



Presents

**Global Study on the Public's Perceptions
about Identity Management**

March 23, 2006

Independently Conducted by



Private & Confidential Document. Please Do Not Quote Without Express Permission.

Global Study on the Public's Perceptions about Identity Management

Report Prepared by Dr. Larry Ponemon, March 23, 2006

Unisys Corporation commissioned this research.

We are pleased to report the results of the Global Study on the Public's Perceptions about Identity Management. Survey fieldwork was launched on February 3, 2006 and completed on March 10, 2006. This perception-capture research was independently conducted by Ponemon Institute to learn what individuals in North America, Europe, Asia-Pacific and Latin America think about several proposed methods for managing identity within business and government organizations.

Identity verification proposals include the creation of one multi-purpose identity credential that can be used broadly.¹ In addition, this study seeks to understand how individuals' sense of privacy would affect their acceptance of new identity management technologies such as biometrics.

Invitations to 16,683 adult-aged individuals throughout the world were sent by e-mail or letter. We received 1,661 usable Web-based survey responses from individuals residing in all four regions (14 countries), resulting in an overall 9.96% response rate. Of these respondents, 464 are North Americans, 427 are Europeans, 450 reside in Asia-Pacific, and 320 are Latin Americans. In addition, another 262 individuals in four countries were selected to participate in direct or telephone interviews. These interviews were used to validate our Web-based survey findings.

Executive Summary

The Global Study on the Public's Perceptions about Identity Management addresses individuals' attitudes about the importance and value of different identity verification methods. The study also attempts to determine possible differences in the privacy or data sharing preferences of people residing in four different regions of the world. While identity management is essential to achieving the security goals of business and government, it is unclear how the public would react to identity verification or authentication methods. It is also unclear how the public might perceive different enabling technologies.

Understanding the public's opinions about identity verification methods is important for two reasons. First, identity management only works if the public cooperates fully and accepts the identity management technology used. If the public considers a particular method or technology as encroaching on their rights to privacy, they will be resistant to adoption. Second, because many organizations operate in the global economy, identity management systems need to function across national borders. Hence, it is important for businesses and governments to construct identity methods that do not violate the cultural, social or ethical sensibilities of a nation or region of the world.

The following findings are the most informative about respondents' perceptions.

- Respondents appear to be willing to share a significant amount of their personal information with organizations to prove or verify their identity. However, findings suggest that individuals' propensity to share sensitive personal information with businesses and governments varies across geographic regions. Specifically, our survey findings show:

¹ In our study, a multi-purpose identity credential is defined as a credential that can be used for many purposes such as accessing online accounts, performing electronic payments, crossing international borders, and gaining entry onto passenger airplanes.

- ✓ Individuals in North America and Asia-Pacific are willing to share more personal data with both a trusted business organization and government than respondents in Europe and Latin America.
- ✓ Individuals in North America, Europe and Asia-Pacific are willing to share more sensitive personal information with government than a business organization. In contrast, respondents in Latin America are willing to share more personal data with business than government.
- ✓ Individuals in all four regions are willing to share substantially more sensitive personal information to receive enhanced verification capabilities (such as having one multi-purpose identity credential that can be used for various functions).
- ✓ The data elements that respondents are most willing to share with business and government includes, name, address and telephone number. The data elements respondents are least willing to share include race, religion, and credit card number.
- ✓ The data element “mother’s maiden name” is accepted by North Americans for identity verification purposes, but is not well accepted in other parts of the world (especially Latin America).
- Respondents in all geographic regions prefer having one identity credential that can be used for multiple purposes or functions. Specifically, our survey findings show:
 - ✓ According to respondents, the most important functions for a multi-purpose identity credential are to prove identity in order to access transportation channels (such as airplanes, trains, and buses), enter public locations (stadiums, airports and others), cross borders (customs) and access Internet accounts.
 - ✓ The least important functions for a multi-purpose identity credential are to use cellular telephones, enter workplace locations (office), drive automobiles (replace key), use PDAs or enter homes.
 - ✓ While many individuals prefer the multi-purpose identity credential to reside on an ID card, a large number of respondents like the idea of having it contained in a biometric, within a cellular phone, or in an article of clothing or jewelry.
 - ✓ While most respondents do not like the idea of an identity credential as a chip implanted in their body, over 10% of individuals in the Asia-Pacific region prefer the implanted chip.
 - ✓ On average, respondents in all regions believe that banking institutions would be the most trusted to issue and manage the multi-purpose identity credential. In contrast, law enforcement (police) and tax authorities are the least trusted to issue identity credentials.
 - ✓ Interoperability across national borders is critical to the success of the multi-purpose identity credential. That is, over 68% of individuals believe it is important or very important that the credential is able to operate across national borders.
- A majority of respondents in all geographic regions accept the use of biometrics for identity verification purposes. Specifically, our survey findings show:
 - ✓ Individuals in North America hold the most positive view of biometrics (71% say yes), while respondents in Latin America hold the least positive view (58% say yes).
 - ✓ The most preferred biometric methods are voice recognition and fingerprints, and the least preferred method is a scan of the iris or eye.

- ✓ The top reasons why respondents consider biometrics a good idea is convenience (not having to remember passwords) and efficiency (or speed) to prove identity. For those who don't want to use biometrics, the top reason is fear or suspicion about how these technologies work. Another concern by some respondents is the loss of privacy.
- A majority of individuals believe certain types of business and governmental organizations need to have more rigorous identity verification methods than others. Our survey findings show:
 - ✓ Banks, law enforcement (police), credit card companies and health care providers are viewed as having the strongest (or most effective) forms of identity verification.
 - ✓ Food (grocery) stores, utilities and education are viewed as having the weakest (or least effective) identity verification methods.

In summary, our global survey findings suggest that personal information sharing preferences vary by organization (business vs. government) and region of the world. Europeans and Latin Americans appear to be more privacy-centric than respondents in North America and Asia-Pacific countries. Despite differences in individuals' privacy-orientations, respondents around the world are supportive of one card or credential that will allow them to prove their identity with different organizations and functional uses. The most important features of this credential would be access to transportation, secure physical locations and crossing international borders.

Individuals around the world overwhelmingly welcome banking institutions to issue this multi-purpose identity credential. They appear to be extremely hesitant, however, to have police or tax authorities control the identity credentialing issuance or management process. Most people appear to be willing to use biometrics to establish their identity with business and government organizations. While many respondents prefer a credential that resides on an ID card, a large number of people are interest in biometrics or an identity device built into their cellular phone.

Conclusions

The purpose of this study was to learn individuals' perceptions about identity management methods and technologies. The universal truth from respondents is that they want the identity management process to be convenient. It appears that people throughout the world want identity verification to make their lives less complex and more secure.

We anticipate that the results of our study will assist global organizations in the private and public sectors determine the most appropriate identity management methods. Each will have to decide on the following:

- Who should administer the identity credential?
- How should it be administered?
- What features should be contained in the credential?
- What education and outreach efforts need to be implemented to ensure acceptance?

Based on the results of our study, banking institutions are most trusted to issue and manage identity credentials. The least trusted organizations of credential issuance are police or law enforcement. Tax authorities are also not viewed favorably as an issuing entity. In consideration of the administrative issues, many respondents in our study appear to be worried that having too much information about themselves in one place will make them more vulnerable to criminal attacks and identity theft.

Respondents to our study are receptive to a variety of methods to prove and manage their identity. However, there are cultural differences that need to be considered. It seems that smart

cards, biometrics and chips imbedded in cell phones or articles of clothing are accepted by people in most countries. While respondents in Asian countries are more accepting of chip implants, the rest of the world does not hold a favorable view of this identity method. With respect to biometrics, people are most receptive to voice recognition and fingerprints. They are uncertain about facial scans, hand geometry and iris (eye) scans.

People are supportive of a multi-purpose identity credential that operates across national borders. Most important to people is the ability to use this credential to travel safely, cross national borders and enter public places that require security safeguards. There is no agreement, however, to use such a credential for more mundane tasks such as having access to your home or starting your car. Another universal finding is that people in all regions of the world are willing to share three key facts about themselves. These are: name, address and telephone number. And, they do not want to share information about their race or religion.

Identity management and technologies are new concepts for most people to understand and feel confident about. Therefore, organizations need to take steps to educate and inform people about how the possible use of identity management methods will make them more secure and provide greater convenience in their daily lives. Without such awareness, universal adoption will be much harder to achieve and may be met with resistance.

Survey

As part of the survey instrument review process, we sought input from a number of learned individuals, including privacy and data security experts. Draft survey items were reviewed and refined with input from Unisys and its research department personnel.

In total, the final survey form consisted of 22 items and nine demographic questions. Items on the survey form were randomized or rotated to mitigate demand or order effects. All completed returns were evaluated for consistency and internal reliability before including in our final sample. Because of our international audience, the English version of the survey instrument was translated in eight natural languages.

Respondents were given the following basic instructions before starting the survey process.

Dear Participant,

The purpose of this study is to learn your opinion about methods used in business and government to verify your identity before allowing you to have access to data systems or secure physical locations. We also want to learn what you expect private and public organizations to do to protect your identity.

We greatly appreciate your response to all survey questions. We believe your participation will help organizations improve their privacy and security protection efforts. Please note, we do not collect any personally identifiable information. If you have questions or concerns about this study, please feel free to contact us at research@ponemon.org.

The survey utilized randomly generated sampling frames developed by Ponemon Institute or purchased from other leading survey sampling companies. In total, separate sampling frames were created within 14 countries. By design, each country's sampling frame was representative of the population of adult-aged individuals who have an active email address (or access to the Internet). The target respondents were recruited and paid nominal compensation. Individuals were invited to participate by email or post card.

Following are the response statistics for 14 countries according to four geographic regions of North America, Europe, Asia-Pacific and Latin America. In total, 16,683 adult-aged respondents submitted survey results. Of these responses, 168 failed reliability tests and were removed from the sample. The final sample of 1,661 represents a 9.96% overall response rate. Non-response bias was tested and there does not appear to be significant sampling discrepancies.²

² A random sample of individuals who elected not to participate were contacted by the researcher to determine the extent of non-response bias. It appears that the main reason for non-response is email address bounce-backs (terminations). Accordingly, there does not appear to be any systematic differences between respondents and non-respondents in these countries.

Pie Chart I and the accompanying Table 1 show the distribution of sample respondents by country, geographic region of the world, sample size and response rate.

Pie Chart 1: Sample Response by Geographic Region

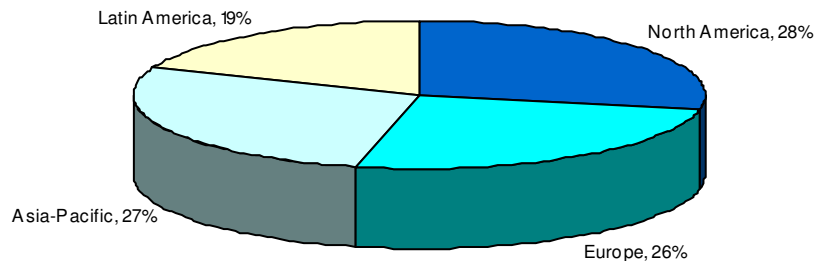


Table 1: Sample Response Statistics by Country and Region

Country	Geographic Region	Sampling Frame	Final Sample	Response Rate
United States	North America	4,832	397	8.22%
Canada	North America	799	67	8.39%
Germany	Europe	1,411	140	9.92%
France	Europe	1,186	103	8.68%
United Kingdom	Europe	1,230	150	12.20%
Denmark	Europe	451	34	7.54%
Japan	Asia-Pacific	2,350	262	11.15%
Korea	Asia-Pacific	485	54	11.13%
Thailand	Asia-Pacific	299	26	8.70%
Taiwan	Asia-Pacific	312	57	18.27%
Australia	Asia-Pacific	406	51	12.56%
Argentina	Latin America	895	79	8.83%
Brazil	Latin America	1,004	116	11.55%
Mexico	Latin America	1,023	125	12.22%
14 Countries	Four Clusters	16,683	1661	9.96%

Our sample includes U.S. residents who are 18 years or older. Because respondents completed the survey on a Web site, most individuals had control or ownership of a desktop or laptop computer. The researcher believes that a Web-based collection method is appropriate given that the topic of identity management required subjects to have some level of technical sophistication.

To determine the extent of possible response bias resulting from Web versus on-Web survey collection methods, the researcher conducted a validation sample of 262 non-Web users in four countries (United States, United Kingdom, Japan and Argentina). Validation tests were conducted on five key survey items.³ The results, which did not reveal any statistically significant difference for all five survey items, are summarized in a later section of this paper.

All survey respondents were paid a nominal incentive for completing the survey within a pre-defined holdout period (approximately \$5 dollars or the equivalent). All responses were completed within a three week period.

³ The five Yes/No survey questions included in this test are as follows: (1) Would you consider a multi-purpose identity credential? (2) Would you permit an organization to use personal data collected for secondary purposes? (3) Would you consider using biometrics? (4) Do you think certain types of organizations require stronger forms of identity verification? (5) Are you aware that nations around the world are beginning to issue electronic, biometric-enabled passports?

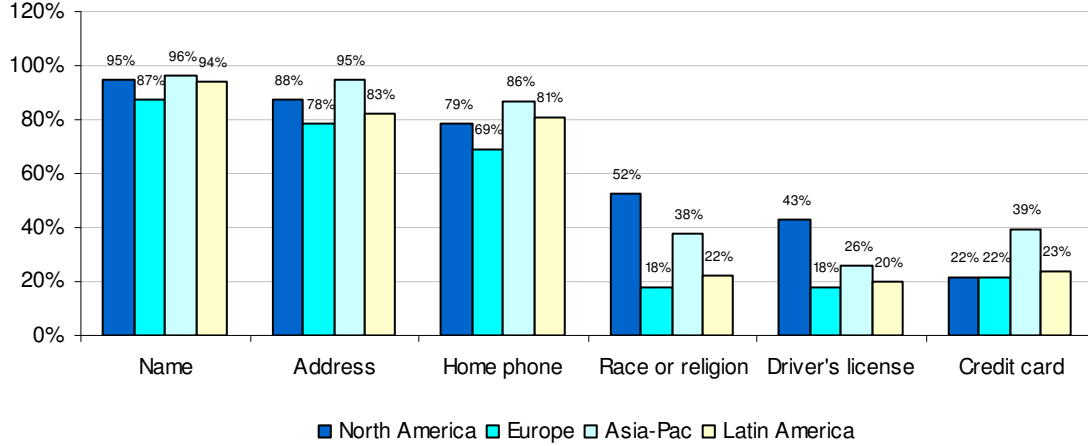
Detailed Findings

The detailed findings are reported for four geographic regions – North America (NA), Europe (EU), Asia-Pacific (AP) and Latin America (LA). The actual survey frequencies and percentage frequencies are reported in tabular format. The abbreviation “Pct%” means that the tabled percentages sums to the sample total. And, “Tot%” means that the table percentages sum to the response sample total (which is greater than the sample total if the question requested more than one response). The first set of analyses focuses on personal data elements that respondents in different regions are willing to share with business (Table 2) and government (Table 3).

Table 2 What information are you willing to share about yourself with a business organization such as a bank, airline, telephone company, retailer and others to help the organization verify your identity?	NA	EU	AP	LA	Overall	Tot%
	464	427	450	320	1661	
Other phone number	72%	24%	56%	30%	784	47%
Mother's maiden name	73%	35%	35%	28%	732	44%
SSN or Country ID	42%	11%	53%	37%	598	36%
Date of birth	65%	27%	48%	58%	817	49%
Credit card or debit card number	52%	18%	38%	22%	562	34%
E-mail address	78%	57%	71%	46%	1072	65%
Nationality	50%	41%	63%	36%	804	48%
Driver's license number	43%	18%	26%	20%	456	27%
Digital signature	47%	31%	46%	29%	655	39%
Digital photo	54%	46%	61%	41%	852	51%
Race or religion	22%	22%	39%	23%	444	27%
Home phone number	79%	69%	86%	81%	1307	79%
Finger or thumbprint	41%	38%	50%	32%	676	41%
Home address	88%	78%	95%	83%	1431	86%
Name	95%	87%	96%	94%	1548	93%
None of the above	5%	10%	3%	4%	94	6%
Avg data elements to be shared	9.00	6.05	8.61	6.58	7.71	48%

Bar Chart 1 shows that most respondents are willing to share name, address and home phone with a trusted business organization for purposes of identity verification. The least popular data elements include credit card, driver's license and race or religion.

Bar Chart I: Top and bottom three data elements respondents are willing to share with a trusted business organization to prove identity



	NA	EU	AP	LA	Overall	Tot%
	464	427	450	320	1661	
Finger or thumbprint	56%	31%	71%	13%	751	45%
Other phone number	76%	28%	62%	23%	827	50%
SSN or Country ID	51%	71%	85%	33%	1026	62%
E-mail address	67%	26%	40%	16%	655	39%
Digital photo	47%	29%	60%	12%	649	39%
Digital signature	47%	15%	51%	20%	574	35%
Driver's license number	56%	58%	51%	19%	801	48%
Mother's maiden name	68%	33%	43%	32%	753	45%
Nationality	60%	74%	96%	64%	1229	74%
Race or religion	28%	27%	50%	14%	513	31%
Date of birth	63%	40%	67%	60%	958	58%
Home phone number	85%	72%	86%	63%	1293	78%
Credit card or debit card number	32%	14%	16%	6%	300	18%
Home address	91%	83%	98%	85%	1493	90%
Name	93%	88%	99%	93%	1549	93%
None of the above	7%	10%	1%	3%	93	6%
Avg data elements to be shared	9.21	6.93	9.70	5.51	8.09	51%

Bar Chart 2 shows that most respondents are willing to share name, address and home phone with a governmental organization for purposes of identity verification. The least popular data elements include credit card, race or religion and digital signature.

Bar Chart 2: Top and bottom three data elements respondents are willing to share with a governmental organization to prove identity

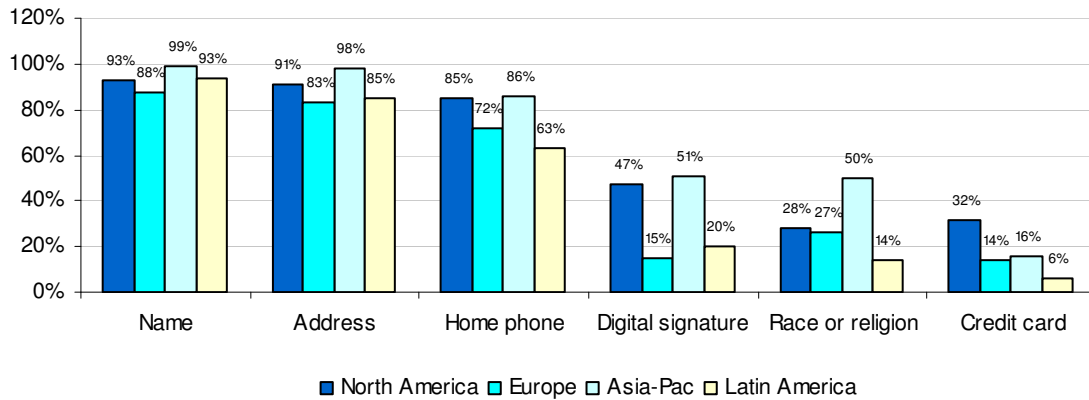
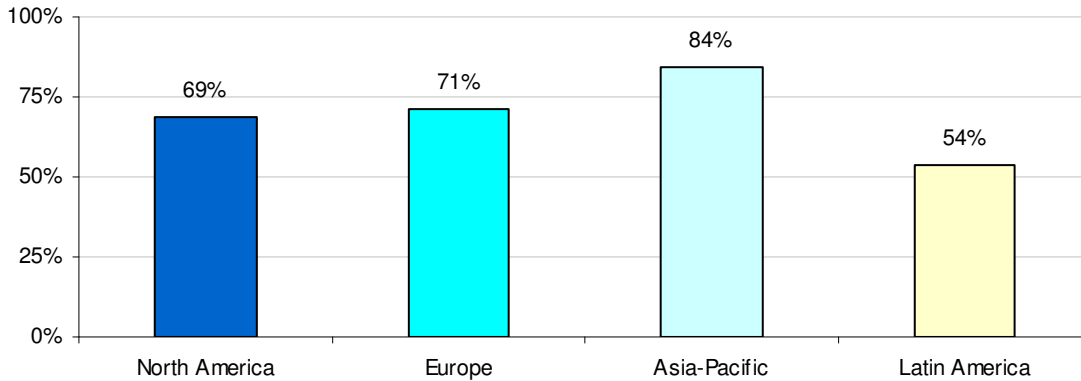


Table 3 reports the frequency of respondents who would consider a multi-purpose identity credential (see definition in footnote 1).

	NA	EU	AP	LA	Overall	Pct%
Yes	69%	71%	84%	54%	1173	71%
No	31%	29%	16%	46%	488	29%
Total	464	427	450	320	1661	100%

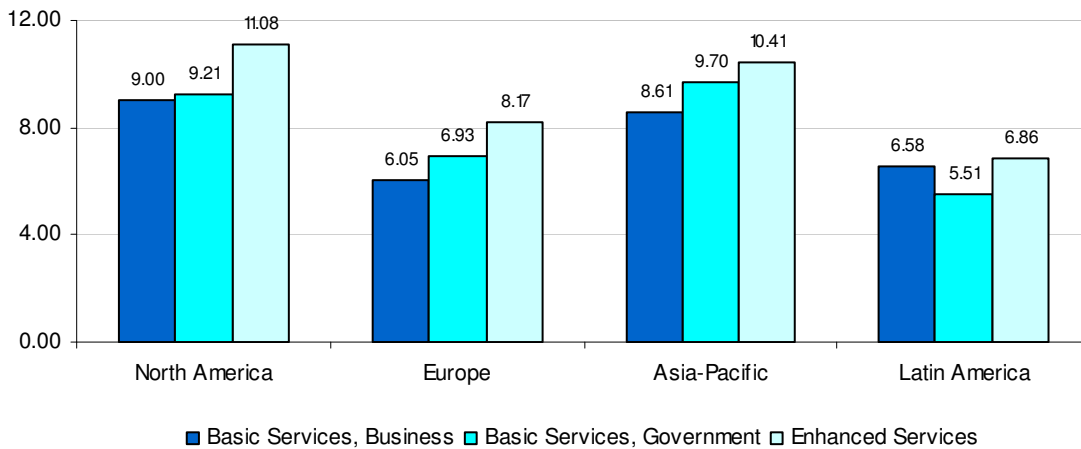
Bar Chart 3 shows that a majority of respondents in all four regions would elect to have an identity credential that can be used by many organizations for multiple functions. The chart also reveals that respondents in Asia-Pacific are most receptive, while those in Latin America are least receptive, to this proposal.

Bar Chart 3: Percentage of respondents in four global regions who would consider having a multi-purpose identity credential



Bar Chart 4 reports the average frequency of personal data elements that respondents will share with business and government (for basic identity verification purposes) and for enhanced identity services (as provided by a multi-purpose identity credential). Results clearly show that individuals in all four regions are willing to provide more pieces of personal data to obtain enhanced identity services. Results also show that people in North America, Europe, and Asia-Pacific are willing to share more personal data with government than business organizations. In contrast, respondents in Latin America will share more with business than government.

Bar Chart 4: Average pieces of personal data shared with business, government and for enhanced services across four global regions



What identity functions do respondents want the most? Table 4 reports that respondents view access to transportation, public locations and international travel (customs) as the most desirable features of a multi-purpose identity credential. According to respondents, the least important features are access to cellular telephones and the workplace (place of employment).

Table 4 Please check the functions that you would like this multi-purpose identity credential to provide access to:	NA	EU	AP	LA	Overall	Tot%
	318	303	379	173	1173	
Transportation channels such as planes, trains and buses	84%	89%	89%	86%	1023	87%
Secure public locations such as stadiums, transit stations or schools	81%	80%	82%	80%	949	81%
Travel to another country	61%	80%	81%	82%	881	75%
Internet customer accounts	92%	65%	65%	66%	852	73%
Your patient health records	51%	67%	71%	62%	741	63%
Your home computer	82%	56%	50%	62%	727	62%
Bank accounts	69%	53%	56%	55%	689	59%
Electronic payments against credit card, debit card or bank accounts	81%	36%	37%	41%	578	49%
Private government records such as tax or real estate information	56%	34%	36%	34%	475	40%
Your home	41%	25%	26%	86%	451	38%
Your automobile	40%	30%	27%	25%	364	31%
Your PDA	52%	22%	22%	20%	350	30%
Office or place of employment	34%	27%	28%	28%	345	29%
Your wireless telephone	45%	20%	21%	28%	332	28%

Bar Chart 5 shows six identity functions by geographic region. Respondents in North America appear to be more receptive to having one credential that accesses the Internet, personal computers and bank accounts than individuals in the other three regions. In contrast, North Americans appear to be less receptive to having a multi-purpose identity credential that provides access to health records or serves as a passport (crossing borders) than respondents in Europe, Asia-Pacific and Latin America.

Bar Chart 5: How should the multi-purpose identity credential be used?

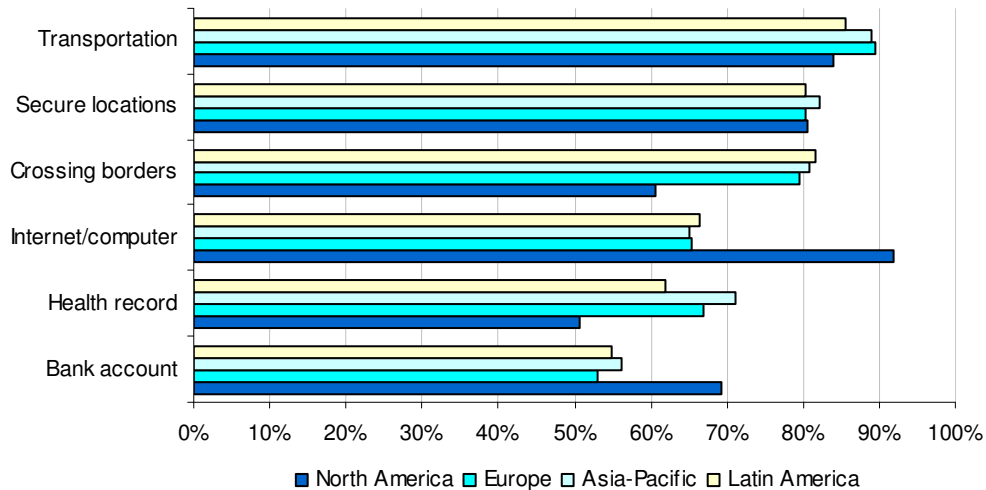


Table 5 reports the reasons why respondents think that a multi-purpose identity credential is a good idea. The top reasons are efficiency and convenience.

Table 5 What are your primary reasons why respondents are willing to consider a multi-purpose identity credential?	NA	EU	AP	LA	Overall	Tot%
	318	303	379	173	1173	
It would speed up the identity verification process.	85%	91%	92%	83%	1037	88%
Convenience, I won't have to remember separate logins, PINs or passwords.	94%	77%	92%	68%	999	85%
My information would be more secure.	75%	74%	90%	79%	939	80%
It would protect my privacy.	55%	44%	52%	51%	593	51%
I like to adopt new technology early.	24%	20%	62%	31%	426	36%

Table 6 reports the devices that respondents most prefer to manage their multi-purpose identity credential.

Table 6 Please select the one device from the list below that you most prefer to manage your multi-purpose identity credential.	NA	EU	AP	LA	Overall	Pct%
	317	303	379	173	1172	
An ID card that I carry.	33%	45%	21%	36%	384	33%
A biometric system such as my finger prints and facial scan.	26%	21%	23%	20%	270	23%
A secure chip in my cellular phone.	18%	11%	17%	25%	200	17%
A secure chip in my PDA or laptop computer.	12%	11%	11%	9%	126	11%
A secure chip on an article of clothing or jewelry	11%	12%	17%	9%	149	13%
A chip implanted in my body.	1%	1%	10%	1%	43	4%
Total	317	303	379	173	1172	100%

Bar Chart 6 reports that most respondents prefer having the credential in the form of an ID card. However, many respondents are interested in biometrics or having the credential embedded in a cellular phone. Very few respondents prefer the idea of having an identity chip implanted in their body. However, over 10% of individuals in the Asia-Pacific region see this proposal as the best option available.

Bar Chart 6: Devices preferred to manage the multi-purpose identity credential

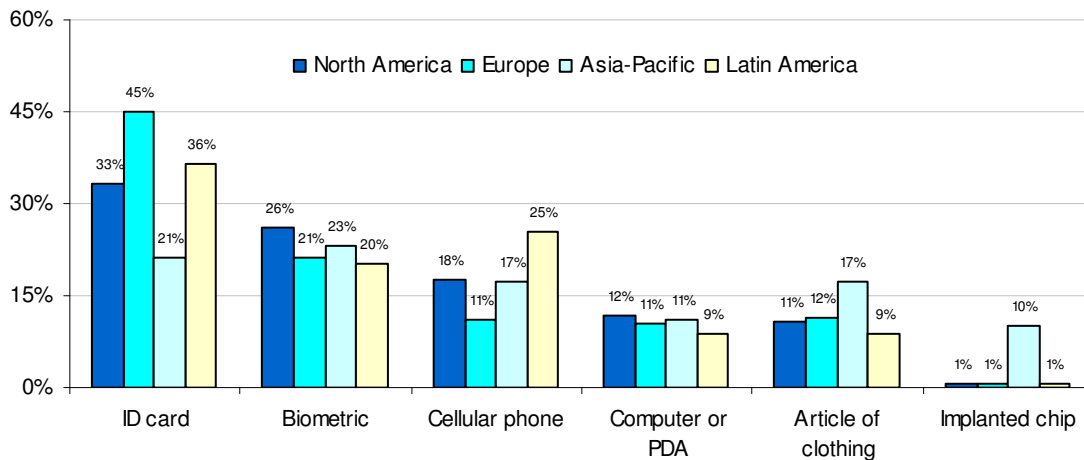


Table 7 reports the organizations that respondents believe are most trusted to issue and manage a multi-purpose identity credential. Banking institutions and a dedicated agency of the government are the two most preferred solutions. While North Americans view the postal service as the most preferred organization for issuing and managing an identity credential, this opinion is not shared by respondents in other regions of the world.

Table 7 Organizations most trusted to issue a multi-purpose identity credential.	NA	EU	AP	LA	Overall	Tot%
	318	303	379	173	1173	
Banking institution	46%	44%	50%	42%	539	46%
Governmental agency established to issue identity card	39%	56%	50%	27%	528	45%
Law enforcement (police)	7%	39%	41%	34%	357	30%
Private company established to issue identity card	29%	24%	35%	24%	338	29%
Transportation providers	39%	21%	13%	5%	247	21%
Postal services	47%	12%	10%	13%	245	21%
Telephone or wireless company	19%	17%	26%	17%	241	21%
Internet service provider (ISP)	17%	22%	25%	12%	237	20%
National tax authority	21%	12%	10%	3%	148	13%
None of the above	6%	10%	17%	10%	132	11%
Any local government organization	7%	11%	11%	6%	108	9%
Health care provider	4%	8%	10%	4%	84	7%
Educational institution	7%	2%	3%	0%	43	4%

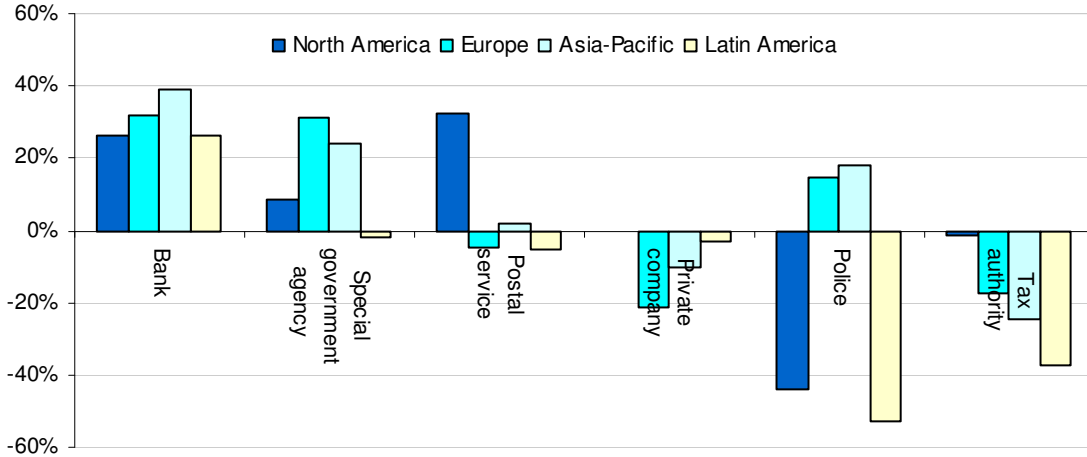
Table 8 reports the organizations that respondents believe are least trusted to issue and manage a multi-purpose identity credential. Law enforcement or police organizations are least trusted, followed by the creation of a private company dedicated to identity management.

Table 8 Organizations least trusted to issue a multi-purpose identity credential.	NA	EU	AP	LA	Overall	Tot%
	318	303	379	173	1173	
Law enforcement (police)	51%	24%	23%	87%	474	40%
Private company established to issue identity card	29%	45%	45%	27%	447	38%
National tax authority (IRS)	23%	30%	35%	40%	365	31%
Governmental agency established to issue identity card	30%	25%	26%	28%	318	27%
Transportation providers	30%	21%	23%	11%	265	23%
Telephone or wireless company	17%	22%	23%	20%	242	21%
Internet service provider (ISP)	20%	22%	25%	5%	234	20%
Any local government organization	33%	10%	8%	13%	190	16%
Banking institution	20%	12%	11%	16%	167	14%
Postal services (USPS)	15%	17%	8%	18%	159	14%
Health care provider	8%	7%	6%	5%	81	7%
Educational institution	5%	4%	6%	1%	50	4%
None of the above	3%	2%	2%	1%	28	2%

Bar Chart 7 shows the net differences calculated as the difference between positive and negative ratings. The results clearly show that respondents from all four regions view banks as most trusted for manage identity credentials. Least trusted are tax authorities and police.

Bar Chart 7 What organizations are trusted to issue identity credentials?

Net differences between "Most Trusted" and "Least Trusted" survey ratings



It is interesting to see that North Americans and Latin Americans have a net negative reaction to the idea of having the police or law enforcement as the primary issuers of a multi-purpose identity credential. On the other hand, respondents in Europe and Asia-Pacific have a net favorable view of police or law enforcement as issuers of an identity credential.

Table 9 reports that over 68% of respondents believe that the identity credential needs to operate in different countries. This interoperability criterion appears to be important to individuals in all four regions.

	NA	EU	AP	LA	Overall	Pct%
Very important	15%	31%	27%	14%	271	23%
Important	44%	41%	47%	49%	527	45%
Not important	29%	21%	20%	26%	276	24%
Irrelevant	13%	6%	6%	11%	99	8%
Total	318	303	379	173	1173	100%

Bar Chart 8 shows that the relative importance of this “cross-border” feature appears to by region. As can be seen, global interoperability is most important for respondents in Europe (Very Important = 31%) and Asia-Pacific (Very Important = 27%).

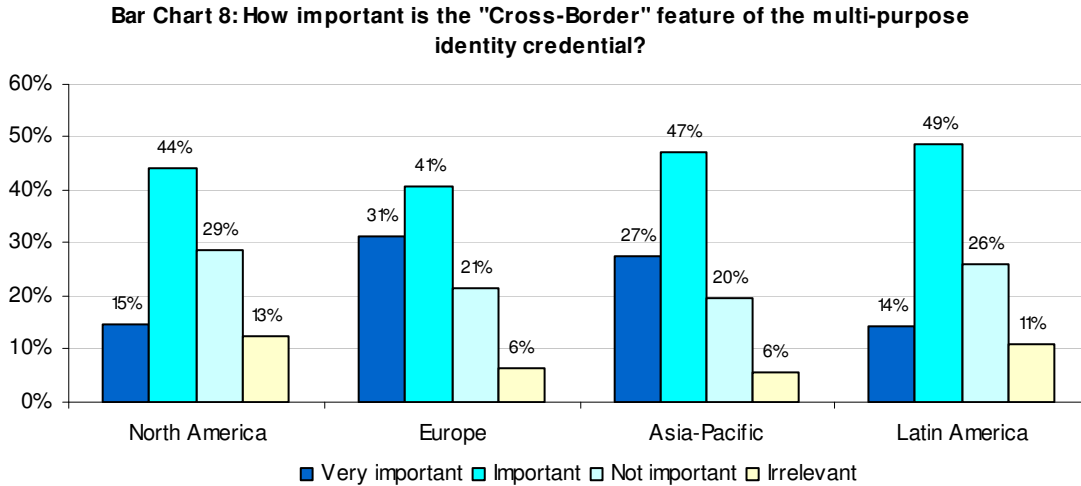


Table 10 reports results for a subset of respondents who stated that they were not interested in a multi-purpose identity credential. These respondents are most concerned about security and privacy risks associated with having one centralized credential, including identity theft or other related crimes.

Table 10 Why would you not consider having a multi-purpose identity credential?	NA	EU	AP	LA	Overall	Tot%
	146	124	71	147	488	
I don't like the idea of having my identity in one ID card or device.	84%	72%	56%	73%	360	74%
The multi-purpose card might get lost or stolen.	65%	88%	68%	56%	334	68%
I am suspicious of how the ID card would work.	49%	49%	41%	65%	257	53%
I am fearful of this information could be accessed by criminals.	39%	33%	48%	38%	188	39%
I like the old ways best.	34%	35%	56%	33%	181	37%
I would prefer to provide identification information for each relationship separately.	26%	35%	20%	16%	120	25%

Table 11 reports how respondents feel about organizations using their personal information (initially provided for identity verification) for secondary purposes such as marketing or promotions to them.

A majority of respondents in all geographic regions say “never” or “only if they can choose” the recipient of their personal data. In other words, results suggest organizations collecting information for identity management purposes need to be careful not to use or share this type of information without first obtaining consent from the data subject.

Table 11 Would you permit an organization to use the personal information it collects to verify your identity for other purposes, such as promoting products and services to you?	NA	EU	AP	LA	Overall	Tot%
Yes	26%	14%	30%	23%	385	23%
Only if I can choose	28%	26%	40%	27%	508	31%
Never	47%	60%	30%	50%	768	46%
Total	464	427	450	320	1661	100%

Table 12 reports how respondents feel about biometrics for identity verification purposes.

Table 12 Is it acceptable for a trusted organization such as your bank, credit card company, health care provider or governmental organization to use biometrics such as your voice or fingerprints to verify your identity?	NA	EU	AP	LA	Overall	Pct%
Yes	71%	69%	68%	58%	1114	67%
No	10%	16%	18%	29%	288	17%
Unsure	19%	15%	14%	13%	259	16%
Total	464	427	450	320	1661	100%

Bar Chart 9 shows that respondents in all four regions of the world are very positively oriented toward the use of biometrics. The most positive results are for respondents in North America (71%), and the least positive results are respondents in Latin America (58%).

Bar Chart 9: Will you consider using biometrics to prove your identity?

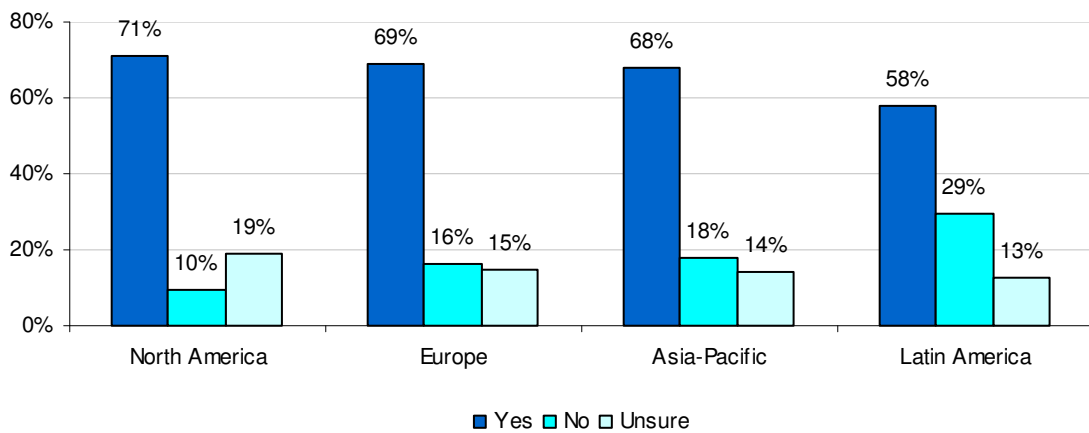


Table 13 reports that reason why the respondent would consider using biometrics to prove their identity. Similar to results for multi-purpose identity credentials, the two top reasons are convenience and efficiency.

Table 13 What are your primary reasons why you would consider using biometrics?	NA	EU	AP	LA	Overall	Tot%
	330	294	305	185	1114	
Convenience, because I won't have to remember separate logins, PINs or passwords.	92%	68%	92%	71%	914	82%
It would speed up the identity verification process.	69%	85%	70%	84%	847	76%
My information would be more secure.	61%	57%	51%	50%	617	55%
It would protect my privacy.	52%	41%	38%	41%	481	43%

What biometric methods are most accepted by respondents? Table 14 shows that voice recognition and fingerprints are most preferred. Eye (iris) scan is least accepted for respondents.

Table 14 What type of biometric authentication method would be most acceptable to you?	NA	EU	AP	LA	Overall	Pct%
Voice recognition	36%	25%	31%	38%	356	32%
Fingerprints	32%	25%	25%	24%	298	27%
Facial scan	10%	27%	23%	20%	218	20%
Hand geometry	16%	13%	9%	9%	133	12%
Eye (iris) scan	7%	10%	13%	10%	109	10%
Total	330	294	306	184	1114	100%

Bar Chart 10 shows that North Americans are more negatively disposed to facial scans than respondents in other regions (especially Europeans). Voice recognition appears to be the most favorable form of biometrics for respondents in all regions.

Bar Chart 10: Repondents' preference for biometric methods

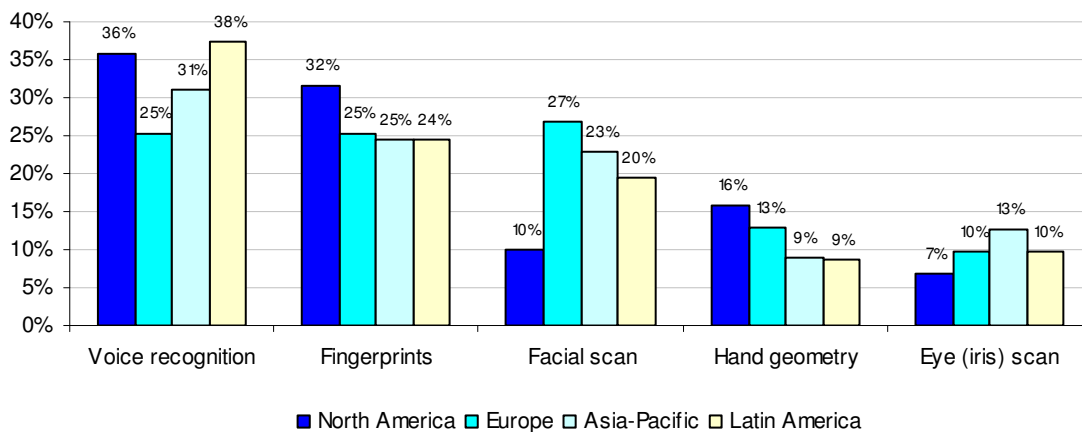


Table 15 reports results for a subset of respondents who stated that they were not interested in using biometrics. These respondents are suspicious of how this technology works.

Table 15 Why would you not consider using biometrics?	NA	EU	AP	LA	Overall	Tot%
	134	133	145	135	547	
I am suspicious about how biometrics work.	73%	72%	74%	76%	404	74%
I prefer providing non-biometric identification information.	60%	58%	68%	60%	337	62%
I do not believe biometrics accurately identifies me.	37%	39%	30%	37%	195	36%
I am fearful of this information being accessed and abused by external parties.	34%	32%	31%	33%	176	32%

Table 16 provides validation to the above results. Respondents clearly prefer using biometrics in banking and other financial service applications as a way to reduce incidents of fraud such as identity theft.

Table 16 Which of the following methods, if any, do you think would be a good idea for organizations such as a bank or other financial service companies to use for combating fraud and identity fraud?	NA	EU	AP	LA	Overall	Tot%
	464	427	450	320	1661	
Biometrics	61%	69%	70%	64%	1099	66%
Smart card reader	45%	46%	47%	46%	764	46%
Security tokens	44%	40%	43%	40%	696	42%
More passwords or PIN numbers	16%	14%	13%	16%	245	15%
Other	7%	3%	16%	3%	128	8%

Do respondents expect different types of organizations to have stronger identity verification methods in-place to protect them. Results in Table 17 show that 89% says "yes" to this question.

Table 17 Do you expect certain types of organizations or entities to have stronger identity verification methods and safeguards in place?	NA	EU	AP	LA	Overall	Pct%
Yes	86%	92%	92%	86%	1477	89%
No	14%	8%	8%	14%	184	11%
Total	464	427	450	320	1661	100%

What types of organizations do respondents view as requiring the strongest identity management methods? Table 18 reports the top ten organizations. These respondents see banks, law enforcement, credit card companies and airlines as needing the most rigorous identity management methods.

Table 18 Top ten organizations or entities that should have strong identity verification and authentication safeguards	NA	EU	AP	LA	Overall	Tot%
	399	392	412	274	1477	
Banks	91%	87%	91%	91%	1327	90%
Law Enforcement	92%	89%	93%	59%	1261	85%
Credit Card Companies	86%	76%	84%	89%	1232	83%
Airlines	88%	83%	87%	61%	1205	82%
Hospitals & Clinics	83%	57%	86%	81%	1129	76%
Railways or Bus Lines	74%	73%	74%	76%	1096	74%
Courts & Public Records	75%	71%	74%	77%	1093	74%
Drug Stores (Druggist)	70%	45%	68%	73%	938	64%
Internet Service Providers	59%	47%	60%	59%	827	56%
Government Agencies	54%	59%	57%	52%	823	56%

Tables 19 and 20 provide ratings from respondents on different types of organizations that they believe are doing a good job or poor job in verifying identity today. Only the top and bottom ten of each organizational list is reported.

Table 19 shows that banks, hospitals and clinics, courts and public records, and credit card companies are doing a reasonably good job in identity verification or providing authentication.

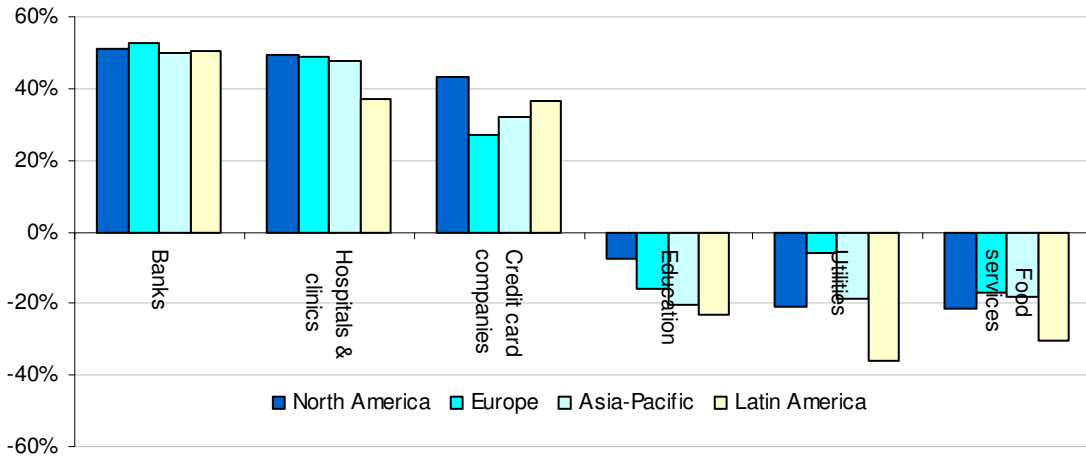
Table 19 What organizations are doing a Good job verifying identity? Top ten list.	NA	EU	AP	LA	Overall	Tot%
	399	392	412	274	1477	
Banks	85%	81%	78%	80%	1198	72%
Hospitals & Clinics	79%	70%	70%	65%	1056	64%
Courts & Public Records	72%	66%	62%	65%	980	59%
Credit Card Companies	75%	63%	61%	65%	976	59%
Law Enforcement	58%	63%	62%	63%	907	55%
Drug Stores (Druggist)	65%	54%	52%	53%	829	50%
Government Agencies	59%	48%	49%	44%	747	45%
Airlines	50%	50%	46%	50%	721	43%
Internet Service Providers	57%	41%	43%	43%	680	41%
Web Retailers	47%	42%	44%	45%	658	40%

Table 20 shows that hotels, schools and universities, telephone and wireless providers, and Web retailers are perceived by respondents as not doing an adequate job in identity verification.

Table 20 What organizations are doing a Poor job verifying identity? Bottom ten list.	NA	EU	AP	LA	Overall	Tot%
	399	392	412	274	1477	
Hotels	60%	44%	42%	61%	752	45%
Schools & Universities	50%	45%	48%	53%	721	43%
Telephone & Wireless	53%	31%	39%	50%	629	38%
Web Retailers	39%	36%	40%	42%	576	35%
Cable Companies	55%	15%	33%	56%	569	34%
Retail Stores	41%	28%	32%	43%	526	32%
Internet Service Providers	29%	39%	39%	31%	514	31%
Catalogue Merchants	33%	34%	34%	35%	502	30%
Railways or Bus Lines	47%	19%	27%	45%	496	30%
Public Utilities	35%	30%	34%	33%	491	30%

Bar Chart 11 shows the net differences calculated as the difference between positive and negative ratings from the above lists.

Bar Chart 11: How respondents view the identity practices of different organizations that they regularly interact with
 Net different between "Best" and "Worst" survey ratings



The above results clearly show that respondents from all four regions view banks and health care providers (hospitals and clinics) as doing the best job in terms of managing identity. With respect to these net differences, respondents view food services (such as grocery stores), utilities and educational institutions as least effective in managing their identity.

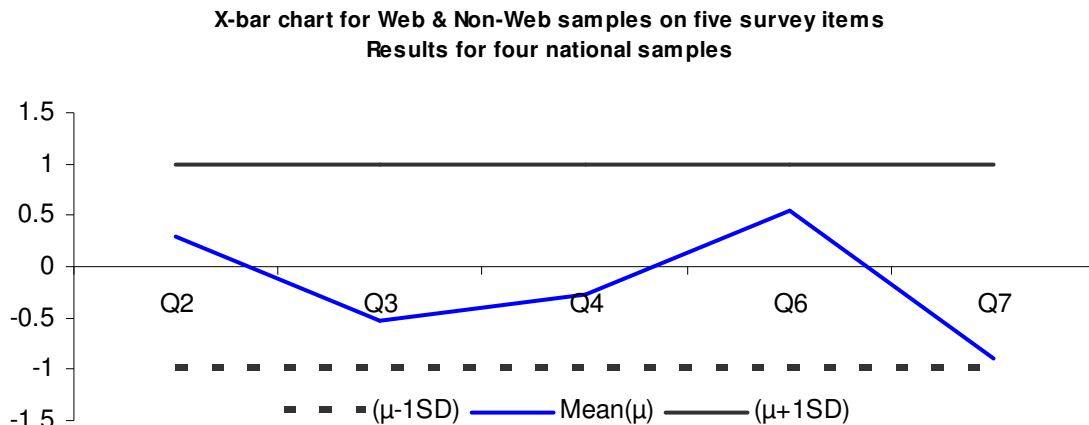
Validation of Web to Non-Web results

As noted before, we attempted to validate the Web-based survey findings to non-Web respondents. To do this validation test, we conducted four separate samples in the United States, United Kingdom, Japan and Argentina (totaling 262 adult-aged respondents). These respondents were drawn from an entirely new sampling frame based only on telephone or physical location.

Contact was made by telephone. We asked these individuals to provide responses to five survey questions (Q2, Q3, Q4, Q6 and Q7) incorporated within our original instrument. The five test questions are as follows:

- ✓ Q2: Would you consider having a single multi-purpose identity credential that will be accepted by many organizations to verify who you are before providing access to secure records or locations?
- ✓ Q3: Would you permit an organization to use the personal information it collects to verify your identity for other purposes, such as promoting products and services to you?
- ✓ Q4: Is it acceptable for a trusted organization such as your bank, credit card company, health care provider or governmental organization to use biometrics such as your voice or fingerprints to verify your identity?
- ✓ Q6: Do you expect certain types of organizations or entities to have stronger identity verification methods and safeguards in place?
- ✓ Q7: Are you aware of the fact that nations around the world are beginning to issue electronic, biometric-enabled passports?

We analyzed average responses against results from the Web-based survey. The X-bar chart below reveals that average responses from the non-Web sample (n=262) falls between the ± 1 normalized standard deviation for all five survey questions. This suggests that our Web-based findings are not significantly different from the non-Web sample.



What Did We Learn from the Open-ended Survey Question?

In total, 608 (37%) of the study's respondents responded to the survey's last item – which was an open-ended question that permitted up to 500 characters. Individuals from Asian countries were the least likely to utilize this optional contextual field. Respondents from Latin America and Europe were more likely to express additional views in this survey field.

Results support findings that people around the world are willing to share personal information to make the identity process work better and faster than current methods. Despite generally positive results, Europeans and Latin Americans appear concerned about sharing sensitive data elements – and especially those that capture information about family relatives, such as the data element “mother's maiden name.”

Many people in Europe, Asia-Pacific and Latin America did not know how to respond to the driver's license number as a personal identifier (on the survey), because they do not own or drive an automobile. Several Latin Americans and Europeans did not like the idea of using country ID for general identity verification because it could be abused by government.

Based on responses, the key to successful identity management is making it very convenient for the public to use. It appears that both convenience and efficiency issues are more important than individual privacy or safety concerns. Also, many people stated that privacy issues would likely be improved if the identity credential was not based solely on personal information – preferring biometrics or smart cards to data.

Privacy issues resulting from the collection of too much personal data or misused technologies such as location tracking systems was cited by several people as a serious threat to them and their families. Our results suggest that respondents in Europe and Latin America have much stronger opinions about diminished privacy rights, especially if the identity credential is controlled or managed by a central (national) government.

Most people throughout the world do not like the idea of police or law enforcement controlling the identity vetting and credentialing process. Many people fear “Big Brother” concerns as a result of governments using identity management systems to track the general population. Also, some people suggested that the identity credential should never become a mandatory process.

A surprising number of people place high levels of trust and confidence in their primary banking or financial services institution. People felt strongly that their bank is best equipped to issue and manage the identity credential. Despite strong positive feelings about banks, however, many people wanted the credential to be limited primarily to transportation or access to public places such as a stadium or airport (and not used for online banking or automated bill payments).

The multi-purpose identity credential was consistently praised by subjects throughout the world. A majority of subjects liked the idea of having one identity proof point rather than having to remember passwords or PIN numbers. However, many people did not want this credential to be part of their personal life such as opening doors to homes or to starting the ignition to their automobiles. In general, a large number of people expressed distain for passwords, primarily because they are required to remember too many today (or had bad experiences in having to reset them often). Many people felt biometrics or smart cards would be a good replacement for password-oriented access controls.

Some people felt that biometrics should be expanded beyond very limited uses today. They like the idea of having their credit card payments associated with biometric readers and cell phones. A few people in Europe mentioned that biometric payment systems are already being implemented such as in retail and grocery stores.

People felt strongly that implanted chips are a very scary proposition. Latin Americans and Europeans expressed serious privacy concerns, especially if chips were going to be used by central governments. In contrast, no one in the Asia expressed concerns about the use of an implanted chip. In fact, a few Asian respondents felt that such a device would be helpful and potentially convenient – especially for individuals who were elderly or handicapped.

Some people had strong concerns that the multi-purpose identity credential could evolve into a global ID registration program. Again, these concerns are based on the idea that global ID can create ethical and social problems for people if not controlled or managed well. Some individuals expressed real concern about the United Nations managing such a credentialing program.

Several Europeans and Latin Americans expressed concerns about the ID program being managed or manipulated by the United States. Similar to “Big Brother” concerns, some people expressed serious reservations if a large software or technology companies having control over the credentialing or vetting process.

Many people stated that in order to make identity management work and be accepted throughout the world, the issuer of the credential must have impeccable ethical standards and transparency (open standards). Some people believed that without controls over the “credential issuer” the public would be at great risk.

Demographics

Following are the results for remaining survey items including respondents' demographics.

Table 21 Please indicate the one attribute that best describes your position on adopting new technologies.	NA	EU	AP	LA	Overall	Pct%
I consider myself an early adopter.	24%	34%	28%	9%	409	25%
I consider myself middle of the pack.	59%	45%	47%	65%	888	53%
I consider myself a late adopter.	17%	21%	25%	26%	363	22%
Total	463	427	450	320	1660	100%

Table 22 How many credit cards do you own?	NA	EU	AP	LA	Overall	Pct%
Zero to one	20%	47%	50%	65%	723	44%
Two	27%	29%	37%	28%	508	31%
Three	24%	17%	7%	7%	238	14%
Four or more	28%	7%	6%	1%	190	11%
Total	462	427	450	320	1659	100%

Table 23 Do you own a cellular phone	NA	EU	AP	LA	Overall	Pct%
Yes	90%	94%	90%	84%	1493	90%
No	10%	6%	10%	16%	164	10%
Total	462	425	450	320	1657	100%

Table 24 How many hours each week do you spend using the Web or doing email?	NA	EU	AP	LA	Overall	Pct%
1 hour or less	12%	11%	9%	16%	192	12%
1-2 hours	11%	13%	10%	22%	217	13%
2-5 hours	13%	16%	15%	15%	243	15%
5-10 hours	22%	16%	16%	21%	306	18%
10-20 hours	22%	19%	21%	16%	330	20%
More than 20 hours	21%	25%	29%	11%	367	22%
Total	460	425	450	320	1655	100%

Table 26 Approximately, when did you start using the Internet or start doing email?	NA	EU	AP	LA	Overall	Pct%
In 2006	1%	0%	0%	1%	12	1%
In 2005	10%	7%	6%	13%	147	9%
In 2004	9%	13%	14%	11%	193	12%
In 2003	7%	12%	14%	16%	194	12%
In 2002	29%	27%	22%	18%	405	24%
In 2001	27%	27%	22%	31%	438	26%
In 2000 or earlier	17%	14%	22%	9%	263	16%
Total	459	423	450	320	1652	100%

Table 27 What is your highest level of education attained?	NA	EU	AP	LA	Overall	Pct%
High School (or Equivalent)	29%	38%	38%	33%	571	35%
Vocational	19%	26%	28%	29%	414	25%
University	38%	24%	26%	26%	475	29%
Post Graduate	11%	10%	8%	11%	165	10%
Doctorate	3%	2%	0%	1%	23	1%
Total	457	421	450	320	1652	100%

Table 28 Please check your age range?	NA	EU	AP	LA	Overall	Pct%
18 to 25	20%	21%	23%	23%	354	21%
26 to 35	20%	23%	22%	25%	363	22%
36 to 45	23%	24%	29%	28%	424	26%
46 to 55	14%	13%	12%	15%	218	13%
56 to 65	12%	9%	9%	5%	151	9%
66 to 75	7%	6%	5%	5%	95	6%
75+	5%	4%	1%	0%	42	3%
Total	455	422	450	320	1652	100%

Table 29 Approximately, what is your household income (approximate conversion from Euros€ or other national currencies to US\$)?	NA	EU	AP	LA	Overall	Pct%
Less than \$20,000	14%	18%	25%	54%	424	26%
\$20,000 to \$40,000	18%	22%	26%	22%	359	22%
\$41,000 to \$60,000	22%	18%	17%	10%	283	17%
\$61,000 to \$80,000	15%	14%	10%	8%	194	12%
\$81,000 to \$100,000	12%	13%	8%	4%	157	10%
\$101,000 to \$150,000	8%	7%	7%	1%	97	6%
\$151,000 to \$200,000	8%	7%	6%	1%	100	6%
\$201,000+	2%	1%	1%	0%	21	1%
Total	450	415	450	320	1635	100%

Table 30 Do you travel to other countries?	NA	EU	AP	LA	Overall	Pct%
Frequently	19%	57%	49%	40%	678	41%
Sometimes	33%	35%	43%	53%	662	40%
Never	49%	8%	7%	7%	310	19%
Total	456	424	450	320	1650	100%

Table 31 Please check:	NA	EU	AP	LA	Overall	Pct%
Female	51%	49%	47%	48%	809	49%
Male	49%	51%	53%	52%	845	51%
Total	457	427	450	320	1654	100%

Caveats to this Survey

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

- **Non-Response Bias:** The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests (see footnote 2), it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- **Sampling-Frame Bias:** Because sampling frames in different countries were derived from purchased lists, the quality of results is influenced by the accuracy of contact information and the degree to which the list is representative of individuals who are informed about current events. We also acknowledge that the results may be biased by media coverage at the time of the study.

Compensation was provided to ensure that respondents completed the survey task in a two day holdout period. While compensation was held to a nominal amount, we acknowledge potential bias caused by compensating subjects to complete this research within a short holdout period. Finally, since we used a Web-based collection method, it is possible that non-Web responses (form survey or telephone) would result in a different pattern of findings. The validation exercise mitigates this potential problem.

- **Self-Reported Results:** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote from or reuse this report), please contact by letter, phone call or email:

Ponemon Institute, LLC
Attn: Research Department
212 River Street
Post Office Box 601
Elk Rapids, Michigan 49629
1.800.887.3118
research@ponemon.org

Ponemon Institute, LLC **Advancing Responsible Information Management**

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

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