
Male	↓	--	↑
Aged 45 to 54 years	↓	--	↑
Early adopters of new technology	↓	--	↑
Broadband-enabled	↑	↓	↑

Group 1: "Extremely Private" (40% of consumers)

Decides to share PII based on: The sensitivity of PII requested

Overall willingness to share PII: Low

They are more likely to be:

- Female (59%)
- Individuals with broadband access (87%)

They are less likely to be:

- Between the ages of 45 to 54 (15%)
- Early-adopters of new technology (19%)

Synopsis:

Displaying the least willingness to share PII among all of the groups, these patients will prove the most resistant to attempts to solicit information in any scenario. Further still, these patients are the closest in absolute terms to denying healthcare organizations access to the most sensitive PII. Vetting patients in this group for healthcare products and services will prove extremely challenging, as they are likely to resist all data collection efforts.

Key takeaway:

Healthcare organizations that serve these patients should be prepared to rely on few pieces of directly-sourced PII, and instead use alternative sources of data while also reducing the organization's data collection needs wherever possible.

Group 2: "Tempered Responder" (12% of consumers)

Decides to share PII based on: The sensitivity of PII requested

Overall willingness to share PII: Medium

They are less likely to be:

- Individuals with broadband access (68%)

Synopsis:

Representing the smallest proportion of the general patient population, patients in this group display mild resistance to sharing most PII across every risk scenario. And regardless of the riskiness of a scenario, healthcare organizations are unlikely to be able to solicit more sensitive pieces of PII from patients in this group.

Key takeaway:

Overall, this group displays a comparatively rational response to requests for PII – healthcare organizations which serve this group should avoid requesting more sensitive PII when possible, and instead rely on accurate, but less sensitive pieces of PII to minimize the effect of their data collection efforts on these patients.

Group 3: "Practically Carefree" (48% of consumers)

Decides to share PII based on: The sensitivity of PII requested

Overall willingness to share PII: High

They are more likely to be:

- Male (53%)
- Between 45 to 54 years of age (22%)
- Early-adopters of new technology (28%)
- Individuals with broadband access (91%)

Synopsis:

This group is open to sharing less sensitive forms of PII regardless of the scenario, while displaying mild hesitation when the degree of sensitivity increases. Whether involved in a low, medium, or high risk scenario healthcare organizations can be reasonably assured that requests for most PII will be met with little resistance.

Key takeaway:

Healthcare organizations that avoid soliciting more sensitive PII will provide a painless data collection experience for patients in this group. Limiting the collection of more sensitive data by relying on alternative sources will help to avoid any perceived inconvenience on the part of these patients.

PII collection in the future

Overall, health-care providers and payers believe the current list of PII information they collect is effective for protecting patients' privacy, preventing fraud, and improving the accuracy of medical records. Health-care industry experts believe the volume of information collected along with the large number of touch points maintained with patients makes existing policies and processes fairly effective for verifying patient identities.

"It's a matter of the amount of detailed information that we do collect, and then making sure that all the pieces of the puzzle fit on the day of the exam. If you provided this address, well then your picture ID had better have that address on it. Also, the policy number that you've given us, you should have the insurance card(s) to match that policy."

– Operations Manager, Regional Health-Care Provider

This perception is especially strong among payers who view the current system to be fairly smooth. Payers indicate that improvements in the existing identity verification system could go a long way toward mitigating medical/insurance fraud, but they stressed that any attempt to further streamline the process would weaken existing controls already in place or put greater enforcement pressures on providers.

"[ID verification] is sort of smooth. That doesn't mean that there aren't problems in the system, but I think to fix those problems you turn providers and pharmacies and others who have touch points with patients into policemen, and I don't think that's how we as a society want them to be using their time."

– Director Of Risk And Fraud Security, National Health Plan Provider

For some providers, the sheer volume of data collected is also fairly challenging to collect, track, and store. Admittedly, linking patients' identity to their medical records is fast developing as a crisis in the medical field. The industry currently lacks an easy, uniform way to identify patients and link them to their health data, doctors, hospitals, pharmacies, and insurance plans, which is creating a wall of unrelated patient-identity numbers bogging down the medical records system.¹¹

Collecting less data or limiting data collection to just name and address is a concern for both payers and providers. From a payer's perspective, fraudsters could easily gain this information from secondary sources and breach the verification process.

"It's definitely not enough information. Anybody can pull that just from doing a white pages search. So at that point, to me, you might as well not even verify it. That's not a valid verification in any way."

– Former Chief Privacy Officer, Pharmaceutical And Health-Care Technology Provider

From a provider's perspective, such information would not be unique enough to avoid confusion when names and addresses are closely shared, exposing providers to legal liability. It is in such cases that a unique ID or the SSN proves beneficial.

"Social Security [number] is probably the best, just because it's the single unique identifier. Obviously, your name can be duplicated. Addresses could be wrong – which happens occasionally."

– Compliance Officer, Regional Health-Care Provider

Perhaps the answer for the health-care industry might lie instead in providing access to a concentrated, mobile, and secure source of information, such as a universal health ID.

"Some sort of national ID that would transgress just driver's licenses or passports. The photo ID is most important. Because I could make up a Social Security number right now off the top of my head. It's far more important to us to have an ID with a photo on it than a card with an SSN."

– Director Of Operations, Regional Health-Care Provider

A tool such as the universal health ID could reduce the health-care industry's dependence on very sensitive PII for ID verification while relieving it of one more piece of information it must secure through regulatory guidelines. It would also empower the industry to improve its patient care by providing a unique identifier for each patient. Health-care industry experts indicated that one of the main reasons they collect SSN is to have access to a unique identifier in their systems that can be used to make distinctions between patients who have similarities in other PII data points, such as name and address, and reduce legal liability due to malpractice.

"If we don't have an address on file because this is your first time here or it doesn't match what we have in the system, that's when we'll defer to, 'Let me have your Social Security number.' Like I said, we use any sort of feature that we can use to help distinguish one patient from another. The last thing we ever want to do is mix up medical records and medical charts."

— Compliance Officer, Regional Health-Care Provider

Despite these benefits, the debate is about whether such a universal code will yield benefits for patient security and comfort or result in greater commercial use of patient data and breach of patient privacy. Industry and critics are divided but not dismissive.¹²

Figure 15. Health-Care Industry Key Takeaways

Key Takeaways: Health-Care Industry
Industry Practices and Perspectives • Data collection policies and standards in the health-care industry are bound by regulatory requirements, privacy act guidelines, and software restrictions. • Health-care industry experts express concern about collecting SSNs and indicate that from a compliance standpoint, collecting SSNs is not necessary but the structure of their existing data systems make avoiding collecting SSNs difficult. • Overall, payers and providers are satisfied with current data collection policies their organizations have in place and believe that though improvements are possible, the ID verification system works efficiently and does not place undue pressure on providers to police their patients. • There is a struggle among providers and payers to manage the vast amount of information being collected, but collecting less data is challenging due to identity verification and logistical requirements. • From a privacy perspective, this puts some health-care organizations in a difficult position. They must collect and secure sensitive PII from their patients/customers, increasing their information liability in the case of a data breach. • The industry currently lacks an easy, uniform way to identify patients and link them to their health data, doctors, hospitals, pharmacies, and insurance plans, which is creating a wall of unrelated patient identity numbers bogging down the medical records system. • Streamlining the ID verification system would require more comprehensive tools – such as a universal health-care ID – but a lack of national appetite for such a system limits the chances of these tools gaining traction at a national level. According to industry experts, this is motivating the collection of the SSNs from patients instead.
Consumer Perceptions • Consumers express a defined opinion of what information they believe is relevant for health-care providers to collect vs. what they believe is superfluously collected by the systems. • Regardless of scenarios, overall consumers are willing to share “low sensitivity” PII such as name, age, gender, and address, suggesting that expectations have been well-established. • Yet when patients are examined more closely and broken into groups based on their behaviors, nearly half display flexibility – willing to share most PII and hesitating only slightly when the data is of the most sensitive in nature.

Detailed findings: Retail industry

Overview

The retail industry collects a high volume of PII and is considered more vulnerable to cyberattacks due to a rash of recent high-profile security events.¹³ Retailers require PII in a format similar to that of the financial services industry, in terms of the volume and sensitivity of the data, yet they have seen increased criticism recently for not staying on par with technology and meeting security standards that are common in other industries.¹⁴ Additionally, recent data breaches at national retailers have shaken consumer confidence in the ability of many retailers to provide adequate security around the PII they collect.

PII identification practices in the retail industry are driven by three distinct needs: fraud mitigation, marketing, and regulatory guidelines. For businesses that accept credit card transactions, Payment Card Industry Digital Security Standards (PCI DSS) compliance becomes a critical issue for transforming data collection practices relating to credit and debit card information. Maintaining compliance is an ongoing effort with indirect consequences for other types of PII, but even compliance does not necessarily ensure security.

From a fraud mitigation perspective, retailers continue to struggle to contain the effect of fraud. With retail merchants paying \$3.08 for each dollar of fraud loss they experienced in 2014 (up \$0.29 on the dollar from 2013), they are acutely aware of the real costs associated with data breaches and fraud.¹⁵ Retail industry experts indicated that despite the effectiveness of their current ID verification policies and practices, they are constantly looking for ways to improve them. Doing so is tricky, however, as retailers are forced to balance the demands of strong identity verification procedures with the consumers' demand for swift and easy transaction experiences.

As a result of their unique business requirements, many retailers employ a diversified strategy for ID verification and fraud prevention. The majority of ID verification at the point of sale and online (as well as for credit applications) involves a combination of costly in-house teams and third-party vendors. However, most of this verification involves using less sensitive information and relies less on SSN and other "high sensitivity" PII that might turn customers away from their products.

"In the business of preventing fraud, a lot of it is for verification purposes. We use third-party vendors to verify payment data, and that's kind of the typical standard in the industry. So from a credit standpoint, there's a third-party vendor that we would use in addition to that we have a fraud and audits team. At that level it's usually line level with people doing basic verification and allowing the system to do the rest, so basic verification, phone number, name, address, things like that nature and not the real deep-dive information."

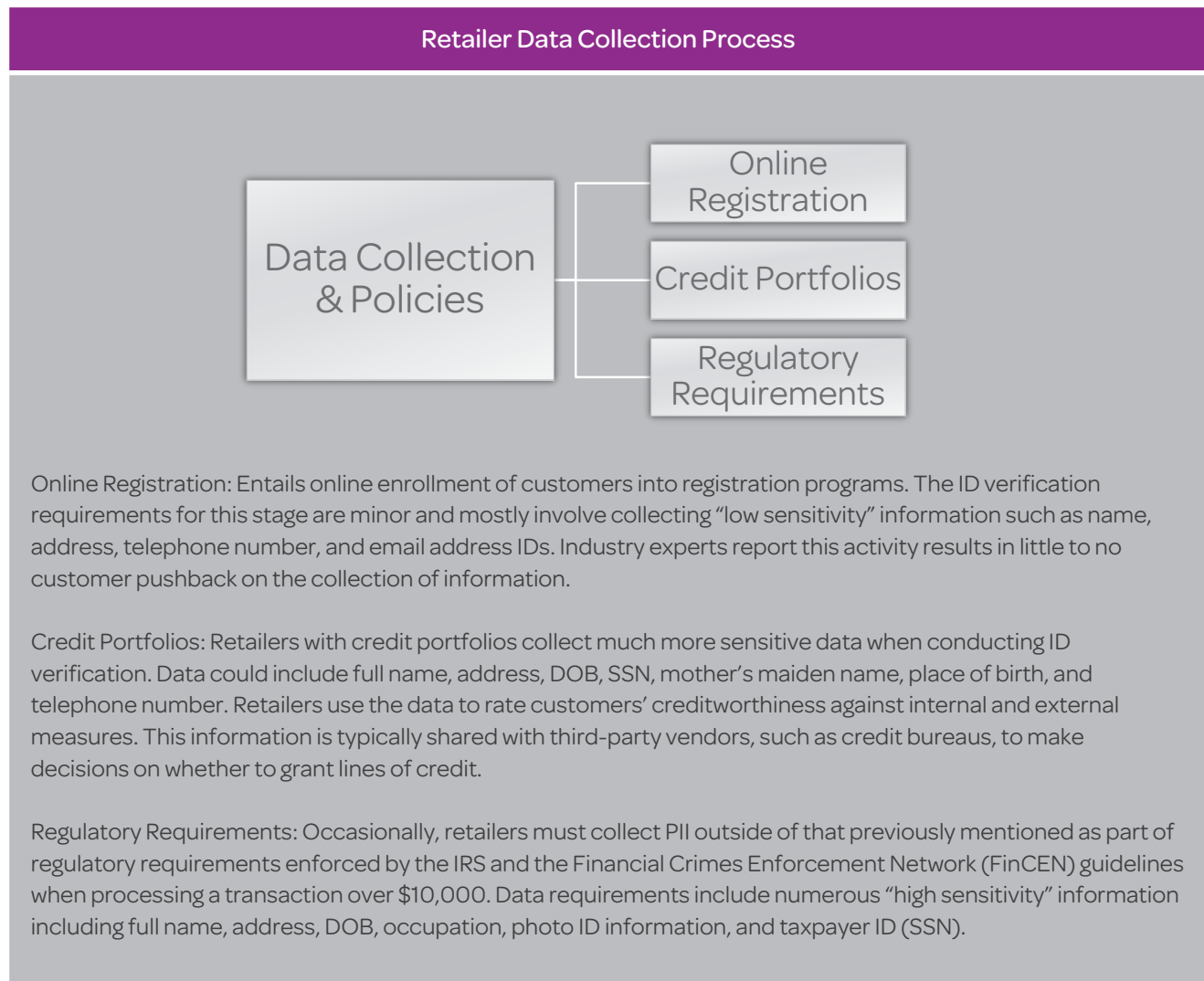
— Data Systems And Investigations Manager, Large Multichannel U.S. Retailer

Types and use of PII collected

Given the variety of payment methods accepted as well as the various touch points (from online and mobile to physical brick-and-mortar) retailers have with their customers, retailers have a more complex method of PII collection than other industries such as financial services or health care. For most everyday interactions, many retailers collect significant amounts of information from their customers. The level and scope of this information can differ depending on the products, policies, and business size.

Policies on the collection of PII in the retail industry are typically divided into three main areas: online registration, credit portfolios, and regulatory requirements.

Figure 16.Areas of PII Collection in the Retail Industry



General consumer data-sharing behaviors

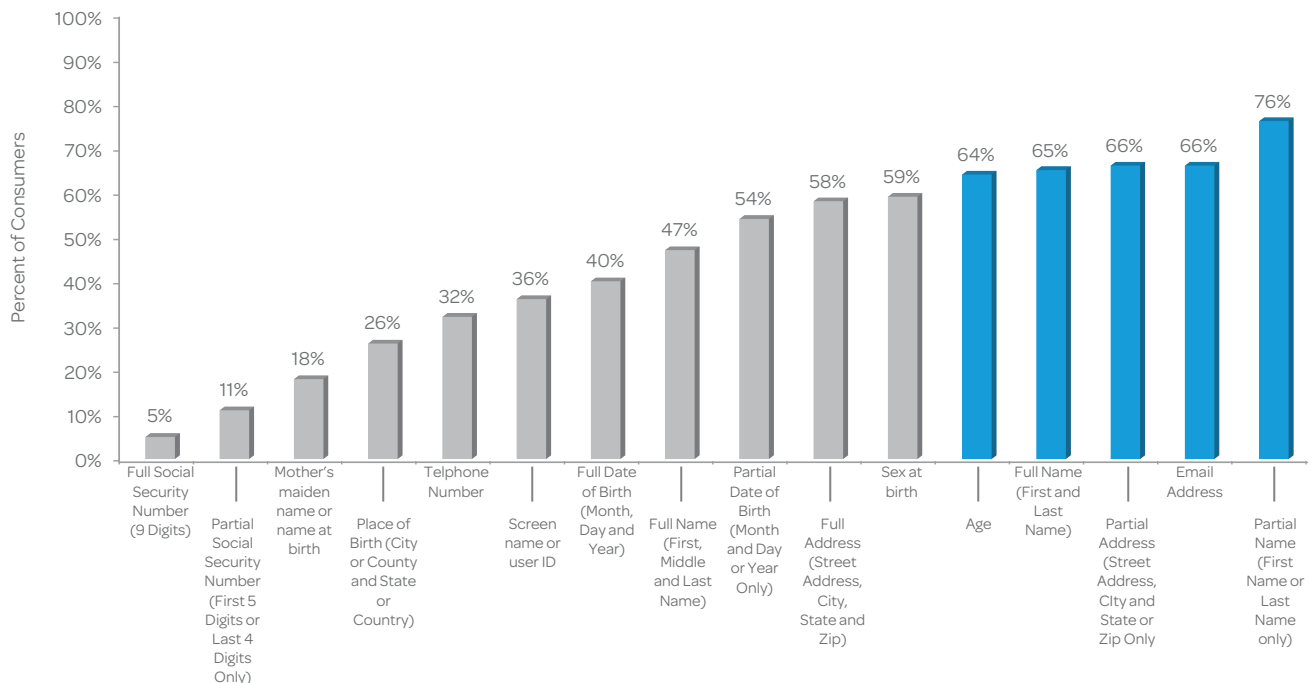
Given the media attention on new data breaches, it is not surprising that data reveals consumers exhibit the least trust in the retail industry. Only 17% of consumers trust retailers with their PII for enrolling to open and maintain an account, compared with 60% of consumers who trust financial institutions and 50% who trust a health-care organization with their information in a similar scenario (see Figure 6).

Interestingly, retailers indicate that despite recent data breaches at big retailers, consumers are still willing to share most types of PII with them. However, they recognize that national media attention is strongly encouraging customers to question why retailers need to collect PII.

“People are much, much more sensitive to it today based on the media with breaches and the NSA side. So I think we are starting to see a shift where customers are becoming not really angry or upset but just asking the question of ‘Is that data you need and why.’”

– Data Systems And Investigations Manager, Large Multichannel U.S. Retailer

Figure 17. Consumers’ Willingness to Share PII When Registering to Receive Coupons and Rewards



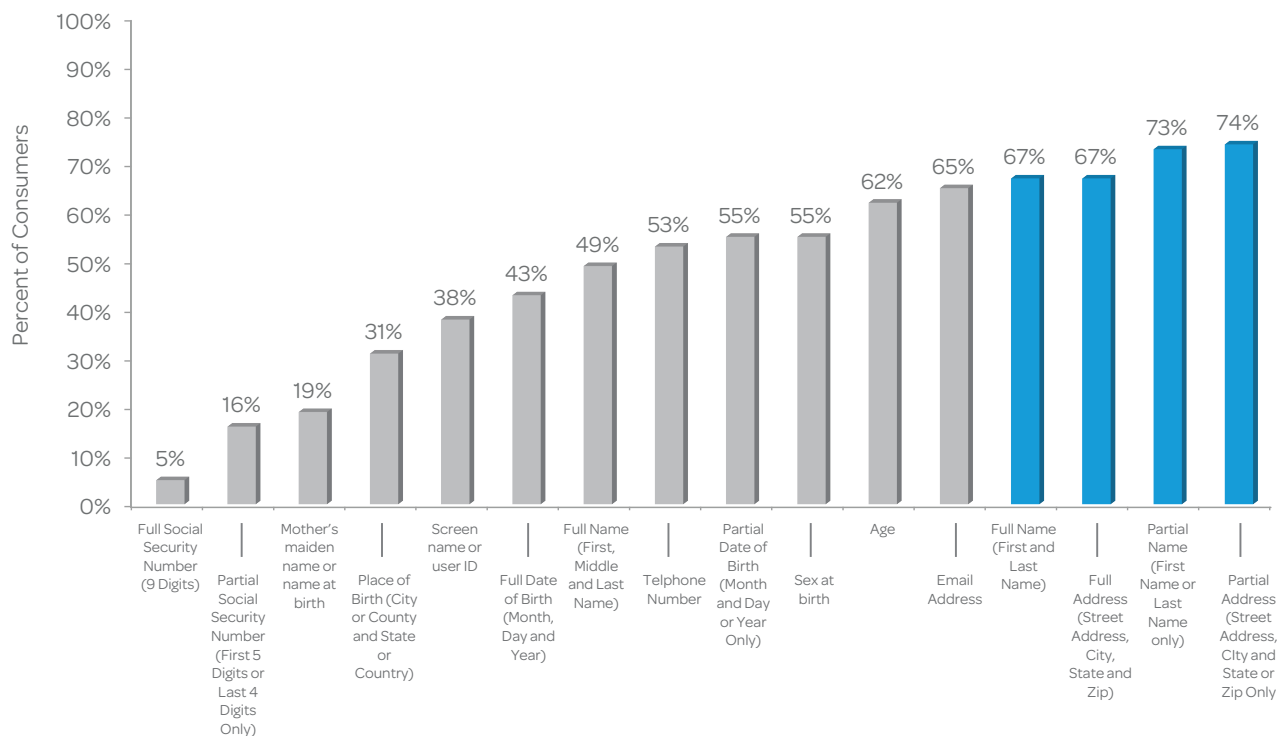
Q: You are registering to receive retailer coupons and discounts, please answer how willingly you will share the information in this scenario. Please rate on a scale of 1 to 10 where 1 means 'Not At All Willing' and 10 means 'Totally Willing'. TOP 3 BOX SHOWN

December 2013, n = 605.
Base: Consumers assigned to Retail Group.

Retailers' perceptions generally match consumers' reported willingness to share PII. In particular, retailers believe consumers who have already shared some information with a retailer to complete a purchase are more inclined to share additional information in order to return a product. However, this is largely true for only "low sensitivity" PII, and retailers are aware that "high sensitivity" PII, such as a full or partial SSN or mother's maiden name, will generate pushback from consumers regardless of the type of transaction.

Consumers expressed similar attitudes when asked if they would be willing to share PII in order to return an item online for a refund. In this scenario, over 2 in 3 consumers said they would be willing to share "lower sensitivity" PII such as name and full address (see Figure 19). And while relatively scant, a small proportion of consumers expressed a willingness to share their SSN to complete an online refund (5%), suggesting indifference or inaccurate expectations among some consumers when sharing sensitive data (see Figure 19).

Figure 18. Consumers' Willingness to Share PII When Registering to Receive Coupons and Rewards, by Age Group



Q: You are returning an online purchase for a refund. For each of these personal identifying information, please answer how willingly you will share the information in this scenario. Please rate on a scale of 1 to 10 where 1 means 'Not At All Willing' and 10 means 'Totally Willing'. TOP 3 BOX SHOWN

December 2013, n = 605.
Base: Consumers assigned to Retail Group.

Retail industry experts say consumers have come to expect that much of this information is required for these types of activities. They note that many customers actively request access to rewards and coupon programs and that even though additional PII (e.g., age, full name, and sex at birth) are sought to support marketing needs, they are typically optional. Other activities, such as returning items online, do not typically require additional PII than what is collected during the purchasing process and do not place additional burdens or risk on the consumer.

“They’re very willing to share. And the reason I say that is because they already provided all that information on the website. It’s ‘You already have my information. Let’s just validate it.’ And that’s that.”

– Senior Manager of Loss Prevention, Large National Retailer

Consumers are much less likely to share “high sensitivity” PII such as SSN and historical identifiers (mother’s maiden name and place of birth). Nearly 31% of consumers say they would be willing to share any “high sensitivity” PII in order to return an item purchased at a retailer. An overwhelming majority, however, is willing to share “low sensitivity” PII with retailers in return for access to coupons or rewards programs or to return items.

Consumer group profiles

Correlating closely with the perspectives of retail industry executives on consumer willingness to share PII, the behaviors of different groups of consumers closely aligns with the sensitivity of the PII being requested. While the respective groups of consumers are not overly polarized with the greatest proportion of the population in the relatively generous group 3 (the Unlikely to Resist group) (40%), at least one in four consumers effectively abstains from sharing PII with retailers (the Total Privacy group). Retailers face the greatest challenge among businesses in all industries examined when soliciting PII from consumers. They can develop more effective strategies for their marketing and sales efforts by understanding how their customer base aligns with the following groups.

Figure 19. Consumer Group Profiles for the Retail Industry

Retail Industry Consumer Groups			
Likelihood that consumers in this group are ...	Group 1. Total privacy, lowest willingness (25% of consumers)	Group 2. Avoid the sensitive, medium willingness (35% of consumers)	Group 3. Unlikely to resist, highest willingness (40% of consumers)
Aged 45-54 years	↓	↓	↑
Aged 65+ years	↑	--	↓
of Hispanic descent	↓	↑	--
Fraud victims (ever in lifetime)	↓	--	↑
Early adopters of new technology	↓	↑	--
Rural-dwellers	↑	--	↓

Group 1: Total Privacy (25% of consumers)

Decides to share PII based on: The sensitivity of PII requested

Overall willingness to share PII: Low

They are more likely to be:

- Over the age of 65 (25%)
- Living in a rural area (34%)

They are less likely to be:

- Between 45 to 54 years of age (15%)
- Hispanic (3%)
- Previous identity theft victims (18%)
- Early-adopters of new technology (10%)

Synopsis:

Whether as a result of a lack of conditioning to share PII with retailers or possibly due to recent public concerns around data breaches in the retail industry, this group is wholly unlikely to share their PII with retailers. While the sensitivity of the PII requested does play a minor role in the likelihood to share that information, they are generally disinclined to share even less sensitive forms of PII with retailers in every scenario.

Key takeaway:

Every effort should be made to minimize requests for PII, including streamlining requirements for this population, and requesting less sensitive, but accurate information that can be supplemented with alternative data sources only when absolutely necessary.

Group 2: Avoid the Sensitive (35% of consumers)

Decides to share PII based on: The sensitivity of PII requested

Overall willingness to share PII: Medium

They are more likely to be:

- Hispanic (12%)
- Early-adopters of new technology (24%)

They are less likely to be:

- Between 45 to 54 years of age (14%)

Synopsis:

Consumers in this group are moderately hesitant to share most PII with retailers, regardless of scenario. Attempts to solicit more sensitive PII are likely to be rebuffed by this group, again irrespective of the level of risk involved in the interaction. Most effectively balancing the data collection needs of retailers with the preferences of these consumers will require relying on fewer pieces of less sensitive PII being directly sourced from them.

Key takeaway:

Any PII that is requested from these consumers should be limited to that which is less sensitive in nature and should be accompanied by an explanation of how it is used. Requesting the most sensitive PII from this group should only be done when no alternative exists, as it could have a deleterious effect on the relationship.

Group 3: Unlikely to Resist (40% of consumers)

Decides to share PII based on: The sensitivity of PII requested

Overall willingness to share PII: High

They are more likely to be:

- Between 45 to 54 years of age (24%)
- Previous identity theft victims (32%)

They are less likely to be:

- Over the age of 65 (15%)
- Living in a rural area (19%)

Synopsis:

The most easygoing of all groups when confronted with data collection requests from retailers, these consumers are generally willing to provide less sensitive PII in scenarios of every risk level. There is likely to be some resistance from this group whenever requesting more sensitive PII as their willingness to share this data is low in every scenario.

Key takeaway:

Retailers can feel free to ask for basic PII from this group as they are unlikely to take issue with these requests. In a scenario where more sensitive PII is needed, retailers can avoid most pushback from this group by turning to alternative sources for collecting the information.

PII collection in the future

There is a general perception among retailers that the amount of data they collect is sufficient to identify their customers given their current needs. When asked to explain their perception, many retailers point to their third-party partnerships for their current success in customer identification.

“From an investigation or even from just a validation standpoint, we’re pretty comfortable that a LexisNexis brand is going to give me the best results available.”

– Data Systems And Investigations Manager, Large Multichannel U.S. Retailer

However, when asked if they could use less information or simply “lower sensitivity” PII, retail industry experts had doubts that lowering their current standards could be sufficient to identify consumers. Given the complexity of PII collection in the retail industry, reducing the PII collected to just name and address could serve some functions, but not all.

Identity verification needs for marketing purposes are very low-risk, and PII such as address and name are sufficient. Marketing does not have the stringent ID verification requirements needed for shipping goods or processing payments. Low-sensitivity PII such as name and address to ID customers would be insufficient for purposes such as processing credit cards or large payments.

However, even as more stringent PII collection serves to bolster fraud mitigation, retailers are also concerned about the customer experience. There is a definite need to balance fraud mitigation with seamless transaction and customer convenience. Maintaining this balance is a challenge for retailers and a leading policy issue.

Figure 20. Retail Industry Key Takeaways

Key Takeaways: Retail Industry	
Industry Practices and Perspectives	
• Retailers have multiple needs for PII: marketing, credit portfolio management, and regulatory requirements and compliance.	
• Marketing programs at major retailers require low-sensitivity PII such as name and address – but these “lower sensitivity” data points are perceived to be insufficient for fraud mitigation.	
• With the growing threat of cyberfraud there is a greater need for effective, low-friction ID verification. Retailers are facing increased pressure to balance customer convenience and ID verification, especially for the online and mobile channels.	
• Retailers expect increasing pushback from their customers going forward as large data breaches, national media attention, and increasing government scrutiny are heightening consumer awareness of the security risks that retailers face when handling customer data.	
• Future needs lie in gaining consumer trust, balancing consumer convenience and privacy concerns with ID verification, as well as strengthening relationships with capable and compliant vendors.	
Consumer Perceptions	
• Consumers display the lowest levels of trust in sharing PII with the retail industry.	
• Overall, consumers are willing to share “low sensitivity” information such as name, address, and email address with retailers, but they are reluctant to share “higher sensitivity” data such as their SSN, mother’s maiden name, and place of birth.	
• Whether due to customer conditioning or the recent slate of retailer data breaches, one in four consumers effectively avoid sharing almost any type of PII with retailers.	

Detailed findings: Government

Overview

Unlike other industries, government agencies' PII collection policies and programs are primarily derived from standards placed upon them by government regulations and their funding sources.

- **Federal regulations** establish standards to verify eligibility for programs and warrant the collection of PII such as income, age, and legal status.
- **The HIPAA and ACA regulations** drive the PII collection in the Health and Human Services sectors and are heavily focused on safeguarding consumers' privacy. They establish the main frameworks for enrolling users in government health-care services.
- **State-level regulations** supplement federal privacy protection regulations and might vary in size and scope at a state-by-state level.

The primary goal for government agencies is meeting the regulatory requirements at the federal and state level and the general safeguarding of PII information. Fraud prevention, mitigation, and identity theft prevention appear almost secondary to the main goal of compliance.

Types and use of PII collected

Government agencies collect the most information of all industry groups. Some government agencies, such as tax revenue entities, require less information from their users but rely heavily on "high sensitivity" data such as SSN. Health and human services organizations collect the most information by far. In addition to full name and SSN, they are also required to collect more sensitive information such as DOB, mother's maiden name, place of birth, annual income, and legal status. Some federal programs, or state and local programs that use federal funding, also request their enrollees to provide demographic data including race, ethnicity, and gender that is used as part of their required program monitoring.

Government officials say most of the sensitive information they collect is the result of state and federal regulations that require local agencies to authenticate the legal status of applicants, verify their eligibility to enroll in the programs, and prevent fraud.

"States use matching funds from the federal government to provide services that have various age and income requirements. So the collection of that data is necessary to determine who is eligible, and we have to prove to the Center for Medicaid Services that we're conducting the program in an efficient and appropriate manner required by federal regulations and law."

— Governmental Program Analyst, State Medicare Agency

The collection and protection of such sensitive data are becoming increasingly problematic. A Government Accountability Office report in 2014 indicated that there were 25,566 "information security incidents" during the previous year, up from 22,156 in 2012. Breaches involving PII at the federal level have also more than doubled over the past several years.¹⁶

"In carrying out its responsibilities, the federal government collects large quantities of PII, such as taxpayer data, census data, Social Security information, and patient health information, on American citizens and other residents of our nation. Consequently, it is critical that federal agencies take steps to secure the information they collect, retain, and disseminate and that, when events such as data breaches occur, they respond swiftly and appropriately."

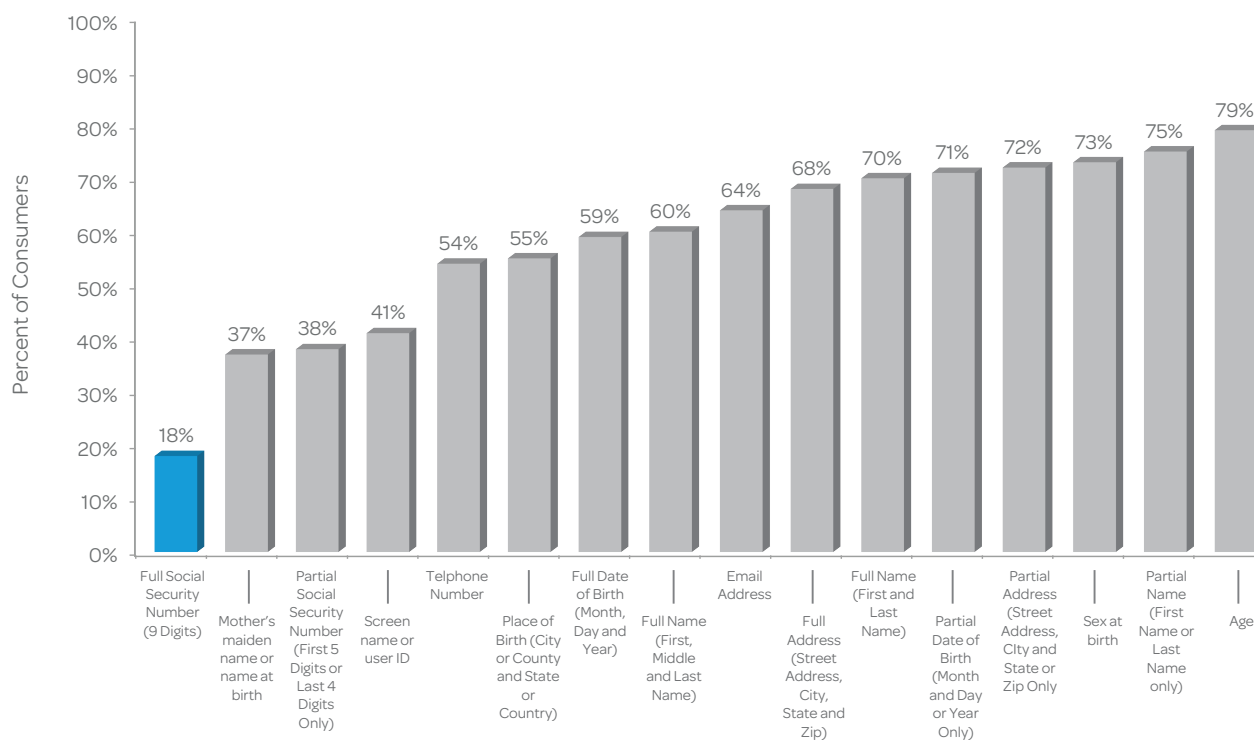
— Gregory C. Wilshusen, Director Of Information Security, GAO, April 2, 2014¹⁷

The report noted that many major federal agencies face challenges in fully implementing their security programs. Some of agencies that the GAO reviewed had incomplete breach-response policies and procedures in place and that their implementation of Office of Management and Budget and National Institute of Standards and Technology guidance was inconsistent.¹⁸ These issues highlight the tenuous situation many government agencies face, particularly those at lower levels of government who might not have the resources to secure the PII they collect from consumers.

General consumer data-sharing behaviors

Despite evidence of increasing numbers of data breaches among government agencies in the U.S, consumer trust in government agencies remains high. Consumers report high willingness to share PII such as address, name, age, gender, and date of birth, regardless of the level of risk. While the government places third, behind the financial services and health-care industries in overall consumer willingness to share PII when opening a new account (see Figure 6), over two-thirds of consumers say they would be willing to share at least low- to medium-sensitivity PII with government agencies even when conducting lower-risk activities such as enrolling in or registering for general programs or benefit details (see Figure 21).

Figure 21. Consumers' Willingness to Share PII With Government Agencies When Registering to Receive Program Details or Benefits

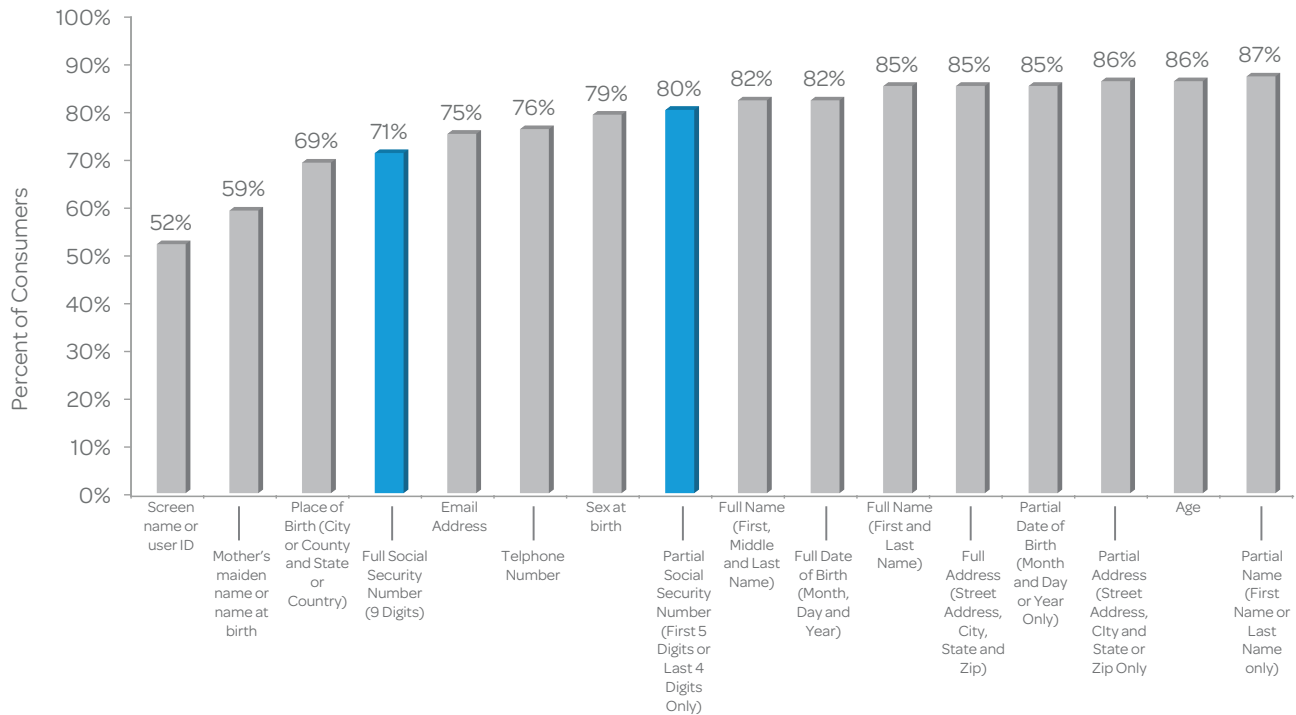


Q: You are registering to receive general program or benefit details, please answer how willingly you will share the information in this scenario. Please rate on a scale of 1 to 10 where 1 means 'Not At All Willing' and 10 means 'Totally Willing'. TOP 3 BOX SHOWN

December 2013, n = 600.
Base: Consumers assigned to Government Group.

Consumers are more willing to share their most sensitive PII such as SSN in high risk scenarios with government agencies, than in high risk scenarios with any other industry. Seventy-one percent of consumers stated they would be willing to share their SSN with the government when filing to get federal refunds (see Figure 22). Consumers' degree of willingness depends on the risk level of the scenario. Willingness dwindles in proportion to the situation's "riskiness," as fewer than 1 in 5 consumers would give up SSN in a low-risk situation (see Figure 21).

Figure 22. Consumers' Willingness to Share PII With Government Agencies When Filing a Tax Return



Q: You are filing your Federal tax return to receive a tax refund, please answer how willingly you will share the information in this scenario. Please rate on a scale of 1 to 10 where 1 means 'Not At All Willing' and 10 means 'Totally Willing'. TOP 3 BOX SHOWN

December 2013, n = 600.
Base: Consumers assigned to Government Group.

This suggests consumers' willingness to share "high sensitivity" PII is heavily tied to their perception of the "risk" of the situation – affecting their view of security needs. Consumers most likely perceive that these riskier activities carry greater governmental security and scrutiny. When asked about the level of perceived security for each risk-based scenario, consumers felt most secure when high-risk information was used to create their account. Seventy percent of consumers said they believed their information was secure when interacting with government agencies during high-risk scenarios such as filing a tax return (see Figure 23).

Figure 23. Perception of Security Risk Based on Risk Scenarios



Q: Considering that your account and unique identity will be created using the following personal identifying information, how secure do you think your account will be? Please rate on a scale of 1 to 10 where 1 means 'Not At All Secure' and 10 means 'Extremely Secure'. TOP 3 BOX SHOWN

December 2013, n = 561, 561, 537.
Base: Consumers assigned to Government Services and Rating At least One PII in Top 3 Box for each type of scenario

Paralleling the consumer mind-set, government officials feel that although consumers might sometimes get frustrated with the long process of data collection, ultimately they understand and agree with the level of scrutiny that is mandated.

"These are typically members of the public looking for assistance, so they rarely have pushback if ever about the types of information they are required to give us. Most of these program participants are used to sharing this kind of information, and there is an inherent trust associated with government agencies."

– Branch Chief, State Department of Housing and Community Development

Consumer group profiles

Politics can be an immensely divisive subject, discussions of which often elicit strong emotions on the role of government and the value of the services it provides. This may contribute to the fact that among all of the industries examined, consumer behaviors in response to government scenarios were the only ones which clearly fell into four groups as opposed to three. Unfortunately, identifying consumers in two of these groups by their demographic factors alone is a challenge.

Representing more than half of all consumers and very different perspectives on sharing PII, the Completely Silent group (42%) and the Open Book group (11%) are barely differentiated from each other demographically, and are only differentiated from the general population by their employment status.

Figure 24. Consumer Group Profiles for the Government

Government Consumer Groups				
Likelihood that consumers in this group are ...	Group 1. Completely silent, lowest willingness (11% of consumers)	Group 2. Active-minders, medium willingness (20% of consumers)	Group 3. Fairly flexible, medium willingness (28% of consumers)	Group 4. Open-book, highest willingness (42% of consumers)
Aged 45-54 years	--	↑	↓	--
Aged 55 to 64 years	--	↓	↑	--
Data breach victims (ever in lifetime)	--	↑	↓	--
Retired	↓	--	↑	↓
Employed full-time	--	--	↓	↑

Group 1: Completely Silent (11% of consumers)

Decides to share PII based on: The sensitivity of PII requested

Overall willingness to share PII: Low

They are less likely to be:

- Retired (14%)

Synopsis:

Government agency attempts to solicit PII from this group will largely be met with consternation. Consumers in this group display the lowest willingness to share every type of PII in every scenario, which includes a nominal willingness to share the most sensitive PII, such as SSNs.

Key takeaway:

Successfully identifying these consumers will require agencies to supplement the very few pieces of PII that they are willing to share with data from alternative sources, making the effectiveness of any data collected critical.

Group 2: Active Minders (20% of consumers)

Decides to share PII based on: The sensitivity of PII requested and the riskiness of the situation

Overall willingness to share PII: Medium

They are more likely to be:

- Between 45 to 54 years of age (27%)
- Previous data breach victims (47%)

They are less likely to be:

- Between 55 to 64 years of age (9%)

Synopsis:

Consumers in this group actively mind their PII, with their decision to share this information guided by both the sensitivity of the data requested and the risk level of the scenario. Government agencies that request PII from this group will find that they are generally willing to share less sensitive PII in medium and high risk scenarios, while they may be less inclined to share that same PII in low-risk scenarios.

Key takeaway:

Overall they will take greatest issue with requests for the most sensitive PII, so attempts to identify these consumers should rely on the breadth of less sensitive information they are willing to share. When PII is necessary for riskier situations, communicating the drivers for the use and collection of that information will encourage their participation.

Group 3: Fairly Flexible (28% of consumers)

Decides to share PII based on: The sensitivity of PII requested

Overall willingness to share PII: Medium

They are more likely to be:

- Between 55 to 64 years of age (20%)
- Retired (30%)

They are less likely to be:

- Between 45 to 54 years of age (14%)
- Previous data breach victims (31%)
- Employed full-time (30%)

Synopsis:

This group behaves similarly to the Active Minders group as they display a willingness to share PII that is based on the sensitivity of the information being requested, except in the case of a low-risk scenario. In such a circumstance, government agencies would be met with slightly more resistance when requesting the most sensitive PII.

Key takeaway:

Attempts to identify consumers in this group should involve requesting the most effective mix of PII among less sensitive information, except in low-risk scenarios where supplementing with an alternative data source may be necessary.

Group 4: Open Book (42% of consumers)

Decides to share PII based on: The sensitivity of PII requested

Overall willingness to share PII: High

They are more likely to be:

- Employed full-time (45%)

They are less likely to be:

- Retired (17%)

Synopsis:

The easiest of all consumer groups to solicit for PII, members of this contingent will freely share PII in every scenario. This predisposition for sharing PII extends to the most sensitive of PII, with only a slight decline in willingness which is most apparent in low-risk scenarios. Securing PII to positively identify consumers in this group should be met with little to no resistance in most cases.

Key takeaway:

In the case of a low-risk scenario, government agencies could encourage the greatest degree of participation while ensuring identity verification by limiting their requests to less sensitive, but accurate forms of PII.

PII collection in the future

Like experts in other industries, most government officials view their practices as very effective at identity verification. They understand their data collection can be intrusive and lengthy but strongly believe the current federal and state requirements for photo IDs and detailed PII collection are integral in making the current verification system function smoothly.

In fact, far from data minimization, there is a growing perception among health and human services agencies that identification requirements will likely become even more rigorous as consumer identity theft-related fraud – which was an \$18 billion problem in 2013 – gains increasing public attention.¹⁹ As media attention on the dangers of ID theft grows, most government officers believe federal and state regulators will likely place additional requirements on government agencies for ID verification. These new requirements will most likely result in increased data collection requirements.

Despite this perception, some agencies have made attempts at curtailing the amount of information they require in the face of growing public resistance. Some tax revenue agencies reported that in the past they have explored the use of alternative taxpayer IDs and secured email messaging in order to avoid requiring users to provide “higher sensitivity”.

“Taxpayers are reluctant to share personal identifying information because of [identity fraud and the threat of data breaches] except when required to do so. Our organization has researched alternative methods of requesting information, such as using TPIDs instead of SSNs, truncating SSNs, etc. We also use additional security methods such as secured email, encryption, etc.”

– Public Affairs Officer, State Franchise Tax Board

There is also some interest in exploring biometrics as an identification tool in the future. Some health and human services organizations indicated that biometrics could play a stronger role in the future of ID verification. However, most government experts say increasing public resistance to this technology makes the prospect of bringing it to government agencies dubious at best.

Alternatively, some agencies are taking steps to protect the data they already collect, rather than reduce their current volumes. With the release of recent GAO reports, industry experts are also speculating whether better protection of collected PII might be the more urgent task at hand. Ultimately, a balance between the two would satisfy existing federal mandates while providing security against threats that target data that must be collected and maintained.

Figure 25. Government Agencies Key Takeaways

Key Takeaways: Government Agencies
Industry Practices and Perspectives
• Government agencies collect the most comprehensive and intrusive levels of PII. • Identity verification policies at government agencies are often driven by policies mandated by federal and state funding requirements. • Protection and privacy of collected data are emerging as a key concern in the face of growing data breaches and cyberattacks at all levels of government. • Despite the risk that collecting additional PII could create in the event of a data breach and federal mandates to the contrary, experts in government agencies fear that data collection might become even more onerous to consumers in an attempt to better mitigate identity fraud.
Consumer Perceptions
• Consumers' trust in government agencies lags behind that of the financial services and health-care industries. • While nearly half of consumers will freely share most PII with government agencies, a small but demographically similar group refuses to let the government know much more than their name. This makes distinguishing between them, and consistently verifying their identity through PII a considerable challenge.

Appendix

Figure 26: Heat map of Financial Industry Consumer Information-Sharing Profiles

Financial Industry		Consumer PII-Sharing Profiles (mean rating of willingness-to-share)		
		Group 1. Cautious, yet flexible, medium- willingness (28% of consumers)	Group 2. Data- sharing skeptics, lowest willingness (26% of consumers)	Group 3. Ready and willing, highest willingness (47% of consumers)
Mean Overall Willingness to Share PII (on a scale of 1 to 10, where 1 = not at all willing and 10 = totally willing)		7	5	8
High risk: Opening a new bank account	Full Name (First, Middle and Last Name)	9	6	9
	Full Name (First and Last Name)	10	6	9
	Partial Name (First Name or Last Name only)	9	6	9
	Full Address (Street Address, City, State and Zip)	9	6	9
	Partial Address (Street Address, City and State or Zip only)	9	6	9
	Full Date of Birth (Month, Day and Year)	9	5	9
	Partial Date of Birth (Month and Day or Year Only)	9	6	9
	Age	10	6	9
	Place of Birth (City or County and State or Country)	8	5	9
	Full Social Security Number (9 Digits)	8	4	8
	Partial Social Security Number (First 5 Digits or Last 4 Digits Only)	9	5	8
	Telephone Number	9	6	9
	Email Address	9	6	9
	Screen name or user ID	7	5	8
	Sex at birth	9	6	9
Medium risk: Applying for a new auto loan	Mother's maiden name or name at birth	8	4	8
	Full Name (First, Middle and Last Name)	9	5	9
	Full Name (First and Last Name)	9	6	9
	Partial Name (First Name or Last Name only)	9	6	9
	Full Address (Street Address, City, State and Zip)	9	5	9
	Partial Address (Street Address, City and State or Zip only)	9	6	9
	Full Date of Birth (Month, Day and Year)	9	5	9
	Partial Date of Birth (Month and Day or Year Only)	9	5	9
	Age	9	6	9
	Place of Birth (City or County and State or Country)	7	5	9
	Full Social Security Number (9 Digits)	7	3	7
	Partial Social Security Number (First 5 Digits or Last 4 Digits Only)	8	4	8
	Telephone Number	9	5	9
	Email Address	9	5	9
	Screen name or user ID	6	4	7
Low risk: Using an online mortgage calculator	Sex at birth	9	6	9
	Mother's maiden name or name at birth	6	3	8
	Full Name (First, Middle and Last Name)	3	4	8
	Full Name (First and Last Name)	3	5	9
	Partial Name (First Name or Last Name only)	5	5	9
	Full Address (Street Address, City, State and Zip)	3	4	8
	Partial Address (Street Address, City and State or Zip only)	5	5	9
	Full Date of Birth (Month, Day and Year)	3	4	8
	Partial Date of Birth (Month and Day or Year Only)	4	5	9
	Age	6	5	9
	Place of Birth (City or County and State or Country)	3	4	8
	Full Social Security Number (9 Digits)	1	2	4
	Partial Social Security Number (First 5 Digits or Last 4 Digits Only)	2	3	6
	Telephone Number	4	4	8
	Email Address	5	5	8
	Screen name or user ID	3	4	7

Figure 27: Heat map of Health-Care Industry Consumer Information-Sharing Profiles

Healthcare Industry		Consumer PII-Sharing Profiles (mean rating of willingness-to-share)		
		Group 1. Practically carefree, highest willingness (48% of consumers)	Group 2. Tempered responder, medium willingness (12% of consumers)	Group 3. Extremely private, lowest willingness (40% of consumers)
Mean Overall Willingness to Share PII (on a scale of 1 to 10, where 1 = not at all willing and 10 = totally willing)		9	7	4
High risk: Opening an account with a healthcare provider or retail pharmacy to review your medical records, lab results or prescription history online	Full Name (First, Middle and Last Name)	9	7	4
	Full Name (First and Last Name)	10	8	4
	Partial Name (First Name or Last Name only)	10	8	4
	Full Address (Street Address, City, State and Zip)	9	8	4
	Partial Address (Street Address, City and State or Zip only)	9	8	5
	Full Date of Birth (Month, Day and Year)	9	7	4
	Partial Date of Birth (Month and Day or Year Only)	10	8	4
	Age	10	8	5
	Place of Birth (City or County and State or Country)	8	6	4
	Full Social Security Number (9 Digits)	5	3	3
	Partial Social Security Number (First 5 Digits or Last 4 Digits Only)	7	5	3
	Telephone Number	9	8	4
	Email Address	9	7	4
	Screen name or user ID	8	5	3
	Sex at birth	10	8	5
	Mother's maiden name or name at birth	8	4	3
Medium risk: Applying for health insurance via a state or federal online health insurance exchange	Full Name (First, Middle and Last Name)	9	7	3
	Full Name (First and Last Name)	10	8	4
	Partial Name (First Name or Last Name only)	10	8	4
	Full Address (Street Address, City, State and Zip)	9	8	4
	Partial Address (Street Address, City and State or Zip only)	10	8	4
	Full Date of Birth (Month, Day and Year)	9	7	4
	Partial Date of Birth (Month and Day or Year Only)	10	8	4
	Age	10	8	4
	Place of Birth (City or County and State or Country)	9	6	4
	Full Social Security Number (9 Digits)	6	3	3
	Partial Social Security Number (First 5 Digits or Last 4 Digits Only)	8	6	3
	Telephone Number	9	7	4
	Email Address	9	7	4
	Screen name or user ID	8	5	3
	Sex at birth	10	8	4
	Mother's maiden name or name at birth	9	5	3
Low risk: Making an appointment online with a new dentist or doctor	Full Name (First, Middle and Last Name)	9	7	3
	Full Name (First and Last Name)	10	8	4
	Partial Name (First Name or Last Name only)	10	8	4
	Full Address (Street Address, City, State and Zip)	9	8	4
	Partial Address (Street Address, City and State or Zip only)	9	8	4
	Full Date of Birth (Month, Day and Year)	9	7	4
	Partial Date of Birth (Month and Day or Year Only)	10	8	4
	Age	10	8	4
	Place of Birth (City or County and State or Country)	9	6	4
	Full Social Security Number (9 Digits)	6	3	2
	Partial Social Security Number (First 5 Digits or Last 4 Digits Only)	8	5	3
	Telephone Number	9	7	4
	Email Address	9	7	4
	Screen name or user ID	8	5	3
	Sex at birth	10	8	4
	Mother's maiden name or name at birth	8	5	3

Figure 28: Heat Map of Retail Industry Consumer Information-Sharing Profiles

Retail Industry		Consumer PII-Sharing Profiles (mean rating of willingness-to-share)		
		Group 1. Unlikely to resist, highest willingness (40% of consumers)	Group 2. Avoid the sensitive, medium willingness (35% of consumers)	Group 3. Total privacy, lowest willingness (25% of consumers)
Mean Overall Willingness to Share PII (on a scale of 1 to 10, where 1 = not at all willing and 10 = totally willing)		8	6	4
High risk: Purchasing an age restricted product like tobacco products or lottery tickets.	Full Name (First, Middle and Last Name)	9	5	2
	Full Name (First and Last Name)	9	7	3
	Partial Name (First Name or Last Name only)	9	7	4
	Full Address (Street Address, City, State and Zip)	8	5	3
	Partial Address (Street Address, City and State or Zip only)	9	6	3
	Full Date of Birth (Month, Day and Year)	9	7	4
	Partial Date of Birth (Month and Day or Year Only)	9	8	5
	Age	9	9	6
	Place of Birth (City or County and State or Country)	8	4	3
	Full Social Security Number (9 Digits)	3	1	1
	Partial Social Security Number (First 5 Digits or Last 4 Digits Only)	5	2	2
	Telephone Number	7	4	3
	Email Address	8	5	3
	Screen name or user ID	6	3	3
	Sex at birth	9	6	4
	Mother's maiden name or name at birth	6	2	2
Medium risk: Returning an online purchase for a refund.	Full Name (First, Middle and Last Name)	9	7	4
	Full Name (First and Last Name)	9	8	5
	Partial Name (First Name or Last Name only)	9	9	6
	Full Address (Street Address, City, State and Zip)	9	8	6
	Partial Address (Street Address, City and State or Zip only)	9	9	6
	Full Date of Birth (Month, Day and Year)	9	6	4
	Partial Date of Birth (Month and Day or Year Only)	9	7	4
	Age	9	7	5
	Place of Birth (City or County and State or Country)	8	4	3
	Full Social Security Number (9 Digits)	3	1	2
	Partial Social Security Number (First 5 Digits or Last 4 Digits Only)	5	3	2
	Telephone Number	8	7	5
	Email Address	9	8	6
	Screen name or user ID	7	5	4
	Sex at birth	9	6	4
	Mother's maiden name or name at birth	7	3	2
Low risk: Registering to receive retailer coupons and discounts.	Full Name (First, Middle and Last Name)	9	6	4
	Full Name (First and Last Name)	9	8	6
	Partial Name (First Name or Last Name only)	9	9	6
	Full Address (Street Address, City, State and Zip)	9	8	5
	Partial Address (Street Address, City and State or Zip only)	9	8	5
	Full Date of Birth (Month, Day and Year)	8	6	3
	Partial Date of Birth (Month and Day or Year Only)	9	7	4
	Age	9	8	5
	Place of Birth (City or County and State or Country)	7	3	3
	Full Social Security Number (9 Digits)	3	1	1
	Partial Social Security Number (First 5 Digits or Last 4 Digits Only)	4	2	2
	Telephone Number	7	5	3
	Email Address	9	8	6
	Screen name or user ID	7	5	3
	Sex at birth	9	7	5
	Mother's maiden name or name at birth	6	3	2

Figure 29: Heat Map of Government Group Consumer Information-Sharing Profiles

Government		Consumer PII-Sharing Profiles (mean rating of willingness-to-share)			
		Group 1. Active-minders, medium willingness (20% of consumers)	Group 2. Open-book, highest willingness (42% of consumers)	Group 3. Fairly flexible, medium willingness (28% of consumers)	Group 4. Completely silent, lowest willingness (11% of consumers)
Mean Overall Willingness to Share PII (on a scale of 1 to 10, where 1 = not at all willing and 10 = totally willing)		7	9	8	5
High risk: Filing your Federal tax return to receive a tax refund.	Full Name (First, Middle and Last Name)	9	10	9	5
	Full Name (First and Last Name)	9	10	9	5
	Partial Name (First Name or Last Name only)	9	10	9	6
	Full Address (Street Address, City, State and Zip)	9	10	9	5
	Partial Address (Street Address, City and State or Zip only)	9	10	9	5
	Full Date of Birth (Month, Day and Year)	9	10	9	5
	Partial Date of Birth (Month and Day or Year Only)	9	10	9	5
	Age	9	10	9	6
	Place of Birth (City or County and State or Country)	7	9	8	5
	Full Social Security Number (9 Digits)	9	9	7	4
	Partial Social Security Number (First 5 Digits or Last 4 Digits Only)	9	10	8	5
	Telephone Number	9	10	8	5
	Email Address	8	10	7	5
	Screen name or user ID	6	9	4	4
	Sex at birth	8	10	8	6
	Mother's maiden name or name at birth	5	9	6	4
Medium risk: Requesting a copy of your birth certificate.	Full Name (First, Middle and Last Name)	9	10	9	5
	Full Name (First and Last Name)	9	10	9	5
	Partial Name (First Name or Last Name only)	9	10	9	5
	Full Address (Street Address, City, State and Zip)	9	10	9	5
	Partial Address (Street Address, City and State or Zip only)	9	10	9	5
	Full Date of Birth (Month, Day and Year)	9	10	9	5
	Partial Date of Birth (Month and Day or Year Only)	9	10	9	6
	Age	9	10	9	6
	Place of Birth (City or County and State or Country)	9	10	9	6
	Full Social Security Number (9 Digits)	5	8	5	3
	Partial Social Security Number (First 5 Digits or Last 4 Digits Only)	7	9	6	4
	Telephone Number	8	10	8	5
	Email Address	8	10	7	5
	Screen name or user ID	5	9	4	4
	Sex at birth	9	10	9	6
	Mother's maiden name or name at birth	8	10	9	5
Low risk: Registering to receive general program or benefit details	Full Name (First, Middle and Last Name)	4	9	8	4
	Full Name (First and Last Name)	6	9	9	5
	Partial Name (First Name or Last Name only)	7	10	9	5
	Full Address (Street Address, City, State and Zip)	6	9	9	4
	Partial Address (Street Address, City and State or Zip only)	7	9	9	5
	Full Date of Birth (Month, Day and Year)	5	9	8	4
	Partial Date of Birth (Month and Day or Year Only)	6	10	9	5
	Age	7	10	9	6
	Place of Birth (City or County and State or Country)	4	9	8	5
	Full Social Security Number (9 Digits)	2	5	4	2
	Partial Social Security Number (First 5 Digits or Last 4 Digits Only)	2	7	7	4
	Telephone Number	5	8	8	5
	Email Address	7	9	8	5
	Screen name or user ID	4	8	4	4
	Sex at birth	6	9	9	5
	Mother's maiden name or name at birth	3	7	6	4

Sources

- ¹ <http://online.wsj.com/news/articles/SB10001424052970204124204577154661814932978>
- ² 2013 LexisNexis True Cost of Fraud Study: Merchants Struggle Against an Onslaught of High-Cost Identity Fraud and Online Fraud, Javelin Strategy & Research, September 2013.
- ³ 2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends, Javelin Strategy & Research, February 2014
- ⁴ "Federal Agencies Need to Enhance Responses to Data Breaches." United States Government Accountability Office. Released: April 2, 2014. Source: <http://www.gao.gov/assets/670/662227.pdf>
- ⁵ <http://www.fdic.gov/bank/statistical/stats/2014mar/industry.pdf>
- ⁶ http://www.fincen.gov/statutes_regs/patriot/
- ⁷ http://www.fincen.gov/statutes_regs/bsa/
- ⁸ How to Upgrade Online and Mobile Account Opening for an Omnichannel Era, Javelin Strategy & Research, July 2013.
- ⁹ <http://www.hhs.gov/ocr/privacy/>
- ¹⁰ <http://www.hhs.gov/healthcare/facts/timeline/timeline-text.html>
- ¹¹ <http://online.wsj.com/news/articles/SB10001424052970204124204577154661814932978>
- ¹² Ibid
- ¹³ <http://usa.marsh.com/NewsInsights/MarshRiskManagementResearch/ID/37598/Data-Security-and-Information-Privacy-Risks-in-the-Retail-Industry.aspx>
- ¹⁴ <http://www.tripwire.com/state-of-security/regulatory-compliance/majority-retail-sector-meet-new-pci-standards/>
- ¹⁵ 2014 LexisNexis True Cost of Fraud Study: Post-Recession Revenue Growth Hampered by Fraud As All Merchants Face Higher Costs, Javelin Strategy & Research, August 2014.
- ¹⁶ "Federal Agencies Need to Enhance Responses to Data Breaches." United States Government Accountability Office. Released: April 2, 2014. Source: <http://www.gao.gov/assets/670/662227.pdf>
- ¹⁷ Ibid
- ¹⁸ Ibid
- ¹⁹ 2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends, Javelin Strategy & Research, February 2014.

For more information:

Call: 866.818.0265

Visit: lexisnexis.com/identity

Or email: identitymanagement@lexisnexis.com

About Javelin Strategy & Research

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.

The views expressed by Javelin Strategy & Research are not necessarily those of LexisNexis.

The opinions and quotes expressed in this paper are those of the interviewees and do not necessarily reflect the positions of LexisNexis.

About LexisNexis Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis products. LexisNexis does not warrant this document is complete or error-free. If written by a third party, the opinions may not represent the opinions of LexisNexis.

