



Final Report

Volume I: Findings and Recommendations

ANSI-BBB Identity Theft Prevention and
Identity Management Standards Panel

January 31, 2008



**IDENTITY THEFT PREVENTION AND IDENTITY MANAGEMENT
STANDARDS PANEL (IDSP)**

FINAL REPORT – VOLUME I: FINDINGS AND RECOMMENDATIONS

Sponsoring Organizations

American National Standards Institute

Better Business Bureau

Report publication date

31 January 2008

More information

www.ansi.org/idsp

ANSI

25 West 43rd Street – Fourth Floor

New York, NY 10036

T: 212.642.8921

F: 212.840.2298

E: jmccabe@ansi.org

BBB

4200 Wilson Blvd, Suite 800

Arlington, VA 22203

T: 703-247-9358

F: 703-525-8277

E: smunn@council.bbb.org

TABLE OF CONTENTS*

Part / Title

1. Report Summary	1
2. Introduction	21
3. Target Audience for this Report	21
4. Background / Panel Objectives	22
5. Scope of Work / Coordination with Other Initiatives	23
6. Methodology	24
7. Participation and Funding	27
8. Findings and Recommendations (Preamble)	30
9. Working Group 1 -- Issuance of identity documents	
A. Foundational creation – issuance of birth certificates and Social Security cards	31
B. Subsequent credentials – issuance of driver’s licenses, ID cards and passports	35
C. Commercial issuance	44
D. Security of the issuance process	50
E. Credential security	55
10. Working Group 2 -- Exchange of identity data	
A. Fraudulent use of “perceived” secret information	60
B. Inadequate validation of credentials	66
C. Attacks on special populations	70
D. Security freezes	73
11. Working Group 3 -- Maintenance of identity data	
A. Intentional information systems breach	76
B. Mismanagement	83
C. Excessive data collection / retention / access	88
D. Security breach notification	91
E. Interface with the consumer / remediation	95
12. Acknowledgements	100

* This document is best utilized in electronic format as it contains embedded hyperlinks to additional information. **There are two-directional hyperlinks between the table of contents and the main section headers for ease of navigation.**

Annexes

Annex 1 – Panel Charter..... 104

Annex 2 – Process Flows and Narrative 105

Annex 3 – Standards Culled from the Inventory..... 109

Volume II (issued separately)

Standards Inventory

1. Report Summary

Introduction

Identity theft¹ has become one of the nation's most prominent marketplace issues in recent memory, and a large threat to commerce. That prompted the Better Business Bureau (BBB) and the American National Standards Institute (ANSI) to team up to create a new market-wide initiative that would help arm businesses and other organizations with the tools they need to combat ID theft and fraud and protect consumers – and themselves – from the risks associated with these crimes.

Launched on September 13, 2006, the Identity Theft Prevention and Identity Management Standards Panel (IDSP) was comprised of a diverse mix of private and public sector interests. The Panel charged itself with cataloguing existing standards, guidelines, best practices, and related compliance systems germane to this issue across all market sectors and industries, and publishing them as a “one stop shopping” resource, which currently does not exist. The Panel was also directed to identify where additional standards / guidelines work may need to be done by subsequent groups.²

The Panel set a timetable of 15 months to complete its work. This timetable was uniquely aggressive for the standards community, but was deemed critical, given the ever-changing landscape of identity theft and fraud. The Panel's work focused primarily on financial identity theft. Other types of fraud were also discussed (e.g., medical identity theft) and, while less time was spent on those, much of the analysis potentially can apply.

How this Report Will Advance Marketplace Interests

Businesses and other organizations will be able to map and measure their current identity theft prevention and identity management practices against the Panel's report and corresponding Standards Inventory. This represents a significant step forward in that it facilitates marketplace economies of scale. With a single resource cataloguing the spectrum of what currently exists, individual businesses no longer need to research

¹ For purposes of this report, identity theft is defined as the stealing or illicit use of someone else's identity credentials to commit fraud, for example, by opening new financial accounts, gaining access to existing accounts and loans, receiving health care services, etc.

² Annex 1 of this report is the Panel's charter. Modifying / rank ordering standards, or developing new standards, was outside the Panel's scope.

and track down existing standards, best practices and guidelines germane to this issue on their own. Ultimately, this will fortify the identity protection and identity management support systems for businesses, both individually, and across the marketplace as a whole...and the consumers they serve.

Government agencies and the private sector are presented with a checklist of recommendations to modify existing standards and practices to enhance identity theft protection.

Legislators will benefit from a timely report on current best practices and standardization / regulatory activities. This report, along with the Panel’s recommendations, can help to guide their legislative efforts and may pre-empt unnecessary lawmaking on issues where the private sector can effectively and innovatively lead with support from the public sector.

Consumers will be better served and protected as government, industry and the standards development community work more collaboratively to put into action the Panel’s recommendations.

For its part, the IDSP – with the continued support and input of issue stakeholders – will continue in its commitment to addressing these issues, and helping to facilitate forward movement on the recommendations outlined below.

Methodology

Three Working Groups – reflecting a “life-cycle” view of identity – were organized by the Panel’s Steering Committee as a work flow mechanism:

- **Working Group 1 - Issuance**: sought to identify and assess standards relating to the issuance of identity documents³ by government and commercial entities;
- **Working Group 2 - Exchange**: focused on standards pertaining to the acceptance and exchange of identity data;
- **Working Group 3 - Maintenance**: addressed standards relating to the ongoing maintenance and management of identity information.

³ For the sake of simplicity, various credentials that are commonly used to verify identity are referred to throughout this report as “identity documents.” It is recognized that these documents were in fact created for other purposes: a birth certificate to confirm a birth event as a public health record, a Social Security card to enroll in the Social Security program, a driver’s license to obtain driving privileges, and a passport to permit border crossings.

The first task of each Working Group was to compile an inventory of existing standards, guidelines, best practices and compliance systems related to identity theft prevention and identity management. Based on the discussions, the Panel's Standards Inventory ultimately grew to also include applicable laws, regulations, proposed legislation, white papers, and research studies and reports.⁴

Next, each Working Group identified and prioritized various identity fraud-related problems. They considered the range of possible solutions to these problems, not to define what the solutions should be, but to help ascertain whether there are standards or best practices that are relevant or potential gaps where no standards currently exist. New Account Processing was identified by each group as a pertinent risk scenario and two process flows were created relating to the acquisition of identity credentials and a typical new account establishment procedure.⁵

Finally, the Working Groups each performed a gap analysis against these process flows, overlaying the identified problems. From this emerged examples of existing laws, regulations, standards, guidelines, best practices, etc. that were seen as having particular relevance to the problem areas of concern.⁶ To the extent that potential gaps were identified, recommendations on the need for new or enhanced standards or best practices were formulated.

Participation in the Working Groups was open to all Panel members who elected to participate, and drew from a broad range of expertise. Some Panel members actively participated, while others did not. The Working Groups carried out their deliberations electronically and via conference calls, largely working independently of one another. At each phase of the process there were designated checkpoints, teleconferences and meetings where the Working Group leaders reported to the Steering Committee for purposes of coordination and to maintain forward progress. Plenary meetings of the full Panel were held in November 2006 and September 2007 to exchange information and help shape the Panel's report and recommendations, respectively. The Panel also endeavored to outreach to and coordinate with other organizations and initiatives addressing identity-related issues.

⁴ Volume II of this report, issued separately, is the comprehensive Standards Inventory resulting from this cataloguing exercise.

⁵ Annex 2 of this report presents these process flows and their accompanying narratives.

⁶ Annex 3 of this report contains these examples of "Standards Culled From the Inventory" mapped against the identified problems. They are also discussed where applicable in the main text of this report.

Findings and Recommendations

The findings and recommendations contained in this report were not formally voted on by the Panel. They represent the consensus⁷ views of the stakeholders actively participating in the Panel's Working Groups.

The collective findings and recommendations resulting from the Working Groups' gap analysis are summarized⁸ below under headings corresponding to the three Working Groups:

- A. The Issuance of Identity Credentials*
- B. The Exchange of Identity Data*
- C. The Maintenance of Identity Information*

There are a multitude of organizations and initiatives working on the issues raised in this report. Ultimately, these efforts should work toward greater convergence in terms of defining solutions.

A. The Issuance of Identity Credentials

Security of the Issuance Process⁹

A birth certificate establishes that a birth event occurred on a specific date, but there is no way to conclusively match an individual to the presented birth certificate to verify that it is the same person. If the authenticity of a birth certificate cannot be verified, then subsequently-issued documents that rely upon the birth certificate may not be accurate. These include the state-issued driver's license and identification card, the Social Security card, the passport, and the recently-introduced enhanced driver's license, which doubles in function as a travel document.

Given the circular nature of the issuance process -- wherein all of the issuers of the major documents use the others' credential to verify the identity of an applicant -- the issuance verification process needs to be fortified.

⁷ Consensus signifies substantial agreement but not necessarily unanimity.

⁸ Please refer to the indicated sections of the report for a fuller description of the identified problem(s) and discussion of issues, more examples of relevant existing standards, and further elaboration on potential gaps and recommendations.

⁹ See sections 9A, 9B and 9D of the report.

Additionally, the secure management of identifying information conveyed by an applicant is another part of the issuance process containing some gaps. Clever fraudsters can collude with employees at the point of issuance or can hack into online ID creation processes. Physical credentials delivered through the mail may not reach intended recipients and online credentials may be intercepted as they are being generated or transmitted. The existing spectrum of key standards and regulatory activities relating to Security of the Issuance Process issues are outlined in the Appendix to this Report Summary.

RECOMMENDATION #1:¹⁰ Enhance the Security of the Issuance Process

- **The National Center for Health Statistics (NCHS) and Social Security Administration (SSA) need to make it a priority to issue standards for birth certificates and Social Security cards, respectively, in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004.**¹¹ The development of standards is needed now and should not be held in further abeyance. The agencies should consult with industry and other stakeholders on the weaknesses associated with the current circular nature of the issuance process, as outlined above.
- **Government agencies that issue identity credentials need to improve communication and cooperation among themselves as well as between the government and the private sector. The National Association for Public Health Statistics & Information Systems (NAPHSIS) needs to continue the development and expansion to governmental agencies of the Electronic Verification of Vital Events (EVVE) system to authenticate credentials presented by applicants for service or benefits.** There currently is no mechanism for vital records offices to consistently and effectively communicate with state motor vehicle departments, the State Department's Passport Office, the Social Security Administration, banks, etc. on incidents of attempted fraud. Similarly, agencies that track birth certificate fraud do not have a mechanism to communicate back to the vital records offices. The challenges and debates surrounding The REAL ID Act notwithstanding, there needs to be improved communication and cooperation among credential-issuing agencies to enhance the overall integrity of issued credentials and to ensure that there is only one state drivers license / ID card issued per person.

¹⁰ Recommendations are numbered for ease of referencing only, not to suggest a hierarchy.

¹¹ This recommendation relates also to credential security, section 9E of the report.

- **Government and industry should expeditiously open a dialogue about the cross-application and implementation of existing security standards to identity issuance processes, and discuss the potential cross-functioning of new standards development, where deemed appropriate.** There are generally applicable information security management standards that may be useful reference documents for constructing stronger security programs for identity issuance processes. These include the ISO/IEC 27000 series of standards on information security and the North American Security Products Organization (NASPO) Security Assurance Standards for the Document and Product Security Industries (ANSI/NASPO Sav3.OP-2005). There are also sector-specific standards that may have cross-relevance to other sectors. Some examples of publicly available, comprehensive guides and standards that can serve as a reference model for new identity issuance security programs include the American Association of Motor Vehicle Administrators *DL/ID Security Framework*, the *HSPD-12 Personal Identity Verification Program*, and the *Australian National Smartcard Framework*.
- **Government and commercial issuers of identity credentials should give further attention to problems associated with secure delivery methods of such credentials to the end user.** One area that may require additional attention is the interface between the issuer and the recipient. In particular, further work may be needed on problems associated with secure delivery of credentials, both online and offline.

Commercial Issuance¹²

Identity thieves will employ various means at their disposal to fraudulently open new accounts. In some cases, *the private sector does not have access to government resources to detect, prevent and mitigate identity theft*. Some examples of standards, regulations and systems pertaining to Commercial Issuance issues are noted in the Appendix to this Report Summary.

RECOMMENDATION #2: Augment Private Sector Commercial Issuance Processes

- **Government and industry need to open a dialogue about how to facilitate greater interoperability between public and private sector ID theft prevention mechanisms, with the focus being on strengthening the integrity of the issuance process. This dialogue would include, among other things, providing the private sector appropriate and secure access to government vital record systems.** Three key factors determine the capability and sufficiency for

¹² See section 9C of the report.

identification documents to be truly interoperable across commercial and governmental organizations: physical characteristics, electronic data interchange and trust. The degree of interoperability between government solutions and private sector initiatives needs to be further explored and discussed by representatives of each sector. There are inherent tradeoffs between the needs of law enforcement and the private sector with respect to their use of personally identifiable information, the need to protect such data and personal privacy and the need for interoperability.

This Panel also believes the commercial online vetting process could potentially benefit from the use of the government vital record systems.

Credential Security¹³

ID credentials need to include features that deter alteration and facilitate the detection of fraud at points of inspection or transaction. ID credential authorities face the problem of limited budgets, often a lack of document security expertise and resources, wide security technology choices, no objective methods of measuring security technology effectiveness in advance of investing in it, and no way of objectively calculating return on investment. The spectrum of existing standards and guidance for Credential Security are outlined in the Appendix to this Report Summary.

RECOMMENDATION #3: Improve the Integrity of Identity Credentials

- **The Document Security Alliance (DSA) and North American Security Products Organization (NASPO) should proceed as soon as possible with their project to measure the Effectiveness of Document Security Technologies.** Although there is an abundance of document security technologies available to help prevent and detect ID credential fraud, *no standards exist to address the measurement of their effectiveness.* DSA and NASPO have jointly begun an effort in this area, and have just released a draft project plan for review within NASPO and the DSA.
- **The Department of Homeland Security (DHS) should work with issue stakeholders to develop Adversarial Testing Standards for identity credentials.** There are no published standards related to the critical need to perform adversarial testing of driver's license / ID credentials which may be required by DHS, as indicated in The REAL ID Act final regulations.¹⁴ DHS has indicated its

¹³ See section 9E of the report.

¹⁴ At the time this report was prepared, the final rule had been announced by DHS but had not yet been published in the *Federal Register*.

willingness to work with stakeholders to develop performance standards and a methodology for adversarial testing.

- **The North American Security Products Organization (NASPO), the Semiconductor Industries Association (SIA) and Semiconductor Equipment and Materials International (SEMI) in North America -- as well as CEN in Europe -- should expeditiously proceed with their standards work on Secure Serialization Anti-Counterfeiting Technology as a preventative countermeasure.** This Panel believes that the emerging Secure Serialization Technology looks very promising as a preventative countermeasure to ID credential fraud. An industry standard is in development in North America by NASPO, SIA and SEMI, and the European standards authority (CEN) has just launched a similar effort in response to European demand.

B. The Exchange of Identity Data

Authentication¹⁵

One common way organizations authenticate a person's identity is to see if they know a shared secret, such as a password or other types of personal information, such as a Social Security number. There are known weaknesses to this approach:

- Shared secrets and Social Security numbers have been hijacked by ID thieves, who then use them to commit fraud.
- Relying *only* on what a person knows (single factor authentication) makes the ID thief's job easier.

ID thieves have proven their ability to open new accounts using such means. Accordingly, this Panel sees a need for *stronger authentication practices*. Specifically, the Panel has identified a potential need to develop Best Practices for creditors to validate new account requests for consumers that have placed a fraud alert on their credit file -- in particular, those who have placed an *initial* fraud alert.

Another concern is that physical credentials can be faked by criminals and used to commit identity theft. *Real-time* validation of physical credentials at the issuing authority is needed to thwart ID thieves who exploit weaknesses in the processes for verifying identity.

In addition, specific populations have been known to face additional vulnerabilities to identity theft:

¹⁵ See sections 10A, 10B and 10C of the report.

- Children may become victims of identity theft when their parents or guardians create a fake identity using the child’s Social Security number. Companies currently have no means to verify the age of an individual and thus ensure they do not open accounts for minors.
- The elderly and the terminally ill may suffer fiduciary abuse at the hands of their caregivers or financial custodians.
- Fraud can also be committed when the identity of a deceased person is assumed by a perpetrator, if notification of death is delayed at the state level and not relayed to the Social Security Administration’s Death Master File.
- Active duty military also face special challenges in protecting themselves from identity theft.

Examples of relevant standards, laws, regulations and systems applicable to the Authentication issues raised are included in the Appendix to this Report Summary.

RECOMMENDATION #4: **Strengthen Best Practices for Authentication**

- **When determining an appropriate authentication procedure, financial institutions and other credit grantors should take into account level of risk, cost and convenience considerations.**

Best Practices for the use of various authentication options should depend on several considerations, including the type of application (opening a new account versus access to an existing account), interface type (in-person, online, or telephone), and level of risk. Cost and convenience should be proportional to risk: simplistic data matching for low valued transactions; more rigorous authentication procedures when the stakes are higher. New Account Openings should be considered high risk, as new account fraud typically is more difficult for victims to detect than fraud with existing accounts. New Account Opening fraud is also potentially more damaging, in that a new line of credit is extended, with a corresponding new record with the credit bureaus.

- **Additionally, financial institutions and credit grantors should *not* use easily-obtainable personal information (such as Social Security numbers) **as the sole authenticators.**** A range of alternative authentication tools exist, and need to be employed on a more widespread basis than the current marketplace reflects. These include tools such as:

- Knowledge-based authentication that relies on harder-to-obtain answers to “out-of-wallet” questions.
- Use of trusted third-party identity providers.
- Fraud alerts that require direct contact and authorization from the person whose identity information is being used.

- **The federal financial regulatory agencies and the Federal Financial Institutions Examination Council (FFIEC) are encouraged by this Panel to further review the sufficiency of current authentication practices for online banking.** The *FFIEC Guidance on Authentication in an Internet Banking Environment* says that banks must do something better than using single factor authentication based on passwords for “high risk” transactions involving access to customer information, or movement of customer funds to other accounts. Multi-factor authentication is not specifically mandated in such cases, but it is one of several methods recommended to mitigate risk, along with layered security (which would include mutual authentication). Ultimately, decisions on authentication are left to the banks to decide based on the results of a risk analysis.
- **Industry and standards developers should continue to develop and promote the use of specific trusted networks for multi-factor mutual authentication.** The infrastructure of trust networks between credit grantors (“relying parties”) and credential issuers (“identity providers”) continues to evolve. Recent advances across the industry, such as the development of the Web Services Security Standards (which support the Identity Metasystem and Information Cards), the Security Assertion Markup Language (which supports the Liberty Identity Federation Framework), and the Liberty Identity Assurance Framework may one day enable widely available “authentication networks” that could make this ideal a reality.
- **The public and private sectors need to start a process to work collaboratively to implement systems that allow physical identity documents to be validated in real time.** Systems are needed to verify *in real-time* that physical credentials presented at the time of a transaction (such as a driver’s license, Social Security card, or other government-issued ID) are valid and pertain to the person presenting them.
- **The Federal Trade Commission (FTC) and the federal financial regulatory agencies should provide guidance on best practices for credit grantors responding to fraud alerts.** The Fair and Accurate Credit Transactions (FACT) Act dictates what Credit Reporting Agencies must do regarding fraud alerts, and the red flag rules and guidelines provide further identity theft prevention guidance to financial institutions and other creditors. *What may be missing* is a review of Best Practices that can be used by credit grantors to clear a fraud alert under likely scenarios that may arise when credit grantors attempt to contact someone to *verify the authenticity of a request for credit*.

There is a wide range of users of credit reports that may encounter fraud alerts. However, there is no further guidance as to how these fraud alerts -- or any other type of fraud detection service -- should

operate. Specifically, this Panel uncovered a gap for what specific steps the users of credit reports should take when there is an initial fraud alert.

- **The Social Security Administration should initiate a project with the private sector to develop a process or mechanism that enables companies to verify if a Social Security number belongs to a minor.** Age verification against a Social Security number would greatly reduce identity theft against minors. *This information resides at the Social Security Administration.* At present, companies do not have a national means (e.g., a database) to verify if an individual is a minor before opening an account.
- **Entities reviewing their authentication practices against this Panel’s recommendations should consider the need for best practices and consumer education to help protect the elderly and the terminally ill from fiduciary abuse.** The elderly and the terminally ill, their family members and care-giving organizations need to be educated on the potential for abuse of the Social Security number as a tool to commit identity theft. It seems practical that this type of educational initiative be led by the Social Security Administration, working cooperatively with issue stakeholders across the public and private sectors.
- **The Social Security Administration should consider a new initiative that cooperatively works with individual states and the private sector to improve notification practices when someone is classified as deceased.** There are loopholes and inefficiencies in some current practices, which open a path for identity theft.
- **The FTC should consider a new mechanism to enhance identity theft protection for active duty military personnel.** Active duty military personnel are generally deployed, making the authentication steps a business might normally take impractical or even impossible (such as contacting the person by telephone or mail). Additionally, the current practices of allowing an “appointed delegate” to place or lift a credit alert for a deployed military person increases the risk of identity theft by that delegate.

Security Freezes¹⁶

There is a lot of information available in the marketplace and consumers tend to seek out identity protection measures as their situation warrants. A Security Freeze (a.k.a. Credit Freeze) is one of several options that consumers have to help thwart new account fraud. Importantly, consumers should understand that while a credit freeze may protect against the opening of new accounts, a freeze will not protect against fraudulent

¹⁶ See section 10D of the report.

takeover of existing accounts. Additionally, multiple state rules apply which adds a level of complexity and presents some usability issues for this tool. Consumers need to continue to be educated about the strengths and the limitations of Security Freezes and carefully weigh the benefits and tradeoffs of security freezes before making the decision to use this instrument.

The state credit freeze laws and the procedures of the Credit Reporting Agencies are germane to the discussion of Security Freezes, as noted in the Appendix to this Report Summary.

RECOMMENDATION # 5: Increase Understanding and Usability of Security Freezes

- **The Lenders, Government Agencies, Consumer Advocacy Groups, Credit Reporting Agencies and others should continue to support consumer educational programs that communicate both the benefits and limitations of security freezes.** There are many state-specific rules on security freezes as well as voluntary policies adopted by the Credit Reporting Agencies. To add further complexity, each Credit Reporting Agency has its own procedures for placing and lifting freezes. All of these variables (based both on legislated requirements and industry initiatives) present a communications challenge for educating consumers about how freezes work.

The spectrum of key stakeholders involved with this tool need to assemble to review their processes and standardize them to the extent possible to make security freezes easier for consumers to use.

C. The Maintenance of Identity Information

Data Security Management¹⁷

Information systems may be intentionally breached if an organization fails to adequately secure electronic systems and physical records containing personal information. Organizational mismanagement of personal data – poor data handling and disposal practices, lack of data encryption – also increases the likelihood of a data breach and the potential for identity theft to occur.

To safeguard sensitive information, businesses and other organizations should implement a comprehensive, top-down information security management program -- including a risk assessment and appropriate controls and countermeasures. While many standards and regulations to safeguard data currently exist, there is

¹⁷ See sections 11A and 11B of the report.

clearly an ongoing need to promote good data security management practices in the public and private sectors. Some examples of standards and other guidance relevant to Data Security Management are outlined in the Appendix to this Report Summary, including the ISO/IEC 27000 suite of standards (parts of which are still under development), the PCI Data Security Standard, and the North American Security Products Organization (NASPO) Security Assurance Standards for the Document and Product Security Industries (ANSI/NASPO Sav3.OP-2005).

RECOMMENDATION #6: Enhance Data Security Management Best Practices

ISO/IEC, the PCI Security Standards Council, NASPO and others in the standards developing community should review and augment as appropriate existing data security management standards (or, alternatively, develop new standards as may be needed) to give further attention to the following issues

- **Define the frequency of “periodic” employee security training and the content of an employee awareness program.** Employee awareness is a critical part of an effective information security program. While various third party resources exist, the creation of standards and best practices to better define what is meant by “regular” or “periodic” employee security training and the content of an awareness program would be useful.
- **Clarify requirements for data access credentialing and background checks.** ANSI/NASPO Sav3.OP-2005 provides a platform; however, additional industry guidance and best practices may be useful to clarify requirements for data access credentialing and background checks. Specifically, organizations should credential based on job-specific requirements and apply principles of “least privilege” and “need to know” (i.e., if someone doesn’t need access to data or knowledge of a certain process to accomplish their job, don’t grant them access).
- **Provide guidance on continuous review of access credentials and privileges.** As employees change roles and increase their responsibilities over time, they may be granted greater access to sensitive information. The depth of the background checks performed upon hiring may not be suitable for the increased levels of responsibilities. Guidance should be provided on how frequently and how detailed these background checks should be conducted, the strength of credentials provided, and the related access privileges
- **Develop targeted guidance for industry sectors that are not regulated or that do not have standards.** Some information security concerns and controls are not consistently applicable across all industry sectors. Regulated sectors (healthcare and financial, in particular) tend to be further ahead in their application of information security. Opportunities exist for the development of targeted guidance for non-regulated sectors.

- **Provide guidance to ensure that downstream vendors are secure.** The ANSI/NASPO SAV3.OP-2005 standard provides a foundation; additional guidance may be useful to ensure that third party “downstream” vendors follow information security management practices when receiving personally identifiable information in the course of business, or when certain functions are outsourced (e.g., applications, networks, data centers, or operations management).
- **Implement an ongoing program of security re-evaluation.** The President’s Identity Theft Task Force identified the need for continuous re-assessment. Organizations need to have an ongoing program of security re-evaluation to stay current with technological developments and new marketplace issues. The most effective information security programs include risk management protocols that continuously review technology shifts and related threats and vulnerabilities. Various risk assessment models are available, including NIST special publication 800-30, *Risk Management Guide for Information Technology Systems*, which is soon to be revised (see Appendix for details).
- **Develop a security breach risk assessment for insurance purposes.** Increasingly, insurance companies are excluding coverage for losses due to information security breaches. Additional guidance would be useful for insurance companies to facilitate accurate measurement of information security risks. This would allow organizations with good security practices to be extended coverage against security breaches in their Errors and Omissions and Directors and Officers insurance policies.

“Excessive” Data Collection / Retention/ Access¹⁸

The collection and retention of sensitive customer data (and/or inappropriate access to it) after it has served its intended purposes contributes to the problem of identity theft. Excessive use and storage of Social Security numbers is of particular concern to this Panel. Examples of relevant standards and guidelines for Data Collection / Retention / Access are highlighted in the Appendix to this Report Summary.

RECOMMENDATION #7: Augment Best Practices for Sensitive Data Collection, Retention and Access

- **Industry, the Small Business Administration, Chambers of Commerce and similar organizations that nurture and support small businesses need to develop and distribute practical guidance to their constituencies for data collection, retention and access.** Nearly 26 million small businesses in America collect, store and manage personal customer and employee

¹⁸ See section 11C of the report.

information, often without the expertise, resources or manpower needed to responsibly manage this storehouse of sensitive information. That's a big marketplace loophole for identity thieves to potentially exploit. In March 2006, BBB published a useful primer focused on helping to fill this need, entitled *Security & Privacy – MADE SIMPLER™*. This is a good example of the type of customized education this segment needs, but it needs to be circulated frequently and by more than just one issue stakeholder.

- **Industry and key government stakeholders (e.g. FTC, Office of Management and Budget, Social Security Administration) need to come together and develop uniform guidance on the collection, use and retention of Social Security numbers.** There is growing confusion by companies about which standards to apply or follow. This Panel sees a potential need to develop a unique standard as a means to provide common guidance to companies across industry lines, which would correspondingly eliminate costly and ineffective measures that may be only partially addressing the root issues.

Data Breach Notification and Remediation¹⁹

A wide array of state laws and federal agency guidelines exist concerning data breach notification. This has made the appropriate applications incredibly challenging and complex for businesses of all sizes. Issue stakeholders – individually and collectively – have previously identified the potential need for a uniform standard on notification. This Panel also raises this question and encourages additional dialogue between stakeholders until this issue is resolved.

There is a related issue that little specific or uniform guidance is available to businesses or consumers about what remedial action to take in the event a data compromise occurs.

A sampling of relevant laws and guidance that this Panel uncovered relating to Data Breach Notification and Remediation is reflected in the Appendix to this Report Summary.

RECOMMENDATION #8: Create Uniform Guidance on Data Breach Notification and Remediation

- **Issue stakeholders need to assemble and dialogue further on the desirability and feasibility of developing a private sector standard for data breach notification, recognizing there are**

¹⁹ See sections 11D and 11E of the report.

tradeoffs. Given the wide variety of guidance, it may be desirable for a Voluntary Consensus Standard to be developed by the private sector to provide a common baseline for organizations seeking to establish security breach notification procedures. In breaches involving cross-border information transfers, a Voluntary Consensus Standard could provide some basis for resolving conflicting national laws or regulations. It could also enumerate alternatives for remediation (see below). The potential tradeoff is that a “one size fits all” approach could result in a standard that is a “lowest common denominator,” and one that would only be enforceable if adopted into law or regulation.

This Panel identified two additional gaps in this area:

- *For Businesses* - Uniform guidelines on how to assist customers in the event of data compromise
 - *For Consumers* - A framework to evaluate potential value versus risk tradeoffs for services that detect or mitigate an identity theft incident resulting from the data breach.
- **Industry should take the lead in assembling a cross-sector forum to develop uniform guidance for the business community, government agencies, the non-profit community and academia on consumer remediation in the event of a data compromise.** Guidance should include factors such as the severity of the data compromise, the potential for actual identity theft as an outcome of the compromise, and how long the data leakage was going on before it was disclosed. This Panel believes that remediation guidelines may ultimately be a cascading set of actions, based on these factors. Remedies might include some combination of fraud alerts, counseling / recovery services, credit freezes, public record monitoring or credit monitoring.
- **Issue stakeholders should take the lead to proactively, and consistently, educate / reinforce identity theft prevention strategies to their consumers.** Tracking studies strongly suggest that proactive prevention strategies are a consumer’s best defense against identity theft. Consumers’ consistent behavioral choices and vigilance are keys to their own safeguarding.

Should a consumer be notified that a compromise of their data has occurred, they also need:

- Solid education to help them discern among victim assistance services (including insurance).
- Guidance to help them secure and protect their personally identifiable information in the future.
- Steps for changing their federally-issued documents, as the situation warrants.

Appendix to Report Summary

Existing and/or Pending Standards, Best Practices, Guidelines & Rule-Making

A. The Issuance of Identity Credentials

Security of the Issuance Process

- Expected rulemaking by the National Center for Health Statistics (NCHS) and the Social Security Administration (SSA) on standards for birth certificates and Social Security cards in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)
- NCHS Model State Vital Statistics Act & Regulations
- Rulemaking by the Department of Homeland Security (DHS) implementing The REAL ID Act
- Western Hemisphere Travel Initiative
- DHS / State initiatives for enhanced driver's licenses (EDLs)
- ISO/IEC 27000 series of standards on information security
- American Association of Motor Vehicle Administrators (AAMVA) DL/ID Security Framework
- HSPD-12 Personal Identity Verification Program
- Australian National Smartcard Framework
- North American Security Products Organization (NASPO) Security Assurance Standards for the Document and Product Security Industries (ANSI/NASPO SA v3.OP-2005)
- Document Security Alliance (DSA) white papers on birth certificates and Social Security cards under IRTPA, and recommendations for driver's license security and The REAL ID Act
- National Association for Public Health Statistics and Information Systems (NAPHSIS) white paper on Recommendations for Improvements in Birth Certificates
- Mailing Standards of the US Postal Service Domestic Mail Manual

Commercial Issuance

- ID Theft Red Flags and Address Discrepancies Rule
- Open ID
- National Association for Public Health Statistics and Information Systems (NAPHSIS) Electronic Verification of Vital Event (EVVE) system

Credential Security

- Aforementioned defining of standards for birth certificates and Social Security cards by NCHS and SSA, respectively, in response to IRTPA
- Aforementioned DSA, NASPO white papers
- AAMVA International Specification – DL/ID Card Design (2005)
- AAMVA fraudulent document recognition training curriculum
- Rulemaking by DHS implementing The REAL ID Act
- International Civil Aviation Organization (ICAO) Machine Readable Travel Documents standard
- NASPO, Semiconductor Industries Association (SIA) and Semiconductor Equipment and Materials International (SEMI) project on secure serialization anti-counterfeiting technology, and European Committee for Standardization (CEN) project on same

B. The Exchange of Identity Data

Authentication

- Fair Credit Reporting Act (FCRA) and 2003 Fair and Accurate Credit Transactions (FACT) Act amendments to same
- ID Theft Red Flags and Address Discrepancies Rule
- USA PATRIOT Act – Section 326, Customer Identification Program (CIP) Regulation
- Federal Financial Institutions Examination Council (FFIEC) Guidance on Authentication in an Internet Banking Environment and FAQ's on same
- Social Security Administration's Death Master File

Security Freezes

- State credit freeze laws
- Procedures of the Credit Reporting Agencies

C. The Maintenance of Identity Information

Data Security Management

General industry standards / rules

- ISO/IEC 27000 series of standards on information security
- North American Security Products Organization (NASPO) Security Assurance Standards for the Document and Product Security Industries (ANSI/NASPO Sav3.OP-2005)
- NIST special publication 800-30, *Risk Management Guide for Information Technology Systems*²⁰
- FTC FACTA Disposal Rule

Financial Services Industry-specific standards, laws and rules

- PCI Data Security Standard
- The Financial Modernization Act of 1999, also known as the “Gramm-Leach-Bliley Act”
- Federal Trade Commission Safeguards Rule and Financial Privacy Rule

Healthcare Industry-specific standards, laws and rules

- ASTM E1869-04, Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records
- The Health Insurance Portability and Accountability Act (HIPPA)
- The Dept. of Health and Human Services’ Privacy and Security Rules

Relevant Conformity Assessment Programs

- Certified Identity Theft Risk Management Specialist (CITRMS) ICFE course
- NASPO Certification to ANSI/NASPO Sav3.OP-2005
- Security Audit Procedures for the PCI Data Security Standard

²⁰ An initial draft revision of NIST Special Publication 800-30 is projected for publication in January 2008. Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, will focus exclusively on risk assessments as applied to the various steps in the Risk Management Framework described in NIST Special Publication 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, an initial draft of which was released in October 2007.

“Excessive” Data Collection / Retention / Access

- ISO/IEC 27000 series of standards on information security
- PCI Data Security Standard
- HIPPA
- Office of Management and Budget (OMB) Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, which urges federal agencies to explore alternatives to the use of Social Security numbers
- BBB’s *Security & Privacy – MADE SIMPLER™*

Data Breach Notification and Remediation

- State breach notification laws
- State credit freeze laws
- The President’s Identity Theft Task Force Strategic Plan
- OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- FTC Final Rules on FACTA Identity Theft Definitions, Active Duty Alert Duration, and Appropriate Proof of Identity
- Office of the Privacy Commissioner of Canada: Key Steps for Organizations in Responding to Privacy Breaches, April, 2007
- FTC’s website: Consumer Information

2. Introduction

Identity theft has become one of the nation's most prominent marketplace issues in recent memory, and a large threat to commerce. In 2006, close to a quarter of a million complaints about identity theft were registered with the Federal Trade Commission, topping the list of consumer fraud complaints for the seventh year running.²¹ According to Javelin Strategy & Research Inc., identity fraud cost U.S. businesses and consumers an estimated \$49.3 billion in 2006.²² Estimates on the number of identity fraud victims in 2006 range from about 8.9 million (Javelin) to about 15 million (Gartner, Inc.).²³

The public and private sectors are responding to this crisis. Lawmakers on Capitol Hill are coming down harder on identity criminals. In 2007, the President's Identity Theft Task Force released a four-pronged strategic plan focused on customer data protection including consumer education, identity verification and authentication, victim assistance and recovery, and law enforcement. Across the Americas, to Europe and China, other countries are considering identity theft a global priority. And the voluntary standards community is doing its part to collaborate on standards and best practices that can be used to stem the tide of identity crimes. This report is one of many contributions to this ongoing dialogue.

3. Target Audience for this Report

As more fully articulated below, the primary audiences for this report are businesses and other organizations, be they private or public sector, seeking to augment their arsenal of best practices with which to combat ID theft and fraud and protect themselves and their customers from the risks associated with these crimes. This would include industry analysts who identify trends in the market and help to shape best practices. Another audience would be the standards developing organizations and related conformity assessment bodies that it is hoped will take up the challenge of creating new standards and compliance programs, or updating existing ones, in light of the suggestions herein provided. A third audience is legislators, to draw their attention to the success that the private and public sectors can achieve working in partnership to innovatively deal with these

²¹ <http://www.ftc.gov/opa/2007/02/topcomplaints.shtm>

²² <http://www.javelinstrategy.com/idf2007>

²³ Ibid (Javelin) and <http://www.gartner.com/it/page.jsp?id=501912> (Gartner). The Panel recognizes that there are some discrepancies in the conclusions reached by industry analysts as to the magnitude of the identity theft problem, depending upon research methodologies and definitions used. Volume II of this report contains a sampling of 2007 research studies and reports on ID theft and information security.

challenging issues. A fourth audience would be law enforcement, to keep them current on industry best practices. And, finally, consumers, who in the end stand to benefit from this initiative if the guidance and recommendations described herein are appropriately implemented.

4. Background / Panel Objectives

When the Better Business Bureau (BBB) approached the American National Standards Institute (ANSI) with the idea for this Panel in late 2005, the BBB was already actively engaged in an education and outreach campaign on ways to mitigate ID theft and fraud. Many consumer and industry groups – and some federal agencies – were also pursuing separate identity-related solutions and strategies.

As advocates of industry self-regulation when and where possible, ANSI and BBB agreed that a collaborative cross-sector effort was needed to address this issue. On September 13, 2006, the **Identity Theft Prevention and Identity Management Standards Panel (IDSP)** was officially launched. The Panel leveraged the combined strengths of the two organizations: BBB’s reputation for advancing trust in the marketplace and ANSI’s long service as coordinator of the open, consensus-based U.S. voluntary standards and conformity assessment systems, and its successful track record of establishing and administering standards panels that address urgent national and global priorities.

The Panel was charged with:

1. Identifying and cataloguing existing standards, guidelines, best practices and related compliance systems focused on identity theft and fraud, including definitions, threats and identity management solutions, that could positively impact this issue, and
2. Identifying areas needing updated or new standards, guidelines, best practices or compliance systems, which could further minimize the threat of identity theft or enhance identity management.

Given the complexity of this issue – and its proven ability to morph in how it manifests over time and constituencies – the Panel targeted to complete its work within 15 months. The aim was to deliver by January 2008 a comprehensive, cross-sector report describing standards, guidelines and best practices that businesses and other organizations can use to prevent and respond to identity theft and fraud and protect the confidential personal data of their employees and customers. The expectation was and is that the Panel’s

recommendations for new or enhanced standards and best practices shall serve as a call to action for further work by the standards development community. Annex 1 to this report is the Panel's charter.

5. Scope of Work / Coordination with Other Initiatives

One of the initial questions that the Panel wrestled with was what it could hope to accomplish given its aggressive timetable and the vastness of this issue across sectors, recognizing that its output would be shaped by the concerns, knowledge and commitment of resources of the participants. While much of the Panel's attention focused on financial identity theft, the Panel also noted other forms of identity theft that deserve attention including medical identity theft, criminal identity theft, and employment identity theft. In its early stages of identifying problems, Panel members touched on these facets; however, given the time restrictions that the Panel set for itself to complete this report, there has not been sufficient time to develop these areas. That said much of the analysis contained herein potentially could have application to these forms of identity theft as well.

To the extent possible, the Panel endeavored to outreach to and coordinate with other organizations and national and international initiatives addressing identity-related issues. For example, the Panel established a cooperative relationship with the [Center for Identity Management and Information Protection \(CIMIP\)](#), a research center at Utica College in New York focusing on critical issues in identity management, information sharing policy, and data protection. The Panel also exchanged information with the [International Telecommunication Union Focus Group on Identity Management](#), an effort by telecommunications and information and communications technology experts to facilitate the development of a generic identity management framework. In addition, the Panel outreached to the [Healthcare Information Technology Standards Panel \(HITSP\)](#) which has produced an overarching security and privacy architecture to address data protection issues in electronic health records, though it has not addressed the kind of identity theft issues that came up in the Panel's Working Groups, such as the fraudulent receiving of medical care. The Panel also noted that the [ANSI Homeland Security Standards Panel \(ANSI-HSSP\)](#) has launched a new workshop on Credentialing and Access Control for Disaster Management in response to the Hurricane Katrina aftermath findings which pointed to the failures of credentialing and access control at the incident site as major issues.

As part of its outreach efforts, the Panel chair and staff also made presentations to various audiences including:

American Bar Association's Information Security Committee
BITS Fraud Reduction Steering Committee
Consumer Data Industry Association
Document Security Alliance
Economic Crime Institute of Utica College
General Services Administration's Intergovernmental Teleconference Group
National Electrical Manufacturers Association

6. Methodology

In order to provide effective and substantial direction toward achieving the Panel's strategic objectives, a Steering Committee was constituted. The Steering Committee consisted of the Panel Chairman, Founding Partners, and selected At-large members from a diverse mix of private and public sector organizations that have expertise and recognized leadership in the marketplace on some aspect of the issues.

Following two organizational Steering Committee meetings, the Panel's kick-off plenary meeting was held November 17, 2006. The purpose of the initial plenary meeting was to raise awareness of the issues and the IDSP initiative, to share information and network with others working in this area, and to help frame the scope of the Panel's work for the coming year.

Three Working Groups were established to carry out the Panel's work taking a "life-cycle" approach to identity:

Working Group 1 - *Issuance*: sought to identify and assess standards relating to the issuance of identity documents by government and commercial entities;

Working Group 2 - *Exchange*: focused on standards pertaining to the acceptance and exchange of identity information;

Working Group 3 - *Maintenance*: addressed standards relating to the ongoing maintenance and management of identity information.

Participation in the Working Groups was open to all Panel members who elected to participate, and drew from a broad range of expertise. The Working Groups carried out their deliberations electronically and via conference calls largely working independently of one another. At each phase of the process there were

designated checkpoints, teleconferences and meetings where the Working Group leaders reported to the Steering Committee for purposes of coordination and to maintain forward progress.

The work proceeded according to the following timeline:

Inventory Phase (1st quarter '07) – Each Working Group catalogued existing standards, guidelines, and best practices within its defined scope. Applicable laws, white papers, conformity assessment schemes, and proposed legislation were also noted, along with existing glossaries of identity related terms. A marketplace survey beyond the Panel membership was conducted which elicited further input from standards experts in developing this Standards Inventory. A search of key terms in ANSI's NSSN standards database also was carried out which provided additional results. Volume II of this report, issued separately, is the comprehensive Standards Inventory resulting from this cataloguing exercise. A working list of definitions also was developed as an interim tool to help facilitate common understanding during the assessment phase of the Panel's work.

Assessment Phase (2nd and 3rd quarters '07) – Each Working Group described various identity fraud-related problems as well as possible solutions and idealized “dream states.” While the groups' primary focus was not to define solutions to the problems outlined, it was found to be advantageous to recognize the range of possible solutions (e.g., industry cooperation and best practices including standards, technology, consumer education, law enforcement and legislation) as a means to identify applicable standards and potential gaps. This process did not attempt to define all possible solutions nor quantify the most applicable solutions to each of the problems. An effort was made to prioritize the problem areas.

New account processing was identified by each of the groups as a risk scenario where identity thieves often cause harm by establishing fraudulent new accounts using stolen identities. Process flows and accompanying narratives were created to illustrate 1) the birth of a citizen and the acquisition of identity credentials and 2) a typical new account establishment procedure. Annex 2 presents these process flows and narratives. Using the Standards Inventory compiled earlier, the Working Groups undertook to perform a gap analysis against these process flows, overlaying the identified problems.

As a result of this gap analysis, certain standards, laws and other guidelines were called out by the Working Groups in their reports contained herein as having particular relevance to the problem areas of concern. Annex 3 are these standards culled from the inventory, mapped against the identified problems. The documents listed therein are merely examples of some of the standards and guidelines that may be relevant—

this was not an exhaustive exercise nor is the list intended to be a rank ordering of some standards over others. Many of these items are high-level business process standards that can be or are applied across sectors. There is also a considerable body of standardization work that is highly technical in nature. Many of those items are captured in Volume II of this report.

On September 24, 2007, the Panel held its second plenary meeting. The purpose of the meeting was to present the Panel’s work to a broader audience and obtain additional input, and to work towards consensus in helping to shape the Panel’s report and recommendations. The agenda was built around concurrent breakout sessions where participants considered and debated the work produced by the Panel’s three Working Groups up to that point.

Final Deliverable Phase (4th quarter ’07) – Working Group members were recruited to comprise a drafting committee to draft sections of the Working Group reports taking into consideration the consolidated inputs and recommendations. These drafts were subsequently vetted within the Working Groups during a series of conference calls. The Steering Committee oversaw development of the Panel’s draft report including the Report Summary and Volume II, the Standards Inventory, which were then circulated to the Panel for comment. Comments from this review and subsequent drafts were again vetted with the Working Groups and the Steering Committee. This report and Volume II together represent the Panel’s final deliverable.

For clarity, early on, it was agreed that certain items were within the Panel’s charter, and others were not:

In Scope

Inventory of existing standards
Indexing standards
Gap Analysis of current standards

Out of Scope

Modification of existing standards
Rank ordering of standards
Developing new standards

A “gap” was defined as a lack of standards, guidelines, best practices, or compliance systems that adequately address a problem area. Recommendations to fill gaps were framed as areas needing updated or new standards, guidelines, best practices and related compliance systems. Recommendations for what could be deemed new products, services, or legislation were deemed out of scope.

7. Participation and Funding

From its inception, the IDSP was envisioned as a highly inclusive undertaking where diverse private and public sector interests would come together to identify existing and needed standards to address this emerging national and global priority. Participants included some 165 representatives from 78 organizations: industry, NGOs, government, consumer groups, standards developing bodies, and others, providing a range of perspectives. Participating organizations are listed below. Some actively participated; others did not.

Funding for the Panel came from a mix of private and public sector support. Three (3) levels of participation were created – *Founding Partner, Contributing Member and Panel Participant*:

- *Founding Partners* -- The initial costs for the IDSP were underwritten by a team of nine high profile companies: AT&T, ChoicePoint, Citi, Dell Inc., Intersections Inc., Microsoft, Staples, Inc., TransUnion and Visa Inc. These Founding Partners formed the executive leadership of the Panel's Steering Committee, contributed substantial resources to facilitate the Panel's activities, and received high profile public recognition for doing so.
- *Contributing Members* rounded out the Panel's cross-sector participation and received a different level of public recognition.
- *Panel Participants* paid an annual per person fee to participate, access Panel materials and attend plenary meetings.

Participating Organizations

AARP
Accenture
Accredited Standards Committee X9, Inc. Financial Industry Standards
Affinion Group
Alliance for Telecommunications Industry Solutions (ATIS)
American Association of Motor Vehicle Administrators (AAMVA)
American Financial Services Association
American National Standards Institute
AOL LLC
APCO International - Assn of Public Safety Communications Officials Intl
ARMA International
AT&T
Burton Group
Canadian Standards Association
Cash Pass Inc.
Center for Democracy and Technology

Center for Identity Management Information Protection (CIMIP)
ChoicePoint
Citi
Clarke American Corp
Columbia University
Consumer Data Industry Association
Council of Better Business Bureaus
CSA America, Inc.
Davis & Henderson
Debix
Dell Inc.
Equifax
Europ Assistance USA
Experian
Federal Trade Commission²⁴
Fellowes, Inc.
General Services Administration
Global Identity Solutions
Good Health Network
HID Global Corporation
Identity Theft Resource Center
IdentityTruth
Institute of Consumer Financial Education
Intersections Inc.
IronKey, Inc
KPMG LLP
Kroll's Fraud Solutions
Lifelock
Mag Tek Inc
Microsoft
MRP Solutions
MyPublicInfo, Inc.
National Association for Public Health Statistics and Information Systems (NAPHSIS)
National Association of Professional Background Screeners
National Consumers League
Nationwide Insurance
North American Security Products Organization (NASPO)
Northern Virginia Community College
Oracle
Pay By Touch
Pitney Bowes Inc
Pre-Paid Legal Services, Inc.
Robert Pinheiro Consulting LLC
SourceCheck, Ltd.
Southwest Research Institute
Staples, Inc.
Telcordia Technologies

²⁴ FTC staff participated in the information-gathering phase of this initiative. Commission staff did not contribute to, and the Commission has not considered, the report's findings and recommendations."

Telecommunications Industry Association
The First American Corporation
Thinklikeaspy.com
TransUnion
TrustedID, Inc
Underwriters Laboratories Inc.
US Department of Commerce – International Trade Administration
US Department of Commerce – National Institute of Standards & Technology (NIST)
US Department of Homeland Security
US Department of Justice
US Department of State
US Postal Inspection Service
USinternetworking (AT&T Sub.)
Visa Inc.
Wisconsin Office of Privacy Protection

8. Findings and Recommendations (Preamble)

The findings and recommendations contained in this report were not formally voted on by the Panel. They represent the consensus²⁵ views of the stakeholders actively participating in the Panel's Working Groups.

What follows are the reports from the three Working Groups describing the issues in greater detail. Each section contains a description of the identified problem(s), discussion of the issues, examples of relevant existing standards, and potential gaps and recommendations. As noted earlier, examples of existing standards are just that—they are not intended to be seen as suggesting a hierarchy of some standards over others. It is simply that they were called out by the Working Groups as having particular relevance to the problem areas of concern.

In various places the report discusses advances in the industry and the need for new systems. In such cases, it is generally understood that such developments often stimulate technical standards activity and/or may necessitate the development of best practices.

For purposes of this report, identity theft is defined as the stealing or illicit use of someone else's identity credentials to commit fraud, for example, by opening new financial accounts, gaining access to existing accounts and loans, receiving health care services, etc. Examples of identity theft schemes include:

- Pretending to be another real person by using their credentials to obtain new services and products (i.e., "true name" identity theft);
- Presenting and using a deceased person's identity credentials;
- Presenting and using another person's credentials to gain access to their existing services and accounts;
- Creating a new or synthetic identity by combining real identity information with phony information (e.g., by fabricating a driver's license).

²⁵ Consensus signifies substantial agreement but not necessarily unanimity.

9A. Working Group 1 – Foundational Creation - Issuance of Birth Certificates and Social Security Cards

The Problem

Weak linkage between individual and birth record

There is a weak linkage between an individual and his/her birth record. One concern is whether information on the birth certificate is factual. Another is whether a person obtaining a certified copy of the birth record has legal rights to the record. A third issue is whether the birth certificate presented to an adjudicating agency is a valid record for the person submitting it. The birth certificate establishes the facts that a birth event occurred on a specific date, but there is no way to conclusively match an individual to the birth certificate that is presented to verify that it is the same person.

Circular nature of issuance process

As currently practiced, there is a circularity associated with the use of birth certificates and Social Security cards as “identity documents.”²⁶ Such documents are also referred to as “breeder” documents since they breed other documents such as a drivers’ license that depend on them for initial identity proofing. For example, a birth certificate is used to obtain a card or driver’s license; a Social Security card is used to obtain a driver’s license; and a driver’s license is used to obtain a birth certificate. If the birth certificate is not verified to be accurate, then documents subsequently issued such as the driver’s license, Social Security card or passport that rely upon the birth certificate are also potentially not accurate.

Discussion

Most birth certificates are created in a hospital or birthing center; however problems can occur when birth certificates are not created contemporaneously with birth. The filing of uninstitutionalized births (home births) is not well regulated leaving a reliance on weak secondary documents such as baptismal, church, and school records to establish identity. When the authenticity of secondary documents is not verified, the potential of fraudulent activity is increased.

²⁶ For the sake of simplicity, various credentials that are commonly used to verify identity are referred to throughout this report as “identity documents.” It is recognized that these documents were in fact created for other purposes: a birth certificate to confirm a birth event as a public health record, a social security card to enroll in the social security program, a driver’s license to obtain driving privileges, and a passport to permit border crossings.

Birth certificates are presently included in many states' list of acceptable "breeder" documents. However, in most instances they are not verified by the issuing agency--particularly out-of-state documents. To be issued a REAL ID credential, applicants will have to present (and have verified) at least one of the documents listed in the REAL ID final regulations -- which includes a certified copy of a birth certificate. In the case of passports, the Passport Office requires a certified copy of a birth certificate with a raised seal by the issuing city, county or state. However, the Passport Office does not communicate with issuers of birth certificates to verify them except where there are conditions of suspicion about their authenticity.

The reissuance of a birth certificate or a Social Security card poses additional questions. Individuals may misplace their birth certificate or Social Security card resulting in the need to issue new credentials to those holding existing ones. A fraudster can seek a duplicate credential simply by knowing basic birth information and claiming to be someone already in the system.

There should be a strong linkage established between a birth record and the individual presenting a document to obtain identity credentials. A biometric is one possible solution; however, there are significant economic and social barriers to overcome. The cost of equipment and privacy issues will be major factors.

The National Association for Public Health Statistics and Information Systems (NAPHSIS) has developed an Electronic Verification of Vital Event (EVVE) system which provides government-to-government verification of birth or death information. However, the system is currently only available in a small number of states. It is anticipated that the Department of Homeland Security (DHS) will provide resources to install the system in all states. The system also is not yet available to the private sector. NAPHSIS would need to discuss with the states whether state law permits the releasing of confidential information to the private sector.

When the Social Security Administration (SSA) requires a birth certificate for benefit purposes, the birth certificate needs to be verified. EVVE can be used for that purpose. The SSA has started using EVVE in the states where EVVE is available.

A database, accessible by multiple parties, with alerts and search capability, could help to isolate names and addresses that have been used in the past for fraudulent purposes.

Existing Standards (Examples)

Birth Certificates

The Intelligence Reform and Terrorism Prevention Act (IRTPA) was passed in 2004 (row²⁷ A16). Forthcoming rulemaking by the National Center for Health Statistics (NCHS) on birth certificates (section 7211 of the IRTPA) is expected to be issued for public comment in the spring of 2008. The Document Security Alliance (DSA) and NAPHSIS have submitted white papers to NCHS with recommendations for the IRTPA regulations.

The registration of vital events and issuance of related documentation is a state function and responsibility. Each state has laws and regulations for the collection, preservation, and issuance of vital events information. The NCHS has developed a [Model State Vital Statistics Act & Regulations](#) for registration of vital events (row C4); however, the adoption by states is voluntary. To standardize the collection of birth and death data nationally, revisions to the U.S. Standard Certificates of Live Birth and Death and the Fetal Death Report were made in 2003.

NAPHSIS is in the process of creating a set of guidelines for nearly every recording and issuance situation that exists.

Social Security Cards

Section 7213 of the IRTPA deals with Social Security cards and numbers. It establishes minimum standards for verification of documents submitted by an individual to establish eligibility for the Social Security card. DSA has submitted a White Paper on the Formulation and Definition of Minimum Card Security Standards for the Social Security Administration, dated April 4, 2006.

In the wake of the President's ID Theft Task Force strategic plan, the Federal Trade Commission (FTC) and the Office of Management and Budget (OMB) respectively are looking at the use of Social Security Numbers (SSNs) in the commercial and governmental sectors.

²⁷ Row numbers referenced throughout this document refer to the additional information contained in Annex 3 and Volume II of this report.

Potential Gaps

Recommendation 1: Enhance the Security of the Issuance Process

- **The National Center for Health Statistics (NCHS) and Social Security Administration (SSA) need to make it a priority to issue standards for birth certificates and Social Security cards, respectively, in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004.** The regulatory process under IRTPA for birth certificates and Social Security cards is underway and has superseded the standards process. Agencies have delayed developing standards in anticipation of the regulatory changes. However, the regulatory process appears to be stymied and after two years the regulations have not been promulgated. The development of standards is needed now and should not be held in further abeyance. Agencies need to proceed with standards or guidelines. Adjustments can be made accordingly once regulations are finalized. The agencies should consult with industry and other stakeholders on the weaknesses associated with the current circular nature of the issuance process, as outlined above.

- **Government agencies that issue identity credentials need to improve communication and cooperation among themselves as well as between the government and the private sector. The National Association for Public Health Statistics & Information Systems (NAPHSIS) needs to continue the development and expansion to governmental agencies of the Electronic Verification of Vital Events (EVVE) system to authenticate credentials presented by applicants for service or benefits.** There currently is no mechanism for vital records offices to consistently and effectively communicate with state motor vehicle departments, the State Department's Passport Office, the Social Security Administration, banks, etc. on incidents of attempted fraud. Similarly, agencies that track birth certificate fraud do not have a mechanism to communicate back to the vital records offices. This lack of communication among the agencies enables ID thieves to continue their fraudulent practices.

9B. Working Group 1 – Subsequent Credentials – Issuance of Driver’s Licenses, ID Cards and Passports

The Problem

Issuance processes need to be made more secure

The state-issued driver’s license (DL) and identification card (ID) are the most widely used and accepted form of identification in the United States. As more fully described below, they are at the heart of our identification infrastructure, along with passports and the recently introduced enhanced driver’s licenses that double as a travel document. While credentials can be made as "tamper proof" as possible, if the issuance process for the major identification cards is not made more secure, the preponderance of identity document fraud will continue. Such fraud is commonly perpetrated by criminals enrolling in a system under a false identity.

All of the issuers of the major documents use the others’ credential to verify the identity of applicants, e.g., the driver’s license is used when applying for a certified copy of a birth certificate, the certified copy of the birth certificate is used when applying for a passport, and so on. In spite of this circularity, Congress did not require the other issuing agencies to access motor vehicle agency databases as part of The REAL ID Act.

Discussion

Various initiatives related to the issuance of driver’s licenses, ID cards and passports are described below.

All-State DL/ID Records System

State motor vehicle agencies have proposed a nationwide, integrated information system to verify whether a driver’s license or identification card applicant is already licensed in another state or holding multiple cards. Such a system would combine the functions of the Commercial Driver’s License Information System (CDLIS), the Problem Driver Pointer System (PDPS) and Driver’s License Reciprocity System (DLR). It would be a distributed system with a central pointer file, similar to the one used today by CDLIS, and would encompass approximately 245 million records. The system would direct one state where to find and accurately verify someone’s driving history in another state. It would allow states to better enforce the one driver, one license, one driver control record concept, thus allowing the states to better manage their driver control programs for both commercial and non-commercial drivers. In conjunction with electronically verifying birth certificates and Social Security information, as well as other information provided by the

driver at the time of application, states will be able to do a much better job of limiting individuals to only one active credential.

Commercial Driver's License Information System (CDLIS)

The Commercial Motor Vehicle Safety Act of 1986 (P.L. 99–570) established the commercial driver's license program and the Commercial Driver's License Information System to serve as a clearinghouse and repository of commercial driver licensing and conviction data. CDLIS manages the records of some 13 million commercial motor vehicle drivers. Prior to implementation of CDLIS, in a number of states and the District of Columbia, many drivers were able to obtain driver's licenses from more than one jurisdiction and hide or spread convictions among several driving records and continue to drive.

CDLIS operates a database containing a “pointer file” that points to the state that has taken State of Record (SOR) responsibilities for the commercial driver. In most cases, a pointer indicates that the SOR has issued a commercial driver's license (CDL) to the driver. Prior to issuing a CDL, jurisdictions are required to search the CDLIS database to determine if the applicant currently holds, or previously held, a CDL issued by another state.

In a 2001 report to Congress,²⁸ USDOT stated that the CDL program has accomplished its objective of limiting commercial motor vehicle operators to a single driver license. The one license is now a CDL. All quantitative and qualitative data show that commercial drivers no longer possess multiple licenses – neither multiple CDLs nor a CDL and a non-CDL. The report made the following recommendation: Using the current CDLIS structure for an all-driver system would work using available technologies and would meet current service goals.

The REAL ID Act

On May 11, 2005, Congress passed The REAL ID Act (P.L. 109-13), creating national standards for the issuance of state driver's licenses and identification cards. The act establishes certain standards, procedures and requirements that must be met if state-issued DL/IDs are to be accepted as valid identification by the federal government. REAL ID requires states to verify with the issuing agency the issuance, validity, and completeness of each source or “breeder” document required to be presented by an applicant. The statute specifically directs states to use the U.S. Citizenship and Immigration Services (USCIS) Systematic Alien

²⁸ Report To Congress: Evaluation of Driver Licensing Information Programs and Assessment of Technologies. U. S. Department of Transportation, National Highway Traffic Safety Administration in conjunction with Federal Motor Carrier Safety Administration and American Association of Motor Vehicle Administrators, July 2001

Verification for Entitlements system (SAVE) to verify the legal presence of all non-citizen applicants. While the act contemplates the use of five national electronic systems to facilitate verification, currently only one of these systems is available on a nationwide basis. System development, programming, testing and training will take considerable time and investment that far exceed the deadlines or funds provided by the act or Congress.

The five verification systems are:

1. All-State DL/ID Records System—As described above, a system is necessary to ensure an applicant is not already licensed in another state or fraudulently holding multiple DL/ID cards. As noted by USDOT, such a system could be modeled after the existing Commercial Driver’s License Information System. It also is necessary to verify the validity of an existing REAL ID DL/ID card should that be submitted as proof of identify in another state.

2. Department of State—While the Department of State U.S. Passport database already includes birth records of U.S. citizens born overseas, there is no way for states to access this information. Implementation of The REAL ID Act would require the Department of State to define the requirements for such a system, construct the system and test and work with the states to make it available for deployment.

3. EVVE (Electronic Verification of Vital Events) Records—States have worked with the American Association of Motor Vehicle Administrators (AAMVA) to pilot the NAPHSIS EVVE system to verify birth information. The pilot does not involve all states and does not include information concerning marriage, divorce and death records (which would be a useful addition). In addition, the system is still in its early implementation stage.

4. SSOLV (Social Security On-Line Verification)—Currently 47 states and the District of Columbia have the ability to verify applicants’ Social Security Numbers with the Social Security Administration.

5. SAVE (Systematic Alien Verification for Entitlements)—SAVE was created to verify eligibility for federal benefits. It will have to be retrofitted to fulfill its expanded role under REAL ID. At least 21 states currently are using SAVE or are in the process of gaining access to the system. Once the system is constructed, all jurisdictions would need time to test and certify the system.

Concerns have been raised about the ability to implement REAL ID in the manner originally proposed.²⁹ On January 11, 2008, the Department of Homeland Security (DHS) announced a Final Rule to implement The REAL ID Act³⁰ and stakeholder organizations continue to raise concerns.

U.S. Passports

According to the U.S. State Department's website, some 12 million U.S. passports were issued in Fiscal Year 2006. Through an adjudication process, examiners determine whether to issue passports. Examiners scrutinize identification and citizenship documents to verify identity and U.S. citizenship, and examine applications to detect potential indicators of fraud. The process is facilitated by the Travel Document Issuance System (TDIS). TDIS checks the applicant's name against several databases—including the State Department's Consular Lookout and Support System (CLASS), which contains information provided by various offices within the Department and information on outstanding criminal warrants provided by the U.S. Marshal's Service, the FBI, and other state and federal agencies. When examiners detect potentially fraudulent passport applications, they send the applications to their local fraud prevention office for review and potential referral to the State Department's Bureau of Diplomatic Security for further investigation.

Imposters' use of assumed identities, supported by genuine but fraudulently obtained identification documents, is the most common way to fraudulently obtain a passport, accounting for 69 percent of passport fraud detected in fiscal year 2004, according to the Government Accountability Office (GAO). Other methods include submitting false claims of lost, stolen, or mutilated passports; child substitution; and counterfeit citizenship documents.

The CLASS name-check system does not include names of all criminals wanted by federal and state law enforcement agencies. The State Department receives varying degrees of information from the Department of Health and Human Services, Department of Homeland Security, Social Security Administration, and individual state motor vehicle agencies. The State Department does not verify the authenticity of birth certificates received as part of the passport application process.

²⁹ The Real ID Act: National Impact Analysis. National Governors Association, National Conference of State Legislatures and American Association of Motor Vehicle Administrators, September 2006. The three associations commented, among other things, that a May 11, 2013 deadline for re-enrollment is problematic and would require at least a 10 year timeframe.

³⁰ At the time this report was prepared, the final rule had been announced by DHS but had not yet been published in the *Federal Register*.

Limited fraud prevention staffing, training, oversight, and investigative resources pose additional challenges to fraud detection efforts, according to the GAO.

To improve the coordination and execution of passport fraud detection efforts, the GAO recommended³¹ that the Secretary of State take the following actions:

- Expedite, in consultation with the U.S. Attorney General, Director of the FBI, and Secretary of Homeland Security, arrangements to enhance interagency information sharing, and reach agreement on a plan and timetable for doing so, to ensure that the CLASS system contains a more comprehensive list of individuals identified in the Terrorist Screening Center database as well as state and federal fugitives and that such information is made available to the State Department in an efficient and timely manner.
- Establish and maintain a centralized and up-to-date electronic fraud prevention library that would enable passport agency personnel at different locations across the U.S. to efficiently access and share fraud prevention information and tools.
- Consider designating additional positions for fraud prevention coordination and training in some domestic passport-issuing offices.
- Assess the extent to which and reasons why workload transfers from one domestic passport-issuing office to another were, in some cases, associated with fewer fraud referrals, and take any corrective action that may be necessary.
- Establish a core curriculum and ongoing fraud prevention training requirements for all passport examiners, and program adequate time for such training into the staffing and assignment processes at passport issuing offices. Strengthen fraud prevention training efforts and oversight of passport acceptance agents.

³¹ State Department: Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts. United States Government Accountability Office, Report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate, May 2005 (GAO-05-477).

Western Hemisphere Travel Initiative (WHTI)

The Western Hemisphere Travel Initiative (WHTI) is the Administration's plan to implement a requirement in The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) directing the Departments of Homeland Security and State to develop and implement a plan to require all travelers (both U.S. citizens and foreign nationals) to present a passport or other document, or a combination of documents, that denote identity and citizenship when entering the U.S. Congress amended portions of the Act in 2006.

Effective October 1, 2007, U.S. citizens traveling by air to Canada, Mexico, the Caribbean, and Bermuda are required to present a passport or other WHTI-compliant documentation to enter or depart from the United States. On January 31, 2008, U.S. Customs and Border Protection officers will no longer take verbal declarations of citizenship from U.S., Canadian, or Bermudian travelers as proof of citizenship at sea and land ports of entry. And by summer 2008, at a date to be subsequently announced, the Departments will implement the full requirements of the land and sea phase of WHTI.

A Notice of Proposed Rulemaking published in June 2007 proposes new documentation requirements for U.S. citizens and certain nonimmigrant aliens entering the U.S. by land or sea from within the Western Hemisphere. These documents include: a U.S. passport; a U.S. passport card; a trusted traveler card (NEXUS, FAST, or SENTRI); a valid Border Crossing Card; a valid Merchant Mariner Document when traveling in conjunction with official maritime business; or a valid U.S. Military identification card when traveling on official orders or permit. The NPRM also outlines ongoing efforts to provide other alternative documents.

Enhanced Driver's License Initiatives

To preserve travel, trade, and cultural ties with British Columbia and increase security at the Canadian border, the Washington State Department of Licensing will offer an Enhanced Driver License and Identification card (EDL/ID). The EDL/ID meets federal requirements and best practices for travel documents. It is an approved alternative travel document, to a U.S. Passport, for re-entry into the U.S. at land and sea borders between the U.S., Canada, Mexico, Bermuda, and the Caribbean.

The State of Washington and the Department of Homeland Security established a pilot program in March 2007. Citing the \$35 million in goods flowing both ways daily through the U.S.-Canadian border crossing at Blaine, Gov. Christine Gregoire said the law will help Washington keep the benefits expected to spill south from the 2010 Olympic Winter Games in Vancouver.

Canadian Minister of Public Safety Stockwell Day has said that the Canadian government is also developing a parallel enhanced driver's license system. Currently, Canadian citizens must present a passport to enter the U.S. without a visa.

The EDL/ID will be available beginning in January 2008. Participation is voluntary. The \$40 cost is \$15 more than a driver license or ID card. In-person application is mandatory and includes being photographed, being interviewed, and providing documents to prove U.S. citizenship, identity, and Washington State residence.

According to the Washington Department of Licensing, the following security enhancements are included in the EDL/ID:

- An icon on the front of the card to indicate that it is an EDL/ID.
- The back of the card will have a Machine Readable Zone, like the passport, that can be scanned at the border.
- Passive vicinity radio frequency identification (RFID) will be embedded in the card to facilitate rapid identification checks at the border.
- The RFID tag embedded in the EDL/ID will have a unique reference number and will not contain personal information.
- Data encryption, secure networks, and firewalls will protect the transmission of EDL/ID information.

Vermont Governor Jim Douglas and DHS Secretary Michael Chertoff signed an agreement in September 2007 that will allow Vermont to issue an enhanced driver's license and ID card (EDL/ID) to its residents to use for cross border purposes. Vermont plans to begin issuing the EDL/ID in late 2008. Like Washington, participation will be voluntary.

In announcing the program, the state motor vehicles department (DMV) stressed that the RFID tag embedded in the EDL/ID will have a unique reference number and will not contain personal or biographic information. Data encryption, secure networks, and firewalls will be used to protect the transmission of the EDL/ID information. The unique reference number will be matched to DMV records to verify the information contained on the front of the EDL/ID card. And for added security, the DMV will provide a security sleeve to protect the RFID tag from being read when the cardholder is not at a border crossing station.

In August 2007, DHS and Arizona Governor Janet Napolitano announced that the State of Arizona will partner with the Department of Homeland Security to launch a “3-in-1” driver’s license. The EDL/ID will meet the WHTI requirements, provide the state’s employers with a secure document to validate employee’s legal status, and satisfy future REAL ID requirements. In December 2007, Arizona signed an MOA with DHS confirming this arrangement and pledging future compliance with the requirements of REAL ID.

New York Governor Eliot Spitzer recently indicated that New York State will adopt an EDL but further details were not available at the time this report was being completed.

Existing Standards (Examples)

Driver’s Licenses / ID Cards

- Digital Image Exchange Program between state DMVs, congressionally funded through the National Highway Traffic Safety Administration
- [Final Rule: REAL ID, Minimum Standards for Drivers' Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; announced January 11, 2008](#) (row A3)
- [ANSI/NIST- ITL 1-2007, Data Format for the Interchange of Fingerprint Facial, & Other Biometric Information](#) (row E14)
- [AAMVA DL/ID Security Framework](#) (row G1)
- [Document Security Alliance Recommendations for Driver License Security and The REAL ID Act](#) (row G48)
- [ISO/IEC 18013, ISO compliant driving licenses, Parts 1-2](#) (G 131 and G132)

Passports

- [ICAO Doc 9303, Machine Readable Travel Documents](#) (G100)
 - U.S. passports comply with ICAO

Potential Gaps

Recommendation 1: Enhance the Security of the Issuance Process

- **Government agencies that issue identity credentials need to improve communication and cooperation among themselves as well as between the government and the private sector.** The challenges and debates surrounding The REAL ID Act notwithstanding, there needs to be improved communication and cooperation among credential-issuing agencies to enhance the overall integrity of issued credentials and to ensure that there is only one state driver's license / ID card issued per person.

9C. Working Group 1 – Commercial Issuance

The Problem

Identity thieves will employ various means at their disposal to fraudulently open new accounts, including impersonating other people, stealing the identity of a dead person and creating a fake identity. As commercial enterprises enroll individuals in a variety of programs involving financial services, healthcare, etc., they have certain resources available to them to prevent identity theft. In some cases, the private sector does not have access to government resources and greater compatibility would be desirable.

Discussion

Commercial enterprises issue commercial account cards (e.g., ATM cards, credit cards, phone cards, health insurance cards, etc.) that provide consumers the ability to acquire financial products and services, mobile communications, healthcare services, etc. Commercial enterprises also issue, collect and retain information-based credentials (e.g., user ids / passwords, PINs, responses to challenge questions, etc.) which enable consumers to obtain products and services electronically or online.

Validation of identity documents

The face-to-face process for obtaining commercial identity credentials typically relies upon the presentation of a driver's license or ID card and possibly other "breeder" documents (e.g., birth certificates and Social Security cards) as the form of proof of the applicant's identity. However, the issuance process does not always include authentication of the documents presented by the applicant. Even in cases where a notary is required to be involved in the issuance process, i.e., to observe an individual executing a signature on an identity application, for example, to obtain a healthcare card in some states, the notary generally does not have the legal obligation to, and accordingly will not, actually validate the authenticity of the identity documents to support the identity claims.

Since the passage of the USA PATRIOT Act, the regulatory rules and guidelines have required the presentation and verification of I-9³² documents to be used in the vetting process prior to the establishment

³² In the employment context, the Department of Homeland Security's U.S. Citizenship and Immigration Services has issued the Employment Eligibility Verification Form (I-9) to verify identity and eligibility for employment in the U.S., in accordance with the Immigration Reform and Control Act of 1986. The I-9 form describes various documents that are acceptable for these purposes. Other sectors including the financial services sector have come to rely on these "I-9 documents" in account opening and the issuance of credit.

of a new financial services account or the issuance of credit. Private online service providers are available to verify Social Security Numbers and driver's licenses. However, a valid I-9 document used fraudulently by another individual may fail to be recognized as such unless the proper owner of the identity document has reported such document as being lost or stolen.

Red Flags

Identity abuse has prompted the financial regulatory agencies to issue regulations under the Fair and Accurate Credit Transactions (FACT) Act that require financial institutions and creditors to implement programs to detect, prevent and mitigate identity theft in connection with the opening of an account or any existing account. The multiple regulatory agency joint final rules and guidelines (row A5) identify 31 patterns, practices, and specific forms of activity that indicate a possible risk of identity theft. The regulations require financial institutions and creditors to incorporate into their programs relevant indicators of a possible risk of identity theft called "Red Flags." A "Red Flag" is defined as a pattern, practice, or specific activity that indicates the possible risk of identity theft.

Thus, a financial institution or other creditor should consider whether, for example, a reasonably foreseeable risk of identity theft may exist in connection with business accounts it offers or maintains that may be opened or accessed remotely, through methods that do not require face-to-face contact, such as through the internet or telephone. In addition, those institutions and creditors that offer or maintain business accounts that have been the target of identity theft should factor those experiences with identity theft into risk assessment.

Other ways to curb identity theft

A number of means currently exist which may be used by organizations to curb identity theft:

- Utilize fraud alert systems:
 - Require new account issuers to check for fraud alerts and red flags. There are a variety of fraud alert and notification systems (e.g., credit reporting, returned checks).
- Perform address validation at the time of account opening by utilizing the web catalog of address verification tools of the U.S. Postal Service and credit reporting systems where prior consumer addresses are maintained. Perform address verification when a change of address notification or a request for a replacement card is received, for existing accounts wherein the existing account holder is notified of such a change request to the address on record.
- Create means for consumers to control when their personally identifiable information (PII) is disclosed.

- Expand use to the private sector of the NAPHSIS Electronic Verification of Vital Events (EVVE) system for birth and death records.
- Use a hierarchy of authentication processes based upon risk:
 - Increase security levels to afford higher performance security identification tokens (digital signature certificates, biometrics).
 - Use third parties to perform “face-to-face” authentication with verification of government-issued identity documents (e.g. Post Office, private sector firms).
- Use anti-counterfeiting tools and devices on identification documents (holograms, intelligent bar codes).
- Rely on state vital statistics, especially death records, in the credit review and issuance process.

An emerging concept gaining wide attention in the online world is digital identity transactions using managed Information Cards³³ wherein an individual utilizes trusted identity providers to issue claims on his or her behalf. Relying parties (e.g., employers, financial and health care service providers) then obtain a security token from the identity provider containing claims used to authorize the relying party’s decision to extend goods or services to the individual. The concept is based upon open standards based architecture, is platform independent, and is planned to be demonstrated by the British Columbia government in 2008.

Existing Standards (Examples)

The following are some examples of existing standards, guidelines, rules and systems that relate to the issuance of identity credentials in the commercial context:

- [FFIEC Guidance on Authentication in an Internet Banking Environment](#) which mandates that financial institutions perform a risk analysis and implement security measures that do not rely solely on the use of single-factor authentication based on passwords or PINs for the protection of high-risk transactions involving access to customer information or the movement of funds to other parties (row E6).
- [ANS X9.8 Banking- Personal Identification Number \(PIN\) management and security, Part 1](#) is a standard for the issuance, delivery and use of PINs at ATM and Point-of-Sale terminals in an interchange environment (row G14).

³³ *Windows CardSpace* is Microsoft’s implementation of an Information Card client. Novell’s CardSpace-compatible *Digital Me* client is available for MacOS and Linux, as well as compatible software from dozens of other vendors and projects.

- [American Bankers Association Industry Resource Guide, Identification and Verification of Accountholders](#) is an industry guideline which stipulates the requirements for I-9 document presentation and the validation of the I-9 document prior to the establishment of a new account (row G4).
- [ID Theft Red Flags and Address Discrepancies Rule \(October 31, 2007\)](#) are regulations to detect, prevent and mitigate identity theft in connection with the opening of certain accounts or changing the address of existing accounts (row A5).
- [OpenID](#) is a way for individuals to create identity online with a trusted Identity Provider. OpenID is a decentralized framework for user-centric digital identity which uses existing internet security technology that enables a user to control what pieces of information they wish to share with their Identity Provider such as name, address, or telephone number (row G223).
- [Registered Traveler program](#) – The Transportation Security Administration (TSA) and private industry developed the Registered Traveler program to provide expedited security screening for passengers who volunteer to undergo a TSA-conducted security threat assessment in order to confirm that they do not pose or are not suspected of posing a threat to transportation or national security.

Potential Gaps

Recommendation 2: Augment Private Sector Commercial Issuance Processes

- **Government and industry need to open a dialogue about how to facilitate greater interoperability between public and private sector ID theft prevention mechanisms, with the focus being on strengthening the integrity of the issuance process. This dialogue would include, among other things, providing the private sector appropriate and secure access to government vital record systems.**

There are concurrent vertical industry specific and government attempts to implement programs to detect, prevent and mitigate identity theft. There is a question of whether there should be interoperability between the government solutions and the private sector initiatives. While technically interesting and possibly achievable, there lies a larger social issue of personal privacy and the need for interoperability, and the extent of the use of PII by the private sector. Herein lies the gap in the issuance of commercial identity documents.

There is also the issue of interoperability between different forms of “commercial” identity.³⁴ For example, employer-issued picture identification documents utilize state of the art technology; however, such documents may use a variety of standards (digital images, biometrics, IRD, chip), and so the documents are not interchangeable or interoperable with other companies, nor are they accepted forms of identification for retail and government use. Application-specific identity documents (e.g., private label credit cards, ATM cards, health card provider cards) likewise do not traverse the market as acceptable forms of identification beyond the specific application for which they are intended.

Three key factors determine the capability and sufficiency for identification documents to be truly interoperable across commercial and governmental organizations:

1. Physical characteristics – identification cards, credentials, and documents need to be able to support common standards for physical topography (e.g., picture, printed information, color and printed features) and security features (e.g., hologram, laser etching, microprinting, watermarks, optically variable ink) so that authenticity can be determined for attended authentication use cases.
2. Electronic data exchange – identification documents with data storage capability (e.g., integrated circuit chip “smart” cards) need to support common data model and data interface standards so that data recorded on the documents can be exchanged and read by multiple devices to support electronic authentication use cases.
3. Trust – The identity management policies and practices of document issuing organizations need to support standards for identity verification and vetting, identity binding and management for inter-organizational trust to support any authentication use case.

The degree of interoperability between government solutions and private sector initiatives needs to be further explored and discussed by representatives of each sector. There are inherent tradeoffs between the needs of law enforcement and the private sector with respect to their use of personally

³⁴ A related issue is the lack of interoperability between certain forms of government-issued identity credentials. For example, the content of the information that constitutes an ID / ID credential and the failure of major issuers of ID documents to adopt naming conventions.

identifiable information, the need to protect such data and personal privacy, and the need for interoperability.

Private sector access to government vital record systems

The private sector relies upon multiple forms of I-9 documents for face-to-face vetting in account opening and the issuance of credit. But there is an interoperability gap when the issuance process involves online verification in the private sector. Vital records and driver's licenses are created and maintained by each state, and government-to-government vetting processes have networks whereby birth record data (EVVE) and driver's license data (Digital Image Exchange Program) are available to the document-issuing state agencies but not directly to the private sector. This Panel believes the commercial online vetting process potentially could benefit from appropriate and secure access to government vital record systems. It recognizes that the use of government vital record systems has a social impact if image data is made available to the private sector for use in making risk avoidance decisions. The interests of law enforcement and consumers' expectations with respect to the protection of personally identifiable information and privacy need to be considered as well. These issues need further discussion.

9D. Working Group 1 – Security of the Issuance Process

The Problem

Online and off, attention needs to be given to the actual processes associated with enrolling a person in an identity system, issuing an identity credential and conveying that credential to the correct person. That is, assuming that an organization has sound procedures for verifying the identity assertions of a person seeking enrollment, can a person by-pass those verification procedures and still create an identity or obtain an identity credential? For example, employees can be bribed or can otherwise collude with persons seeking identity credentials to which they are not entitled, and criminals may steal or otherwise obtain without authorization the blank cards and the equipment for manufacturing the cards. (The next section addresses a related problem, which is the security of the credentials themselves – how easy is it to forge or alter a credential. Here the problem is whether a person can obtain a credential by exploiting vulnerabilities at the point of issuance.)

Online identity processes may face similar vulnerabilities to insider fraud. While the absence of human interaction may decrease the risk of collusion, online processes face the risk that a hacker can obtain remote access to ID creation processes. One of the worst forms of computer security breach is when a hacker obtains administrator status, for he can then create new accounts and issue identity credentials to himself or others.

A third security problem associated with the issuance process is that, to create an identity, an applicant often must disclose identifying information, in order to prove his claim of identity and his eligibility for the issuance of credentials. As a result of this process, however, the issuer becomes the custodian of additional identifying information, and thus becomes responsible for the security of this information. For example, the improvements in the issuance of driver's licenses mandated by The REAL ID Act require state motor vehicle departments (DMVs) to collect and store copies of foundational documents such as birth certificates. DMVs then become responsible for protecting these records against unauthorized access and use.

A fourth set of problems involves the delivery of the credentials once issued. For example, when the US mail is used to deliver passports, it is important to ensure that the passport is not diverted from the mail stream or stolen, for example, from the intended recipient's mailbox before he can receive it. Similar risks are associated with the delivery of credit cards or checks. In the online context, spyware and other exploits

can intercept passwords and other credentials as they are being generated or transmitted from the issuer to the user.

Discussion

As in other areas, security here involves risk management: identifying risks and developing solutions to mitigate them, recognizing that there are trade-offs of effectiveness, cost and convenience. Defenses fall into four categories: physical security; technical (logical) security; personnel security; and administrative (business) processes. Solutions include:

- Limiting access (logical and physical) to the issuance process;
 - limiting how many employees can create identities and issue credentials;
 - facilities security – hardening physical locations and controlling access to the physical space where credentials are issued;
 - computer security;
- Protecting production equipment from unauthorized use or theft;
- Securing card stock against loss.

An important aspect of solutions concerns personnel security, ranging from background checks on employees involved in the issuance process to effective supervision, including, for example, monitoring of offices and employees and auditing and accounting mechanisms to deter and detect off-the-books issuance. For example, one stated goal of the federal government’s Personal Identity Verification (PIV) standard (row E16) is that “a single corrupt official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential.”

Other solutions involve the careful design and consistent implementation of business practices for the issuance process. One approach is to fragment the issuance process with access controls, limited authority, and checks built in, so that one person cannot manipulate the system. Centralized solutions may pose trade-offs in terms of customer convenience.

The problems and the solutions have an unavoidable circularity. For example, to prevent substitution (delivery of the credential to someone other than the person who underwent the identity proofing process), it may be necessary to perform a mini-verification process at point of delivery. That is, to complete delivery of an ID credential, the recipient may have to prove his identity using a different credential.

Existing standards (Examples)

These issues have been addressed in a number of standards of general applicability including those listed below.

- The ISO 27000 series of standards relates to information security matters. [ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management](#) establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization, providing general guidance on the commonly accepted goals of information security management (row G146).
- The North American Security Products Organization has issued [ANSI/NASPO SA v3.OP-2005, Security Assurance Standards for the Document and Product Security Industries](#) (row G217).

Driver's Licenses

The final regulations for implementation of The REAL ID Act address five issues associated with the security of DMV facilities where driver's licenses and identification cards are manufactured and produced:

1. Background checks for certain employees;
2. Physical/logical security;
3. Document security features on driver's licenses and identification cards;
4. Security of information stored in the DMV database;
5. Security of personal data and documents collected and managed under the Act.

See [Final Rule: REAL ID, Minimum Standards for Drivers' Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; announced January 11, 2008](#) (row A3).

Other resources on the driver's license / ID issuance process include:

- [AAMVA DL/ID Security Framework \(February 2004\)](#) - This document deals with internal controls within the environment of the driver's license / ID issuance processes, with a view to providing jurisdictions with information about current best practices and recommending specific actions with respect to this business process. Appendices address a range of issues in greater depth. An appendix on issuing systems describes security practices for over-the-counter, centralized and hybrid systems (row G1).

- [Document Security Alliance Recommendations for Driver License Security and The REAL ID Act](#) (row G48).
- [ANSI/NASPO SAV3.OP-2005, Security Assurance Standards for the Document and Product Security Industries](#) (row G217).

Financial Services

The financial services sector has a robust set of security standards addressing information security in general and ID processes and information in particular, including:

- [X9.49-1998, Secure Remote Access to Financial Services for the Financial Industry](#) (row G22).

U.S. Postal Service

The [Mailing Standards of the US Postal Service Domestic Mail Manual](#) (row E38) include requirements regarding mail receptacles, conditions of delivery and other Recipient Services found in Section 508.

Potential Gaps

Recommendation 1: Enhance the Security of the Issuance Process

- **Government and industry should expeditiously open a dialogue about the cross-application and implementation of existing security standards to identity issuance processes, and discuss the potential cross-functioning of new standards development, where deemed appropriate.**

There are generally applicable information security management standards that may be useful reference documents for constructing stronger security programs for identity issuance processes.

These include the ISO/IEC 27000 series of standards on information security and the North American Security Products Organization (NASPO) Security Assurance Standards for the Document and Product Security Industries (ANSI/NASPO Sav3.OP-2005). There are also sector-specific standards that may have cross-relevance to other sectors. Some examples of publicly available, comprehensive guides and standards that can serve as a reference model for new identity issuance security programs include the American Association of Motor Vehicle Administrators *DL/ID Security Framework*, the *HSPD-12 Personal Identity Verification Program*, and the Australian *National Smartcard Framework* (row F1).

- **Government and commercial issuers of identity credentials should give further attention to problems associated with secure delivery methods of such credentials to the end user.** One area that may require additional attention is the interface between the issuer and the recipient. In particular, further work may be needed on problems associated with delivery of credentials, both online and offline.

9E. Working Group 1 – Credential Security

The Problem

The incidence of forging, counterfeiting and altering identity credentials varies widely from credential to credential. Some birth certificates have low counterfeit and alteration resistance and some are so lacking in basic security features that professional document examiners often reject genuine certified copies believing them to be fake. At the other end of the spectrum we now have the passport loaded with traditional document security and data protection features that now has the added protection of an embedded RFID chip and data encryption. Most driver's licenses fall somewhere in between. The new Enhanced Driver License and Nexus border crossing card³⁵ are the first to feature built in electronic security and biometric technology.

The problem faced by all physical credentials is that the bulk of persons who examine and authenticate them lack both the knowledge and/or special instruments required to properly authenticate. Seasoned fraudsters, of course, know this and trade on it to the extent that they match the fidelity in their fakes to the likelihood of getting caught. They know that they can easily fool certain socio-economic/demographic groups but not a highly trained expert examiner at the airport. For this reason, all modern ID credentials use a layered document security approach in an attempt to cater to the general public as well as lightly and highly trained expert examiners. On top of this, both government and commercial issuers of ID credentials tend towards an overall strategy that is aimed as much at fraud prevention as fraud detection.

To pose as another real person (who has likely been carefully selected) the identity thief must either:

- a) alter the other person's genuine ID credentials that have been stolen;
- b) fully counterfeit the other person's credentials;
- c) cannibalize parts of other stolen but genuine credentials to build the other person's set of credentials;
- d) use a deceased person's identity.

To create a fictitious identity (in order to hide true identity) the identity fraudster, who must avoid contact with the authorities, can use any of the above methods to craft a set of new false identity credentials.

³⁵ NEXUS is designed to expedite the border clearance process for low-risk, pre-approved travelers into Canada and the United States. The Canada Border Services Agency (CBSA) and United States Customs and Border Protection (CBP) are cooperating in this joint venture to simplify border crossings for members, while enhancing security.

The challenge that ID credential authorities face is to create a set of preventative countermeasures that combine with high levels of counterfeit and alteration resistance within the credentials to deter and, if it happens, to easily detect the fraud at points of inspection or transaction.

To do this, ID credential authorities face the problem of limited budgets, often a lack of document security expertise and resources, wide security technology choices, no objective methods of measuring security technology effectiveness (in advance of investing in it) and no way of objectively calculating return on investment (ROI).

Discussion

Solutions to all of the problems facing the government ID credential authorities are in the making in one form or another. Problems with the birth certificate are the subject of ongoing work by the National Center for Health Statistics (NCHS) who are required to respond to Section 7211 of the Intelligence Reform and Terrorist Prevention Act (IRTPA) with new minimum counterfeit and alteration resistance standards but have not yet done so. NAPHSIS is working with NCHS to resolve birth certificate problems. Problems with the Social Security card are the subject of ongoing work by the Social Security Administration (SSA) which is required to respond to Section 7213 of the IRTPA also with new minimum counterfeit and alteration resistance standards. The passport travel document has recently undergone a radical upgrade under the auspices of the International Civil Aviation Organization (ICAO) with the addition of an RFID chip embedded in the cover and is currently not the target of any new regulation. State issued driver's licenses and ID cards (DL/ID Cards) on the other hand are the subject of the most intense scrutiny by the Department of Homeland Security (DHS) which has responded to The REAL ID Act with the formulation and conversion into regulation of new minimum standards for the prevention and detection of DL/ID card fraud. A link to its final regulations for DL/ID card security can be found in the IDSP Standards Inventory.

Expert advice in all of the above areas has come from several organizations including the Document Security Alliance whose white papers on each credential are also referenced in the IDSP Inventory. NAPHSIS has contributed to and supported the work of NCHS, and their white paper on how to solve the birth certificate fraud problem is also referenced in the IDSP Inventory. AAMVA has contributed heavily to the work of DHS on the DL/ID cards and a summary of the overall status of the DL/ID card prepared by AAMVA can be found earlier in this report under the heading of Subsequent Credentials. In addition, AAMVA has created a common unique identifier in the form of a 3D hologram for use on all U.S. and Canadian DL/ID cards.

Unfortunately, uncertainty concerning the final requirements of The REAL ID Act has caused most states to defer use of this valuable feature pending the outcome of final rulemaking.

Noteworthy in the DHS final REAL ID Act regulation is the possibility of requiring all DL/ID card issuers to subject their card credentials to adversarial testing to prove to DHS (in advance of issuance) that the ability of their design will resist compromise and document fraud attempts. Unfortunately, laboratories that perform adversarial testing of this form are few and no published or even restricted access standards are known to exist that DHS was able to reference. In an attempt to close this gap, the DSA and NASPO (North American Security Products Organization) have formed a joint steering committee and recently issued a draft plan for the development of methods to objectively evaluate the effectiveness of document security technologies. This work is being carried out with a view to establishing a much needed American National Standard in this area that will address the ROI problem cited earlier.

ID credential authorities have an abundance of traditional and newer overt and covert security technologies to help deter and detect fraud. New, however, are technologies that literally enable anyone to check the authenticity of a credential (or any other item or product) and in some cases be able to obtain information in real time about security features and other attributes to look for. These anti-counterfeiting technologies are based upon the printing (or laser engraving) of secure serialization codes on an identity document and are now the subject of standards work in North America jointly by NASPO, the Semiconductor Industries Association (SIA) and Semiconductor Equipment and Materials International (SEMI) and separately in Europe by CEN, the European Committee for Standardization. These technologies are a strong preventative countermeasure that can be easily verified via use of cell phones and the internet.

Existing Standards (Examples)

Based upon an examination of existing standards and guidelines with respect to the security of physical credentials (e.g., counterfeit resistance, alteration resistance, tamper evidence, etc.), the following documents are among those believed to be relevant:

Birth Certificates

- a) Forthcoming rulemaking by NCHS in response to Section 7211 of the IRTPA
- b) [DSA White Paper: Formulation and Definition of Birth Certificate Minimum Standards](#) (row I3)
- c) NAPHSIS White Paper: Recommendations for Improvements in Birth Certificates (row I6)

Social Security Cards

- a) DSA White Paper: Formulation and Definition of Social Security Card Minimum Standards (row I4)
- b) Forthcoming definition by SSA of minimum standards for Social Security Cards in response to Section 7213 of the IRTPA

State Issued Driver's Licenses & ID Cards

- a) [Final Rule: REAL ID, Minimum Standards for Drivers' Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; announced January 11, 2008](#) (row A3)
- b) [AAMVA Personal Identification - AAMVA International Specification - DL/ID Card Design \(2005\)](#) (row G2)
- c) DSA Discussion Paper: Regarding The REAL ID Act, Secure ID Documents and Related Security Processes
- d) AAMVA fraudulent document recognition training curriculum, which satisfies the requirements of the final rule implementing The REAL ID Act (row G3)

Passports

- a) International Civil Aviation Organization (ICAO), Technical Advisory Group on Machine Readable Travel Documents: [Machine Readable Travel Documents standard](#), ICAO Doc 9303, endorsed as ISO/IEC 7501 (G99)

Potential Gaps

Recommendation 3: Improve the Integrity of Identity Credentials

- **The Document Security Alliance (DSA) and North American Security Products Organization (NASPO) should proceed as soon as possible with their project to measure the Effectiveness of Document Security Technologies.** Although there are an abundance of document security technologies available to help prevent and detect ID credential fraud, no standards exist to address the measurement of their effectiveness. DSA and NASPO have jointly begun an effort in this area, and have just released a draft project plan for review within NASPO and the DSA.
- **The Department of Homeland Security (DHS) should work with issue stakeholders to develop Adversarial Testing Standards for identity credentials.** There are no published standards related to the critical need to perform adversarial testing of driver's license / ID credentials which may be required by DHS, as indicated in The REAL ID Act final regulations. DHS has indicated its willingness to work with stakeholders to develop performance standards and a methodology for adversarial testing.
- **The North American Security Products Organization (NASPO), the Semiconductor Industries Association (SIA) and Semiconductor Equipment and Materials International (SEMI) in North America -- as well as CEN in Europe -- should expeditiously proceed with their standards work on Secure Serialization Anti-Counterfeiting Technology as a preventative countermeasure.** This Panel believes that the emerging Secure Serialization Technology looks very promising as a preventative countermeasure to ID credential fraud. An industry standard is in development in North America by NASPO, SIA and SEMI, and the European standards authority (CEN) has just launched a similar effort in response to European demand.

10A. Working Group 2 – Fraudulent Use of “Perceived” Secret Information

The Problem

Reliance on perceived secret information for authentication

One of the prime enablers of identity theft is the use of personal information by an identity thief to impersonate someone else. Identity theft arises in these cases because of business practices that treat easily-obtainable personal information as authenticators of someone’s claimed identity. One common way that organizations authenticate a person’s identity is to see if they know a shared secret, such as a password. If an ID thief discovers a shared secret, he or she may be able to replay that information, impersonate that individual, and commit some type of fraud. For example, an ID thief who discovers the right personal information could gain access to an existing account, create a new account, commit employment fraud, or illegally get medical services.

Some information used for authentication is not as secret as some people think. A good example is the use of Social Security Numbers (SSNs). Many SSNs and other personal information used for authentication have unfortunately fallen into the hands of ID thieves and can be found for sale on websites that cater to criminals. The weight SSN plays in authentication should be tempered by this potential breach of secrecy. Additional credentials and factors should be considered.³⁶

Techniques used by ID thieves to gather credentials range from online methods like phishing scams and spyware, to offline methods like dumpster diving and snatching laptops. Targets include businesses and consumers. Data breaches that occur at businesses and government agencies may also result in thieves gaining access to sensitive personal information. Consumers also fail to secure confidential data in their home making it easy for an insider such as a relative to steal their secrets. Others are overly trusting and may divulge their secrets over the phone to a convincing attacker.

³⁶ There is a related legal issue regarding the use of SSNs for authentication in that California and some states have statutory restrictions and storage requirements relating to SSNs.

Reliance on Single Factor Authentication based on shared secrets to access existing accounts

Relying only on what a person knows (single factor authentication) makes it easy for ID thieves to attack from a distance (e.g. via phishing). These thieves do not have to mug a person to steal a physical token (something they have) or present a fingerprint (something they are). They just need to trick the person into divulging their shared secrets or otherwise steal the information from a data custodian. While knowledge of personal information may be part of an overall authentication process, stronger methods may be needed to prevent this knowledge from being used for identity theft.

Discussion

Authentication – General

Effective authentication lowers the risk of a company or a consumer becoming a victim of identity theft. Discussion of “the acceptance and exchange of identity information” ultimately focuses on the question of what constitutes effective authentication of a consumer across many different types of industries, accounts, services, transactions and communication channels. Some key points emerge:

- There is no single “right answer” for authentication. What may be effective for online transactions may not be appropriate for an in-store authentication where personal data may be exchanged with a clerk. Similarly, what may be required for one industry sector, may not apply to other sectors. For example, the financial services sector has a range of authentication requirements imposed on it, while other sectors like telecommunications providers and utilities do not have the same requirements.
- As authentication systems and practices evolve, so, too, will the systems and practices of identity thieves of various levels of sophistication. There is a need for ongoing vigilance and dialogue.
- Government and private sector resources for thinking about authentication abound. For example, the Federal Trade Commission hosted a productive workshop on authentication on April 23-24, 2007 which helped summarize views regarding authentication without forcing a particular conclusion. The FTC also held a workshop on December 10-11, 2007 on SSNs and ID theft. In February of 2005, the Department of the Treasury published a report entitled “The Use of Technology to Combat Identity Theft” which at the time was a good summary of the state of play with regard to biometrics.

- Greater use of effective authentication systems will likely lead to less identity theft.
- Consumers need to be educated about ID theft scams and how to protect their personal information. Building on existing FTC initiatives, consumer education should remain a priority.

Use of Social Security Numbers for Authentication

Of particular concern is the use of Social Security cards or the SSN as a single-match authenticator. There is no indication that the Social Security Administration (SSA) is headed towards a real-time validated card which is hardened against forgery and alteration. Furthermore, the SSN was not originally intended to authenticate identity and the Social Security Act does not permit the SSA to allow private sector access to its database for most authentication purposes. While the SSN has become a useful tool as part of the private sector fraud prevention arsenal, it is not reliable as a single-match authenticator to prevent identity theft.

To the extent that the SSN continues to be used as part of an authentication scheme, it would be useful if the SSA provided validation of an applicant's SSN in combination with their name. That would help to properly process applications and also would help to determine whether or not the SSN had been used in previous fraudulent applications.

Beyond Single Factor Authentication

Focusing authentication on any single data element or credential will lead identity thieves to deploy the entirety of their resources to finding a work around. Multi-factor authentication provides the parties greater confidence in who they are transacting with. To the extent possible, authentication should be mutual. For example, if consumers were able to also verify who they are dealing with over the Internet, it could reduce their chances of being tricked into divulging sensitive information to ID thieves.

The challenges associated with identity verification can be mitigated by multi-factor, mutual authentication using tokens, public key infrastructure (PKI), biometrics, and risk-based authentication that depend on monitoring various attributes of the authentication session. This approach depends on the prior issuance of these tokens by some trusted third party to someone whose identity has been initially verified or "proofed" using methods such as knowledge-based authentication (KBA) and others. Examples of trusted third parties that might issue such credentials include banks and other financial institutions, motor vehicle bureaus, post offices, and credit bureaus, and issuers of digital certificates.

Existing Laws, Regulations, Standards, Guidelines, and Best Practices (Examples)

The following are examples of some of the laws and regulations that provide guidance addressing these issues:

- [Fair and Accurate Credit Transactions Act of 2003 \(FACTA\)](#) (row A12)
 - Red Flags Rule (row A5)
- [USA PATRIOT Act – Section 326 Customer Identification Program \(CIP\) Regulation](#) (row A6)
- FCC Privacy Rules To Prevent Pretexting (row A7)
- [GLBA](#) (row A14)
- [HIPAA](#) (row A15)

Examples of existing standards that provide useful guidance include:

- [FFIEC Guidance on Authentication in an Internet Banking Environment](#) (row E6) and [FAQs](#) (row E7)
- American Bankers Assn. [Industry Resource Guide, Identification and Verification of Accountholders, January 2002](#) (row G4)
- [Guidelines for Extended Validation Certificates, October 20, 2006](#) (row G43)
- ISO 9798-1, Entity Authentication, Part 1: General (row G109)
- US Postal Service In-Person Proofing at Post Offices Program (row E37)
- Anti-Pretexting Working Group Best Practices for Authenticating Requests from Purported Customers Related to Call Detail Records (row G8)

Potential Gaps

Recommendation 4: Strengthen Best Practices for Authentication

- **When determining an appropriate authentication procedure, financial institutions and other credit grantors should take into account level of risk, cost and convenience considerations.**

Best-practices for the use of various authentication options should depend on several considerations, including the type of application (opening a new account versus access to an existing account), interface type (in-person, online, or telephone), and level of risk. Cost and convenience should be proportional to risk: simplistic data matching for low valued transactions; more rigorous authentication procedures when the stakes are higher. For example, a consumer should not have to have an iris scan to buy gas, but having to enter a zip code is a reasonable extra step. New Account Openings should be considered high risk, as new account fraud typically is more difficult for victims to detect than fraud with existing accounts. New Account Opening fraud is also potentially more damaging, in that a new line of credit is extended, with a corresponding new record with the credit bureaus.

- **Additionally, financial institutions and credit grantors should *not* use easily-obtainable personal information (such as Social Security numbers) as the sole authenticators.** A range of alternative authentication tools exist, and need to be employed on a more widespread basis than the current marketplace reflects. These include tools such as:

- Knowledge-based authentication that relies on harder-to-obtain answers to “out-of-wallet” questions.
- Use of trusted third-party identity providers.
- Fraud alerts that require direct contact and authorization from the person whose identity information is being used.

- **The federal financial regulatory agencies and the Federal Financial Institutions Examination Council (FFIEC) are encouraged by this Panel to further review the sufficiency of current authentication practices for online banking.** The *FFIEC Guidance on Authentication in an Internet Banking Environment* says that banks must do something better than using single factor authentication based on passwords for "high risk" transactions involving access to customer information, or movement of customer funds to other accounts. Multi-factor authentication is not

specifically mandated in such cases but it is one of several methods recommended to be used to mitigate risk, along with layered security (which would include mutual authentication). Ultimately, decisions on authentication are left to the banks to decide based on the results of a risk analysis.

- **Industry and standards developers should continue to develop and promote the use of specific trusted networks for multi-factor mutual authentication.** The infrastructure of trust networks between credit grantors (“relying parties”) and credential issuers (“identity providers”) continues to evolve. Recent advances across the industry, such as the development of the Web Services Security Standards (which support the Identity Metasystem and Information Cards), the Security Assertion Markup Language (which supports the Liberty Identity Federation Framework), and the Liberty Identity Assurance Framework may one day enable widely available “authentication networks” that could make this ideal a reality.

10B. Working Group 2 – Inadequate Validation of Credentials

The Problem

Inadequate validation of physical credentials

Inadequate validation of physical credentials has been identified as a major cause of identity theft. For example, credentials such as a driver's license, Social Security card, and other identity documents can be faked by criminals if the credentials are not sufficiently secure and easily verifiable with the issuing authority. Criminals also can create new forged credentials using stolen information which enables them to commit several forms of identity theft such as financial (or credit-based), medical, criminal, and employment identity theft. The ability to fake these credentials allows criminals access to existing accounts.

Authentication of a consumer who has placed a fraud alert

ID thieves also may seek to open new accounts by pretending to be another individual using physical credentials and/or acquired information. This prompted some questions and concerns regarding the process of how consumers who have placed a fraud alert are validated by creditors. A discussion of this issue in the context of overall "red flags" follows below.

Discussion

Fraud Alerts

Fraud alerts can be an effective safeguard in helping consumers to protect themselves from identity theft by enabling them to control when credit will be extended in their name. The 2003 Fair and Accurate Credit Transactions (FACT) Act amendments to the Fair Credit Reporting Act (FCRA) dictate what credit reporting agencies must do regarding fraud alerts. For a fraud alert to work, it must be considered as part of the process of authenticating identity.

To set some context, approximately 3.5 million fraud alerts, the vast majority of which are 90-day initial alerts, are placed each year. A total of 3 billion consumer credit reports are produced each year and thus the vast majority of transactions involving use of a consumer credit report do not involve a fraud alert at all (0.12% of all transactions).

Although initial 90-day alerts are tied to "...a suspicion that the consumer has been or is about to become a victim of fraud or related crimes, including identity theft," anyone can place a 90-day alert on their credit file. An initial alert is not a definite assertion of identity theft in all cases, but should be considered in the context of other identity authentication processes. For credit reports containing initial alerts, the FCRA requires the recipient to either contact the consumer at the telephone number provided in the alert, or to take other reasonable steps to confirm the consumer's identity.

It is only in the case of an extended 7-year fraud alert (i.e., where identity theft has happened), that the FCRA contains a strict requirement for the recipient of an alert to contact the consumer to confirm that the application for credit is not the result of identity theft.

Red Flags

On October 31, 2007, the federal financial institution regulatory agencies and the Federal Trade Commission sent to the Federal Register for publication joint final rules and guidelines on identity theft "red flags" and address discrepancies (row A5).³⁷ The final rules implement sections 114 and 315 of the FACT Act of 2003. The final rules are effective on January 1, 2008 and covered financial institutions and creditors³⁸ must comply by November 1, 2008.

The FACT Act addresses a range of identity theft prevention processes which are risk-based. The aforementioned "red flags" include managing address discrepancies, using third-party data sources, and identifying suspicious personal identifying information and suspicious documents. Fraud alerts and other warnings received from consumer reporting agencies or service providers, such as fraud detection services are also covered by the rule. The rule reinforces a key point which is that no one red flag, including the presence of an initial fraud alert, is likely to be definitive with regard to the status of an application. A range of tools should be used to prevent identity theft.

³⁷ <http://www.federalreserve.gov/newsevents/press/bcreg/20071031a.htm>

³⁸ The red flag rules have broad applicability to almost any type of entity that extends credit and requires these entities to establish written identity theft prevention programs.

Existing Laws, Regulations, Standards, Guidelines, and Best Practices (Examples)

The following are some examples of applicable requirements and guidance to address the problem of inadequate validation of credentials:

Laws and Regulations

- [USA PATRIOT Act – Section 326 Customer Identification Program \(CIP\) Regulation](#) (row A6)
- [Final Rule: REAL ID, Minimum Standards for Drivers' Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; announced January 11, 2008](#) (row A3)
- State credit freeze laws (row C3)
- Red Flags Rule (row A5)
- [FACT Act](#) (row A12)

General Standards, Guidelines and Best Practices

- [FFIEC Guidance on Authentication in an Internet Banking Environment](#) (row E6) and [FAQs](#) (row E7)
- [Social Security Administration's Death Master File](#) (row E34)
- American Bankers Assn. [Industry Resource Guide, Identification and Verification of Accountholders, January 2002](#) (row G4)
- [Guidelines for Extended Validation Certificates, October 20, 2006](#) (row G43)
- [ICAO Doc 9303, Machine Readable Travel Documents](#) (row G100)
- US Postal Service In-Person Proofing at Post Offices Program (row E37)
- Anti-Pretexting Working Group Best Practices for Authenticating Requests from Purported Customers Related to Call Detail Records (row G8)
- [ANSI/NASPO SA v3.OP-2005, Security Assurance Standards for the Document and Product Security Industries](#) (row G217) and NASPO Certification to this standard (row J3)

Potential Gaps

Recommendation 4: Strengthen Best Practices for Authentication

- **The public and private sectors need to start a process to work collaboratively to implement systems that allow physical identity documents to be validated in real time.** Systems are needed to verify *in real-time* that physical credentials presented at the time of a transaction (such as a driver's license, Social Security card, or other government-issued ID) are valid and pertain to the person presenting them. For example, a system that would allow a company to review a driver's license, submit a query to authenticate that the document is the original and not forged, and verify that it is tied to that consumer.

- **The Federal Trade Commission (FTC) and the federal financial regulatory agencies should provide guidance on best practices for credit grantors responding to fraud alerts.** The Fair and Accurate Credit Transactions Act (FACT) Act dictates what credit reporting agencies must do regarding fraud alerts, and the red flag rules and guidelines provide further identity theft prevention guidance to financial institutions and other creditors. *What may be missing* is a review of Best Practices that can be used by credit grantors to clear a fraud alert under likely scenarios that may arise when credit grantors attempt to contact someone *to verify the authenticity of a request for credit*. This would encompass employee training and the execution of the process around employee training at credit lenders. For example, a concern was raised as to how creditors will confirm a consumer's identity as a practical matter. Suppose a creditor calls a particular phone number belonging to the person whose credit history/score has been accessed by the credit grantor. What should the credit grantor do if the phone number called does not answer? How many times should the credit grantor call again? Should the credit grantor assume that whoever answers the phone is the person who it is seeking to contact, or should it take additional steps to authenticate that person?

There is a wide range of users of credit reports that may encounter fraud alerts. However, there is no further guidance as to how these fraud alerts – or any other type of fraud detection service – should operate. Specifically, this Panel uncovered a gap for what specific steps the users of credit reports should take when there is an initial fraud alert.

10C. Working Group 2 – Attacks on Special Populations

The Problem

While special populations today are not believed to represent a large portion of those who are victims of identity theft, they are potentially at greater risk than the consumer population as a whole and they may face special challenges in protecting themselves. Accordingly, identity theft of these special populations may warrant extra attention.

Child credit fraud

Children are a special population who can become victims of financial identity fraud. In a typical scenario, an identity is created using a child's Social Security Number (SSN), the name may be completely unrelated to the child, and the birth date is faked. Parents or guardians are the majority of the perpetrators. While there are algorithms that help organizations identify, based on SSN, the date that the number was issued, the SSN does not necessarily reveal the individual's actual age.

Fiduciary abuse of the elderly / terminally ill

The elderly and terminally ill may be exposed to fiduciary abuse in several forms—these include various forms of identity theft and scams as well as having current accounts and other assets accessed or stolen. Unscrupulous family members and employees of care-giving organizations are also at times in a position to commit various types of identity theft and fraud against these vulnerable individuals.

ID theft of deceased to open new accounts

Another special population are the recently deceased. While the practice of the credit reporting agencies is to mark a credit file as deceased once a person dies based on data provided by the Social Security Administration (SSA) in its Death Master File (DMF) database, there are numerous reports of identity theft against those who have passed away. The Consumer Data Industry Association and others have testified at legislative hearings focused on the incomplete nature of the DMF which requires government agencies to timely report the death of someone to the SSA. Unfortunately, notification of death is often delayed at the state level. While notification happens in major cities reasonably quickly, in non-major cities it may never be reported to the SSA.

Identity theft of military personnel

The final special population identified are military personnel. In particular, families of deployed troops may be victimized while their spouses are away on active duty in foreign countries. A recent scam involves a person calling a military spouse, posing as an employee of the Red Cross, and saying that the caller's spouse was injured in Iraq. The caller then asks for the SSN and date of birth of the military member.

Discussion

Verification of SSN against Death Master File (DMF)

A SSN and other data can be used to verify the identity of an individual to make sure that the person is who they say they are. A lender may use the SSN and other data to look for anomalies which may be indications of attempted fraud (for example, do the name, address and SSN match). One measure is whether there is a match between an SSN attempting to be used and its association with an SSN obtained from the SSA's DMF.

Many financial institutions and credit reporting agencies receive regular updates from the DMF which is updated daily and shared with subscribers not less than monthly. Credit reporting agencies also learn about deaths from data furnishers who report decedent information to the agencies. To mitigate the potential for identity theft, consumers should report a family member as deceased to the decedent's creditors.

FACT Act Protections for military personnel

Under the 2003 FACT Act, people in the military who are away from their usual duty stations may request an Active Duty Alert on their credit reports. This alert lasts for one year and may be renewed. An Active Duty Alert removes the person from marketing lists for prescreened credit offers for two years and is otherwise treated the same as an Initial Fraud Alert. The person may delegate someone else to place or remove an Active Duty Alert on his or her behalf.

Existing Laws, Regulations, Standards, Guidelines, and Best Practices (Examples)

The following may have particular relevance to the issue of attacks on these special populations:

- [Social Security Administration's Death Master File](#) (row E34)
- [HIPAA](#) – See rules for special populations (e.g., those that limit access based on role) (row A15)

Potential Gaps

Recommendation 4: Strengthen Best Practices for Authentication

- **The Social Security Administration should initiate a project with the private sector to develop a process or mechanism that enables companies to verify if a Social Security number belongs to a minor.** Age verification against a Social Security number would greatly reduce identity theft against minors. *This information resides at the Social Security Administration.* At present, companies do not have a national means (e.g., a database) to verify if an individual is a minor before opening an account.
- **Entities reviewing their authentication practices against this Panel’s recommendations should consider the need for best practices and consumer education to help protect the elderly and the terminally ill from fiduciary abuse.** As noted elsewhere in this report, better authentication practices, e.g., minimizing use of the SSN for authentication except in conjunction with other factors, would help to mitigate the likelihood of identity theft occurring in general. It would also serve to protect these vulnerable populations specifically. The elderly and the terminally ill, their family members and care-giving organizations, need to be educated on the potential for abuse of the Social Security number as a tool to commit identity theft. It seems practical that this type of educational initiative be led by the Social Security Administration, working cooperatively with issue stakeholders across the public and private sectors.
- **The Social Security Administration should consider a new initiative that cooperatively works with individual states and the private sector to improve notification practices when someone is classified as deceased.** There are loopholes and inefficiencies in some current practices, which open a path for identity theft.
- **The FTC should consider a new mechanism to enhance identity theft protection for military personnel.** Active Duty military personnel are generally deployed, making the authentication steps a business might normally take impractical or even impossible (such as contacting the person by telephone or mail). Additionally, the current practices of allowing an “appointed delegate” to place or lift a credit alert for a deployed military person increases the risk of identity theft by that delegate.

10D. Working Group 2 – Security Freezes

The Problem

There is a lot of information available in the marketplace and consumers tend to seek out identity protection measures as their situation warrants. A security freeze a/k/a credit freeze is one of several options that consumers have to help thwart new account fraud. But there are some limitations that consumers need to be made aware of so they do not make the wrong assumptions about the protections they will receive from security freezes. There are also some issues around the usability of security freezes.

Discussion

Security freezes generally enable consumers to prevent their credit information from being distributed to anyone without their permission. Security freezes, once placed, must be temporarily lifted in order to allow the information to be made available to a would-be credit grantor.

General comments

A security freeze is one tool among many that a consumer may choose to use to prevent identity theft or remediate against it. For example, to prevent new account fraud, many consumers have successfully placed fraud alerts on their credit reports. Importantly, consumers should understand that while a credit freeze may protect against the opening of new accounts, a freeze will not protect against fraudulent takeover of existing accounts.

Many credit grantors will not establish new accounts without first seeing a credit report, so the ability of consumers to place security freezes and prevent disclosure of their credit reports to credit grantors is a powerful tool that can help prevent identity thieves from opening new accounts using someone else's identity. Potential unintended and adverse consequences of placing a security freeze include impeding point of sale opportunities as well as many transactions that often rely on credit reports, of which consumers may be unaware, such as employment applications, applications for residential apartment rentals, small business loans, and insurance.

It is important for consumers to understand how security freezes work.

Usability issues

Some 39 states and the District of Columbia have laws which allow individuals to place a freeze on their credit records. Different jurisdictions have differing requirements for various aspects of the freeze, such as how long it should take for a freeze to be placed after it is requested, and how long it should take for a freeze to be lifted. Some limit the availability of credit freezes to victims of identity theft who have filed a police report, while others allow any consumer to request a freeze regardless of whether they have been a victim. Some require the freeze request to be made by certified or overnight mail, while others allow it to be done by phone. Different states provide for different fees for placing and lifting the freeze. All of this adds a level of complexity and presents some usability issues for this tool.

Recently, the three major credit bureaus announced that they would offer consumers the ability to freeze their credit files regardless of whether or not they had become the victim of identity theft and even if the option to place a freeze is not mandated by state law. As of November 1st, 2007, any consumer residing in a state not already having an active freeze law can opt to have their credit files frozen or lifted for a \$10 fee at each of the three major credit reporting agencies (CRAs). If someone is a victim of identity theft, there is no charge, provided they submit a police report along with the initial freeze request. While all of the CRAs allow a consumer to lift a freeze by phone, at least one allows consumers to also do so online, and there may be differences in how long it takes for the freeze to be lifted, from 15 minutes to three days.

The President's ID Theft Task Force report tasked the Federal Trade Commission to study both the effectiveness of FACT Act protections and also the efficacy of credit freezes. The FTC plans to undertake such studies.

Consumers need to continue to be educated about the strengths and the limitations of security freezes and carefully weigh the benefits and tradeoffs of security freezes before making the decision to use this instrument.

Existing Laws, Regulations, Standards, Guidelines, and Best Practices (Examples)

- State credit freeze laws (row C3)

Potential Gaps

Recommendation 5: Increase Understanding and Usability of Security Freezes

- **The Lenders, Government Agencies, Consumer Advocacy Groups, Credit Reporting Agencies and others should continue to support consumer educational programs that communicate both the benefits and limitations of security freezes.** There are many state-specific rules on security freezes as well as voluntary policies adopted by the Credit Reporting Agencies. To add further complexity, each Credit Reporting Agency has its own procedures for placing and lifting freezes. All of these variables (based both on legislated requirements and industry initiatives) present a communications challenge for educating consumers about how freezes work.

The spectrum of key stakeholders involved with this tool need to assemble to review their processes and standardize them to the extent possible to make security freezes easier for consumers to use.

11A. Working Group 3 – Intentional Information System Breach

The Problem

A fundamental problem is theft of personal information through intentional breaches of information systems. The heavy concentration of personal information in an information system makes a data center and its information systems a rich target for fraud.

Hacking / Theft of Electronic Records

Much has been documented on the various threats and vulnerabilities of information systems, and several standards and best practices are available that address general information security. Certain industry sectors, particularly healthcare and financial, are further along in this area due to regulatory and industry mandates for security. However, research indicates that many information security breaches occur as a result of failure to adequately secure systems.

Theft of Physical Records

The concern of direct security breaches should not be limited to on-line systems. Physical records containing personal information are also subject to theft. Charts, reports, enrollment forms, payment information, and other paper-based record keeping systems all present their own set of threats and vulnerabilities.

The problem can also be extended to physical media, such as tapes, disks, CDs, etc. that are used for longer term storage. Warehousing and archival of information for business continuity, disaster recovery, or even compliance with regulatory data retention standards can result in rich concentrations of personal information.

Inadequate procedures to secure physical data

Threats to physical data might include removal of paper-based personal information, such as information in filing cabinets or left lying on desks. It might also include removal of electronic media, perhaps through misplacement or loss during transportation & storage. These types of theft are enabled in an environment that lacks adequate procedures to secure physical data.

Various industry best practices are available to safeguard physical data, such as inventory controls & recordkeeping, dual control, data retention policies and data destruction policies. Unfortunately, these practices are not consistently applied across all industry sectors.

Inadequate procedures to control persons who have access

A common vulnerability in storage of physical records & storage media is the lack of access controls. Unauthorized personnel in the presence of sensitive information pose a threat of information theft. Intruders, visitors, and even employees could be considered “unauthorized,” and could have motives and opportunity to steal physical records.

Access controls often include a mix of physical and logical methods, such as user-IDs & passwords, door locks, man-traps, and biometrics. While these countermeasures are often found in more sophisticated IT environments, they are not applied consistently or effectively across all industry segments. Even simple best practices of inventory control, separation of duties, and supervision can be effective, yet many organizations lack the policies and procedures for their implementation.

Discussion

There are a number of countermeasures that organizations can take to reduce the risk of a breach in an information system and the attendant loss of personal information. Of primary importance is the implementation of a comprehensive data security management program.

Define / Implement Standard Business Practices For Data Security Management

Most management-level information security standards require a top-down approach to applying security practices to an information system. Starting with an overall information security program endorsed at the executive management level, a comprehensive set of policies, standards, and procedures should be documented, communicated, exercised, audited, and continuously updated.

Secure systems / Protect data

An important part of any information security program is to identify and protect data deemed “sensitive.” In the context of identity theft, a risk assessment should be conducted, with a focus on the storage and maintenance of personally identifiable information (PII). Based on the risk assessment, appropriate controls and countermeasures should be applied to safeguard that information. Examples include physical access controls, logical access controls, and data encryption.

Restrict access to areas where sensitive data is stored

An obvious protection against identity theft is to keep the thief away from the information. This can be accomplished in a number of ways, including physical controls (fences, door locks, guards) and logical

controls (passwords, multi-factor authentication, authorization systems). These controls should be measured against the potential consequence and likelihood of a breach.

A simple but important element of access control is conducting background checks of employees. As employees are granted increasing levels of security access, they should have corresponding levels of background checks to ensure their level of trustworthiness, especially when tasks have limited accountability or dual control.

Monitor systems access / physical access

An equally important part of access control is the concept of auditing. By having a complete audit trail of each user's actions (physical access to system assets, or logical access to sensitive information), one can reconstruct the "crime scene" in case of a security breach. Also, the presence of a strong auditing system can serve as a deterrent to fraudulent activity.

Implement employee awareness training programs

Many organizations have sufficient policies and procedures, yet don't educate their employees on security fundamentals. Simple requirements, such as "don't let visitors wander around without an escort" or "don't open an unknown e-mail attachment" are critical, but will not be executed if not communicated to or understood by the employees. The lack of awareness can render an information security program ineffective. In many cases, lapses of security are a result of the lack of employee awareness and self-discipline.

As a part of an effective information security program, organizations should make sure they have effective employee awareness programs.

Impose sanctions on employees for non-compliance

In addition to an employee awareness program, organizations should also hold their employees accountable for non-compliance. Appropriate consequences should be applied for any lapse in security procedures, up to and including dismissal and law enforcement involvement.

Existing Standards (Examples)

Some examples of standards and other guidance relevant to Data Security Management are identified below including the ISO/IEC 27000 suite of standards (parts of which are still under development), the PCI Data Security Standard, and the North American Security Products Organization (NASPO) Security Assurance Standards for the Document and Product Security Industries (ANSI/NASPO Sav3.OP-2005).

General Industry Standards / Guidance

[ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements](#) (row L79)

[ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management](#) (row G146)

[ISO/IEC 18043:2006, Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems](#) (row G133)

[ISO/IEC TR 18044:2004, Information technology – Security techniques – Information security incident management](#) (row L76)

[ANSI/ARMA 5-2003, Vital records programs](#) (row G9)

[ANSI/NASPO SAV3.OP-2005, Security Assurance Standards for the Document and Product Security Industries](#) (row G217)

The US-CCU Cyber-Security Checklist, Final Version 2007 (row G232)

[President’s Identity Theft Task Force: Combating Identity Theft, Volume II, Supplemental Information, Part C, Guidance for Businesses on Safeguarding Data](#) (row E33)

[FTC Guidance on Information Security—Protecting Personal Information, A Guide for Business, March 2007](#) (row E10)

[OMB Guidance—Protection of Sensitive Agency Information, June 2006](#) (row E31)

[Interagency Guidelines Establishing Information Security Standards Small-Entity Compliance Guide, December 2005](#) (row E8)

[Family Educational Rights and Privacy Act \(FERPA\)](#) (row A13)

Financial Services Industry

ISO/TR 13569:2005, Banking and related financial services – Information security guidelines (row G126)

[X9.49-1998, Secure Remote Access to Financial Services for the Financial Industry](#) (row G22)

[PCI Data Security Standard, version 1.1](#) (G225)

[The Financial Modernization Act of 1999, "Gramm-Leach-Bliley Act"](#) (row A14)

[FTC The Financial Privacy Rule](#) (row A4)

FTC Safeguards Rule (row A11) and [Education & Guidance](#) (row E11)

Healthcare Industry

[The Health Insurance Portability and Accountability Act \(HIPAA\)](#) (row A15)

[HHS Privacy Rule](#) and [Security Rule](#) (row A1 and A2)

ASTM E1869-04, Standard guide for confidentiality, privacy, access, and data security principles for health information including electronic health records (row L34)

[ISO 22857, Health Informatics – Guidelines on data protection to facilitate trans-border flows of personal health information](#) (row G138)

Conformity Assessment Programs

[Certified Identity Theft Risk Management Specialist \(CITRMS\) ICFE course](#) (row J2)

[NASPO Certification to ANSI/NASPO SA v3.OP-2005, Security Assurance Standards for the Document and Product Security Industries](#) (row J3)

[BITS Financial Institution Shared Assessments Program](#) (row J1)

[PCI Data Security Standard, version 1.1 Security Audit Procedures](#) (row J4)

[Visa USA Payment Application Best Practices \(PABP\)](#) (row J5)

FTC Safeguards Rule (row A11) and [Education & Guidance](#) (row E11)

Potential Gaps

Recommendation 6: Enhance Data Security Management Best Practices.

ISO/IEC, the PCI Security Standards Council, NASPO and others in the standards developing community should review and augment as appropriate existing data security management standards (or, alternatively, develop new standards as may be needed) to give further attention to the following issues:

- **Define the frequency of “periodic” employee security training and the content of an employee awareness program.** Employee awareness is a critical part of an effective information security program. While various third party resources exist, the creation of standards and best practices to better define what is meant by “regular” or “periodic” employee security training and the content of an awareness program would be useful.

- **Clarify requirements for data access credentialing and background checks.** ANSI/NASPO SAv3.OP-2005 provides a platform; however, additional industry guidance and best practices may be useful to clarify requirements for data access credentialing and background checks. Specifically, organizations should credential based on job-specific requirements and apply principles of “least privilege” and “need to know” (i.e., if someone doesn’t need access to data or knowledge of a certain process to accomplish their job, don’t grant them access).
- **Provide guidance on continuous review of access credentials and privileges.** As employees change roles and increase their responsibilities over time, they may be granted greater access to sensitive information. The depth of the background checks performed upon hiring may not be suitable for the increased levels of responsibilities. Guidance should be provided on how frequently and how detailed these background checks should be conducted, the strength of credentials provided, and the related access privileges.
- **Develop targeted guidance for industry sectors that are not regulated or that do not have standards.** Some information security concerns and controls are not consistently applicable across all industry sectors. Regulated sectors (healthcare and financial, in particular) tend to be further ahead in their application of information security. Opportunities exist for the development of targeted guidance for non-regulated sectors.
- **Provide guidance to ensure that downstream vendors are secure.** The ANSI/NASPO SAv3.OP-2005 standard provides a foundation; additional guidance may be useful to ensure that third party “downstream” vendors follow information security management practices when receiving personally identifiable information in the course of business, or when certain functions are outsourced (e.g., applications, networks, data centers, or operations management).
- **Implement an ongoing program of security re-evaluation.** The President’s Identity Theft Task Force identified the need for continuous re-assessment. Organizations need to have an ongoing program of security re-evaluation to stay current with technological developments and new marketplace issues. The most effective information security programs include risk management protocols that continuously review technology shifts and related threats and vulnerabilities. Various

risk assessment models are available, including NIST special publication 800-30, *risk management guide for information technology systems*, which is soon to be revised.³⁹

- **Develop a security breach risk assessment for insurance purposes.** Increasingly, insurance companies are excluding coverage for losses due to information security breaches. Additional guidance would be useful for insurance companies to facilitate accurate measurement of information security risks. This would allow organizations with good security practices to be extended coverage against security breaches in their Errors and Omissions and Directors and Officers insurance policies.

³⁹ An initial draft revision of NIST Special Publication 800-30 is projected for publication in January 2008. Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*) will focus exclusively on risk assessments as applied to the various steps in the Risk Management Framework described in NIST Special Publication 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, an initial draft of which was released in October 2007.

11B. Working Group 3 – Mismanagement

The Problem

Mismanagement relates to the lack of sufficient information security management standards, or the insufficient application of those standards by organizations, to control acquired personally identifiable information (PII) in a secure and responsible manner. Most organizations today hold some type of PII as a part of their business functions; this may include for example personnel records, account information and/or medical histories. As a repository of this information, organizations have both a legal and social responsibility to maintain this information in a manner that minimizes or eliminates the risks associated with holding it. Those risks typically are viewed as being a liability risk to the holders and a potential financial or fraud risk to external person(s) if this information is compromised. This review focuses on the responsibility of private and public sector entities, not on the responsibilities of individuals in maintaining their own personal information.

Through the consensus process the problems related to the mismanagement of personal information were narrowed to three primary areas:

1. Loss of Hardware
 - Insufficient controls over laptops and other removable media resulting in the loss of computers and media through accidental or fraudulent means.
 - Lacking or insufficient data encryption for the personal information stored on compromised hardware.
2. Poor Data Handling Practices
 - Careless disposal of data that would allow the information to be fraudulently compromised or publicly disclosed.
 - Inadequate controls over the disposal, recycling or decommissioning of equipment embedded with unencrypted PII.
 - Administrative errors culminating in the accidental release of sensitive personal information.
3. Personal Information Released to Sub-contractor
 - Unencrypted data breach during the transfer of information to a subcontractor.

- Unencrypted data breach due to sub-contractor's security protocols not being in compliance or alignment with primary contractor.

Discussion

Organizations can address the problems associated with mismanagement by taking steps to better define, implement and verify the use of standards and best practices for data security and the maintenance of PII. Such steps include the following:

- Monitor the location of all removable media and implement procedures that restrict the use, removal, and release of any information stored on such media. Provide procedural systems that trace and monitor the usage of any removable media.
- Develop and implement procedures for the disposal of files containing personal information in a manner that would render the information totally inaccessible or unusable.
- Implement standards or procedures to mitigate the possibility of the accidental release of personal information. In addition, these procedures should include security breach handling protocols in the event of an accidental release.
- Employee awareness training programs need to be developed and implemented in any organization that maintains sensitive personal information.
- The primary holder of personal information should implement standards and procedures that require subsequent holders, or subcontractors, to maintain or exceed the same level of data maintenance security as the primary holder.

Existing Standards (Examples)

General Industry Standards / Guidance

[ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements](#) (row L79)

[ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management](#) (row G146)

[ISO/IEC 18043:2006, Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems](#) (row G133)

[ISO/IEC TR 18044:2004, Information technology – Security techniques – Information security incident management](#) (row L76)

[ANSI/ARMA 5-2003, Vital records programs](#) (row G9)

[ANSI/NASPO SAV3.OP-2005, Security Assurance Standards for the Document and Product Security Industries](#) (row G217)

The US-CCU Cyber-Security Checklist, Final Version 2007 (row G232)

[Family Educational Rights and Privacy Act \(FERPA\)](#) (row A13)

[President’s Identity Theft Task Force: Combating Identity Theft, Volume II, Supplemental Information, Part C, Guidance for Businesses on Safeguarding Data](#) (row E33)

[Interagency Guidelines Establishing Information Security Standards Small-Entity Compliance Guide, December 2005](#) (row E8)

[OMB Guidance—Protection of Sensitive Agency Information, June 2006](#) (row E31)

[OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, dated May 22, 2007](#) (row E30)

DHS / OMB paper, [Common Risks Impeding the Adequate Protection of Government Information, July 2007](#) (row E4)

FTC’s website: [Business Information](#)

[FTC FACTA Disposal Rule](#) (row A9)

[FTC Guidance on Information Security—Protecting Personal Information, A Guide for Business, March 2007](#) (row E10)

[BBB Security & Privacy – Made Simpler™](#) (row G42)

[Privacy Rights Clearinghouse Prevent Identity Theft with Responsible Information-Handling Practices in the Workplace](#) (row G227)

[Key Steps For Organizations in Responding to Data Breaches and Privacy Breach Checklist](#) (Canada) (row F2)

Financial Services Industry

ISO/TR 13569:2005, Banking and related financial services – Information security guidelines (row G126)

[X9.49-1998, Secure Remote Access to Financial Services for the Financial Industry](#) (row G22)

[PCI Data Security Standard, version 1.1](#) (row G225)

[X9.99-2004, Privacy Impact Assessment Standard](#) (row G35)

[The Financial Modernization Act of 1999, "Gramm-Leach-Bliley Act"](#) (row A14)

[FTC The Financial Privacy Rule](#) (row A4)

FTC Safeguards Rule (row A11) and [Education & Guidance](#) (row E11)

Healthcare Industry

[The Health Insurance Portability and Accountability Act \(HIPAA\)](#) (row A15)

[HHS Privacy Rule](#) and [Security Rule](#) (rows A1 and A2)

ASTM E1869-04, Standard guide for confidentiality, privacy, access, and data security principles for health information including electronic health records (row L34)

[ISO 22857, Health Informatics – Guidelines on data protection to facilitate trans-border flows of personal health information](#) (row G138)

[HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information](#) (row E2)

Conformity Assessment Programs

[Certified Identity Theft Risk Management Specialist \(CITRMS\) ICFE course](#) (row J2)

NASPO Certification to [ANSI/NASPO SA v3.OP-2005, Security Assurance Standards for the Document and Product Security Industries](#) (row J3)

[BITS Financial Institution Shared Assessments Program](#) (row J1)

[PCI Data Security Standard, version 1.1 Security Audit Procedures](#) (row J4)

[Visa USA Payment Application Best Practices \(PABP\)](#) (row J5)

FTC Safeguards Rule (row A11) and [Education & Guidance](#) (row E11)

Potential Gaps

Recommendation 6: Enhance Data Security Management Best Practices

Numerous standards exist (see above) that are applicable generally to the maintenance and management of personally identifiable information by organizations. Some industry sectors, financial and healthcare, for example, already have standards that provide guidance on what to do in the event of a data breach.

Additional guidance or procedures in the event information is compromised may be useful for those industry sectors that are not regulated or that do not provide standards that address this issue. (See later sections of this report dealing with security breach notification and interface with the consumer / remediation.)

11C. Working Group 3 – Excessive Data Collection / Retention / Access

The Problem

It is necessary for any organization that does business to collect and maintain certain sensitive information about or related to its customers. Advances in technology have automated much of this data collection and made it easier than ever for companies to quickly and inexpensively gather and store vast amounts of consumer data. Electronic storage has made storage capacity virtually unlimited and data can remain available virtually indefinitely. One problem that has arisen out of this situation is the unnecessary and excessive collection and retention of sensitive data after it has served its intended purposes, coupled with the allowance, intentional or otherwise, of inappropriate access to it. Without an established business need, excessive collection upstream can lead to problems downstream if there is excessive retention. Among the many types of data collected by organizations, excessive use and storage of Social Security Numbers (SSNs) is of particular concern. Unauthorized access to such data opens a door to unlimited opportunities for identity thieves with a devastating impact on organizations as well as their customers.

Discussion

It is recommended that organizations adhere to best practices regarding data collection, retention and access. The following are measures that organizations can take in this regard:

- Adhere to general data security standards, e.g., ISO/IEC 27002, or applicable industry-specific data security standards, e.g., PCI Data Security Standard.
- Given the number of local, state, and federal regulations and laws regarding the use of SSNs, collect, use and retain the SSN only when it is required by law or regulation or for prudent management of a specific or potential risk, and only for the life of the transaction or business relationship, in order to prevent future abuse.
- Consider obtaining consumer consent to hold sensitive data if needed beyond the expressed purpose of the transaction or business relationship, or as may be required by law or contract.
- Consider undergoing regular self-audits. During a self-audit, organizations can not only re-confirm their existing practices for collection, retention and access to data, but also identify and mitigate possible risks. The ever-changing legal, financial and technological climate also provides additional tools and perspective on how to better address organizational policies.

Existing Standards (Examples)

There are a number of standards in existence that address some areas or specific industry practices with regard to data collection, retention and access. Among those standards, some are self-regulations and some are mandated or encouraged by local, state or federal law.

- *Self-regulated approach*

One notable example of an industry self-regulating itself is the Payment Card Industry (PCI), which implemented a new standard called the [PCI Data Security Standard \(PCI DSS\)](#) in September 2006. This standard represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information. One of the main requirements addressed by the PCI DSS was implementation of strong access control measures (row G225).

- *Federal government regulated or encouraged approach*

Establishment and implementation of the [Health Insurance Portability and Accountability Act \(HIPAA\)](#) has led the healthcare industry to adopt strong standards regarding the privacy and security of personal health information. In particular, Sec. 1173 of the HIPAA addresses security and confidentiality policies as well as technical practices and procedures, such as individual authentication of users; access controls; audit trails, physical security and disaster recovery; protection of remote access point; protection of external electronic communications; software discipline and systems assessment (row A15).

- *Federal, state and industry combined efforts*

Several states have already passed laws specifically targeting the use and storage of SSNs. The President's ID Theft Task Force recommended that Federal agencies reduce the unnecessary use of SSNs, and that use of SSNs in the private sector be studied. [OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, dated May 22, 2007](#), urged federal agencies to explore alternatives to the use of SSNs (row E30).

- *Global standards*

Identity theft is a crime affecting countries and customers worldwide. On a global level, multinational corporations can use the [ISO/IEC 27002:2005](#) standard as it is a voluntary code of practice for information security management. This International Standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security

management in an organization. The objectives outlined in the standard provide general guidance on the commonly accepted goals of information security management (row G146).

Potential Gaps

Recommendation 7: Augment Best Practices for Sensitive Data Collection, Retention and Access

- **Industry, the Small Business Administration, Chambers of Commerce and similar organizations that nurture and support small businesses need to develop and distribute practical guidance to their constituencies for data collection, retention and access.** Nearly 26 million small businesses in America collect, store and manage personal customer and employee information, often without the expertise, resources or manpower needed to responsibly manage this storehouse of sensitive information. That's a big marketplace loophole for identity thieves to potentially exploit. In March 2006, BBB published a useful primer focused on helping to fill this need, entitled *Security & Privacy – MADE SIMPLER™*. This is a good example of the type of customized education this segment needs, but it needs to be circulated frequently and by more than just one issue stakeholder.

- **Industry and key government stakeholders (e.g. FTC, Office of Management and Budget, Social Security Administration) need to come together and develop uniform guidance on the collection, use and retention of Social Security numbers.** There is growing confusion by companies about which standards to apply or follow. This Panel sees a potential need to develop a unique standard as a means to provide common guidance to companies across industry lines, which would correspondingly eliminate costly and ineffective measures that may be only partially addressing the root issues.

11D. Working Group 3 – Security Breach Notification

The Problem

In general, entities that suffer a security breach of personal information, including businesses, government agencies, academia, and healthcare providers, are confronted with a wide array of state laws and federal agency guidelines concerning notification to the affected population. This has raised the question whether a uniform standard is desirable.

Discussion

The State of California was the first to enact a law⁴⁰ requiring notification of the affected individuals when unencrypted personal information⁴¹ was, or was reasonably believed to have been, acquired by an unauthorized person. Since then, 38 other states, Puerto Rico, and the District of Columbia, have each enacted security breach notice laws. Federally, the issue has floundered in Congress, in large part because of its jurisdictional sweep across many Committees in both the Senate and the House of Representatives. Also, the fact that most of the states have acted may have further dampened the sense of urgency. Finally, competing events such as the current crisis in home mortgage financing and foreclosures tend to crowd out older, more settled issues such as this one.

Nevertheless, a federal standard is still seen by some as desirable. The April 2007 report issued by The President's Identity Theft Task Force included among its recommendations: "that national standards should be established to require private sector entities to safeguard the personal data they compile and maintain and to provide notice to consumers when a breach occurs that poses a significant risk of identity theft."⁴²

The question of risk assessment is significant, and a point of division both among the states and among those advocating this issue federally. Of the 39 states that have laws on security breach notification, 27 have

⁴⁰ California Senate Bill 1386, signed by the Governor September 25, 2002 and effective July 1, 2003.

⁴¹ Personal information is defined in California law, and many of the other states, as: Resident's first name or first initial and her last name in combination with any one or more of the following data elements, when either the name of the data elements is not encrypted or redacted: i) Social Security number; ii) Driver's License or Identification Card Number; iii) Account Number, Credit Card Number or Debit Card Number with any required security code, access code, or password that would permit access to an resident's financial account.

⁴² The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 2007, p. 4. The complete report and more information is available at <http://www.idtheft.gov/>.

provisions requiring some type of risk assessment in order to trigger a notice requirement.⁴³ Consumer advocacy groups generally favor no risk assessment, the only notification trigger being that a breach in the security of protected information occurred, or may have occurred. Policy makers and federal regulators generally support a risk assessment as necessary. In its June 2007 report to Congress, the GAO noted:

Federal banking regulators and the President's Identity Theft Task Force have advocated a notification standard—the conditions requiring notification—that is risk-based, allowing individuals to take appropriate measures where the risk of harm exists, while ensuring they are only notified in cases where the level of risk warrants such action. Should Congress choose to enact a federal notification requirement, use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notification of breaches that present little risk.⁴⁴

In summary, the complexity of the risk assessment issue combined with the jurisdictional complexity among Congressional committees and the reality that most states have acted in this matter, presents a significant impediment to a legislated national standard for security breach notification.

The foregoing notwithstanding, organizations should endeavor to adopt a set of standard business practices with respect to data breach notification.

⁴³ States with no risk assessment trigger in their breach notification laws include: California, Georgia, Illinois, Minnesota, New York, North Dakota, Oklahoma, Puerto Rico, Tennessee and Texas. (Center for Information Policy Leadership, Hunton & Williams LLP: "Enacted State and Local Security Breach Notification Laws", October 5, 2007.)

⁴⁴ GAO Report 07-737. "PERSONAL INFORMATION: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited, However, the Full Extent is Unknown."

Existing Standards (Examples)

A number of relevant laws and guidelines exist, among them:

- State Laws.⁴⁵ The 39 states which have enacted security breach notice laws are: Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Vermont, Washington, Wisconsin, and Wyoming (row C3).
- The President’s Identity Theft Task Force April 2007 report: [“Combating Identity Theft—A Strategic Plan.”](#) Appendix A of this report contains a Guidance Memorandum on data breach protocol. Part D of [Volume II, Supplemental Information](#), lists guidance offered by the federal banking regulatory agencies, the Federal Trade Commission, and the state Attorneys General, as well as private sector guidance offered by the American Bankers’ Association, the Financial Services Roundtable, the Payment Card Industry (PCI), the National Cyber Security Alliance, the Identity Theft Resource Center, and the Council of Better Business Bureaus (row E33).
- [OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007](#)⁴⁶ (row E30)
- [Office of the Privacy Commissioner of Canada: Key Steps for Organizations in Responding to Privacy Breaches, April, 2007](#) (row F3).
- [ANSI/NASPO SA v3.OP-2005, Security Assurance Standards for the Document and Product Security Industries](#) and NASPO Certification to this standard (row G217 and J3).

Potential Gaps

⁴⁵ ARIZ. REV. STAT. § 44-7501; ARK. CODE ANN. § 4-110-101 to -108; CAL. CIV. CODE § 1798.82; COL. REV. STAT. § 6-1-716; CONN. GEN. STAT. § 36A-701B (2007); DEL. CODE ANN. tit. 6 §§ 12B-101 to -104; FLA. STAT. § 817.5681; GA. CODE ANN. § 10-1-910 to -912; HAW. REV. STAT. TIT. 26; IDAHO CODE § 28-51-104-107; 815 ILL. COMP. STAT. 530/1-900; IND. CODE § 24-4.9-1 to -4; KAN. STAT ANN. § 50-7a01-7a02; LA. REV. STAT. ANN. § 51:3071-3077; ME. REV. STAT. ANN. tit. 10, §§ 1346-1349; MD. ANN. CODE § 14-3501 TO 3508; MICH. COMP. LAWS § 445.63-.72; MINN. STAT. § 325E.61; MONT. CODE ANN. § 30-14-1701 to 1705; 2006 Neb. Laws 876; NEV. REV. STAT. § 603A.010-.920; N.H. REV. STAT. ANN. §§ 359-C:19, 359-C:21; N.J. STAT. ANN. §§ 56:8-161 to -166; N.Y. GEN. BUS. LAWS § 899-aa; N.C. GEN. STAT § 75-60-65; N.D. CENT. CODE §§ 51-30-01 to -07; OHIO REV. CODE ANN. §§ 1347.12, 1349.19, 1349.191 and 1349.192; OKLA. STAT tit. 74, § 3113.1 (2006); 73 PA. CONS. STAT. § 2301-2329; R.I. GEN. LAWS §§ 11-49.2-1 to -2, 11.49.2-7; TENN. CODE ANN. § 47-18-2107; TEX. CODE CRIM. PROC. ANN. art. 2.29, TEX. BUS. & COM. §§ 48.001-203; UTAH CODE ANN. §§ 13-42-101 to -301; 9 VT. STAT. ANN. tit. 9, § 2430, 2435; WASH. REV. CODE §§ 19.255.010, 42.17.31922; WIS. STAT. § 895.507; WYO. STAT. ANN. § 40-12-501-509. (Center for Information Policy Leadership, Hunton & Williams LLP: “Enacted State and Local Security Breach Notification Laws”, October 5, 2007.)

⁴⁶ <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>

Recommendation 8: Create Uniform Guidance on Data Breach Notification and Remediation

- **Issue stakeholders need to assemble and dialogue further on the desirability and feasibility of developing a private sector standard for data breach notification, recognizing there are tradeoffs.** Given the wide variety of guidance, it may be desirable for a Voluntary Consensus Standard to be developed by the private sector to provide a common baseline for organizations seeking to establish security breach notification procedures. In breaches involving cross-border information transfers, a Voluntary Consensus Standard could provide some basis for resolving conflicting national laws or regulations. It could also enumerate alternatives for remediation (see next section of report). The potential tradeoff is that a “one size fits all” approach could result in a standard that is a “lowest common denominator,” and one that would only be enforceable if adopted into law or regulation.

11E. Working Group 3 – Interface with the Consumer/Remediation

The Problem

While a number of standards, regulations and industry best practices exist for managing sensitive consumer data, and while at the moment there are 39 states, plus Puerto Rico and the District of Columbia, that have laws that define data breaches requiring consumer notification, there is relatively little specific guidance for business or consumers once a breach occurs.

Discussion

The Business Perspective

Today as defined by law in many states, a business, organization or government agency is required to notify consumers when their personally identifiable information (PII) is lost or compromised. Businesses have reacted quickly to these new laws and inundated consumers with form letters advising them that their PII is missing or was deliberately compromised and the circumstance that contributed to the data breach. Some letters also point recipients to the Federal Trade Commission or to “free” credit reports sites and urge consumers to consult these resources and stay vigilant protecting their identities.

Some businesses take additional measures to pay for a variety of monitoring and issue resolution services, should a consumer believe they are the victim of identity theft. Many states that have passed laws require the breached entity to provide such remediation services but requirements vary by sector. Unfortunately, the guidance available to business generally stops at the notification step. What happens from that point on is largely decided by attorneys and those in corporate risk management. There exists no standard framework to guide a business beyond notification.

Today an organization’s response to a breach is driven by the risk (cost) of inaction and the value of the customer to the organization. Absent business or regulatory guidance, businesses have provided identity theft prevention services to protect their brand and maintain relationships with valued customers.

The Consumer Perspective

A consumer's risk of identity theft is governed by a number of factors. Most involve the consumer making the right behavioral choices and remaining vigilant to protect their identity.

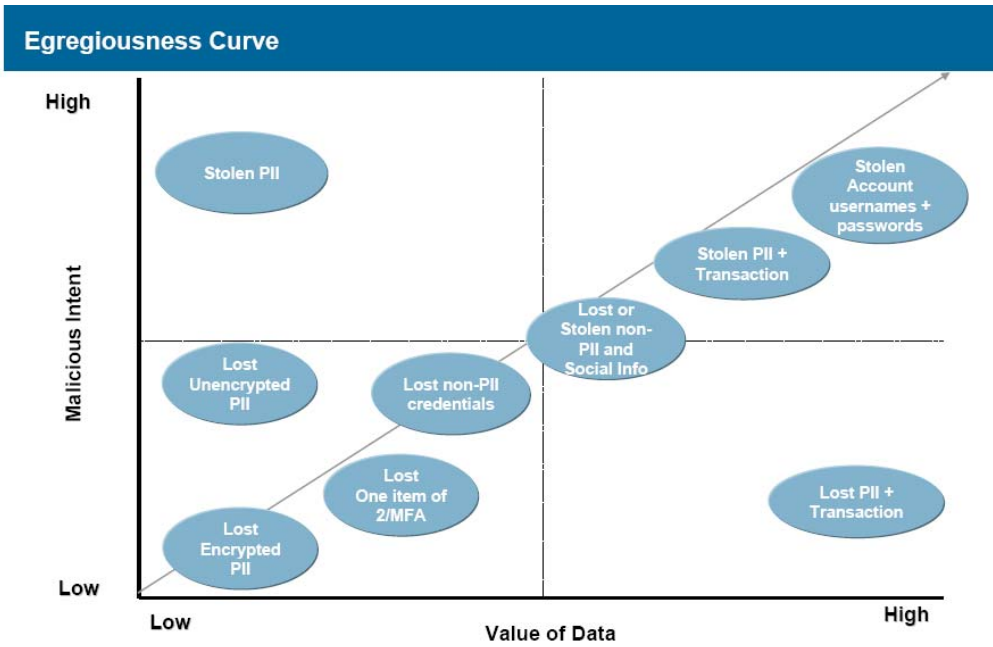
Many consumers have received breach notification letters from a company, educational institution or other organization that has lost their PII or had it taken. Typically, these letters give a benign explanation of the data loss and offer the consumer support ranging from directing them to free services like the FTC once-a-year access to a credit report to full credit report monitoring by the three major credit bureaus and assistance services if the consumer suspects identity theft.

Consumers receive little guidance regarding the likelihood of a threat from a data breach or how long the threat is active. Some PII is valuable for a short period of time while items like the SSN or data history are valuable to a seasoned identity thief for a long time. Consumers also receive little help in discerning between the applicability and effectiveness of a given identity theft protection solution to a given identity theft breach.

Many consumer "experts" and politicians have placed great stock in Credit Bureau Freezes. But Credit Bureau Freezes can only prevent new credit account fraud. A consumer who selects a Credit Bureau Freeze as their only protection may be at risk to many other identity theft threats.

Egregiousness Curve

The following Egregiousness Curve is a framework for characterizing data breaches and quantifying the potential impact to a consumer. While the placement of each type of breach along the curve can be debated, the intent is for businesses and consumers to understand the likelihood of risk given the characteristics of a breach. The Egregiousness Curve is a simple model but is a first step towards the analysis required to guide organizations and consumers regarding risk after a breach of consumer PII.



Key

PII – Personally Identifiable Information

2/MFA – Two/Multi-Factor Authentication

“Social Info.” – Not specifically PII, but enough identifiable information that an identity thief can find PII based on that social information.

Existing Standards (Examples)

Guidance for Business

- State Data Breach Notice Laws (row C2)
- State Credit Freeze Laws (row C3)
- [President's Identity Theft Task Force: Combating Identity Theft, Volume II, Supplemental Information, Part P, Current Remediation Tools Available to Victims](#) (row E33)
- [President's Identity Theft Task Force: Combating Identity Theft, A Strategic Plan, Appendix A, Identity Theft Task Force's Guidance Memorandum on Data Breach Protocol](#) (row E33)
- [FTC Final Rules on FACTA Identity Theft Definitions, Active Duty Alert Duration, and Appropriate Proof of Identity](#) (row A10)
- [Key Steps For Organizations in Responding to Data Breaches and Privacy Breach Checklist \(Canada\)](#) (row F3)
- Standards which provide access to consumer records
 - [The Health Insurance Portability and Accountability Act \(HIPAA\)](#) (row A15)
 - FCC Privacy Rules to Prevent Pretexting (row A7)
 - [FCRA for credit reports](#), etc (row A12)
- Standards which describe how to correct erroneous records
 - Above laws and business practices, etc.
 - Standards on debt collection and financial liability
 - Collection agencies, zero liability

Guidance for Consumers

- FTC's website: [Consumer Information](#)
 - [Identity Crisis ...What to Do If Your Identity is Stolen](#)
 - [Take Charge: Fighting Back Against Identity Theft](#)
 - [ID Theft Complaint Form and ID Theft Affidavit](#)

Potential Gaps

Recommendation 8: Create Uniform Guidance on Data Breach Notification and Remediation

This Panel identified two additional gaps in this area:

- *For Businesses* - Uniform guidelines on how to assist customers in the event of data compromise
 - *For Consumers* - A framework to evaluate potential value versus risk tradeoffs for services that detect or mitigate an identity theft incident resulting from the data breach.
- **Industry should take the lead in assembling a cross-sector forum to develop uniform guidance for the business community, government agencies, the non-profit community and academia on consumer remediation in the event of a data compromise.** Guidance should include factors such as the severity of the data compromise, the potential for actual identity theft as an outcome of the compromise, and how long the data leakage was going on before it was disclosed. This Panel believes that remediation guidelines may ultimately be a cascading set of actions based on these factors. Remedies might include some combination of fraud alerts, counseling / recovery services, credit freezes, public record monitoring or credit monitoring.
- **Issue stakeholders should take the lead to proactively, and consistently, educate / reinforce identity theft prevention strategies to their consumers.** Tracking studies strongly suggest that proactive prevention strategies are a consumer's best defense against identity theft. Consumers' consistent behavioral choices and vigilance are keys to their own safeguarding.

Should a consumer be notified that a compromise of their data has occurred, they also need:

- Solid education to help them discern among victim assistance services (including insurance).
- Guidance to help them secure and protect their personally identifiable information in the future.
- Steps for changing their federally-issued documents, as the situation warrants.

12. Acknowledgements

ANSI and BBB express sincere appreciation to the following organizations for the substantial financial support that they provided for this initiative:

Founding Partners



Contributing Members

AARP

Accredited Standards Committee X9, Inc. Financial Industry Standards

Affinion Group

Alliance for Telecommunications Industry Solutions

AOL LLC

American Financial Services Association

ARMA International

Debix

Experian

Fellowes, Inc.

General Services Administration

IdentityTruth

KPMG

Kroll's Fraud Solutions

Lifelock

North American Security Products Organization

Pay By Touch

Pre-Paid Legal Services, Inc.

SourceCheck, Ltd.

Telecommunications Industry Association

Underwriters Laboratories Inc

ANSI and BBB also acknowledge with great appreciation the participating organizations and individuals who contributed significant investments of time and effort toward this initiative. In particular, we would like to thank:

IDSP Chairman

Mr. Joseph V. Gurreri III, President, Chief Principal, CorporatePlanningGroup.NET

Formerly Vice President, General Manager, Global Solutions Development & Consulting, TransUnion
Analytic Decision Services

Working Group1 Issuance Chairs

Mr. James X. Dempsey, Policy Director, Center for Democracy and Technology (Co-Chair)

Mr. James E. Lee, President, C2M2 Associates, LLC; Formerly SVP and Chief Public and Consumer Affairs
Officer, ChoicePoint (Co-Chair)

Mr. Mark A. Zalewski, Director of E-Standards, American Financial Services Association (Interim Co-
Chair)

Working Group2 Exchange Chairs

Mr. Jeffrey Friedberg, Chief Privacy Architect, Microsoft (Co-Chair)

Mr. Steve Zelinger, EVP, General Counsel & Secretary, Pay By Touch (Co-Chair)

Ms. Julie Ferguson, Vice President of Emerging Technologies, Debix (Interim Co-Chair)

Working Group3 Maintenance Chairs

Mr. Jim Shaffer, Chairman of the Board, ASC X9 Inc, and Senior Security Analyst, ACI Worldwide (Co-
Chair)

Mr. George K. "Chip" Tsantes, EVP and CTO, Intersections Inc. (Co-Chair)

ANSI Staff

Mr. James McCabe, Director, Consumer Relations and IDSP

Ms. Alison Ziegler, IDSP Program Administrator

BBB Staff

Ms. Sally Munn, VP Marketing & Partnerships

Ms. Ronna Brown, Past President, BBB Center for Research and Education

Mr. Mark Kennedy, Director, Marketing & Partnerships

Members of the Steering Committee

Members of the Steering Committee included the Panel Chairman and representatives from the Founding Partners and the following At-Large Members:

AARP

Accredited Standards Committee X9, Inc. Financial Industry Standards

Affinion Group

Alliance for Telecommunications Industry Solutions

American Financial Services Association

AOL LLC

ARMA International

Center for Democracy and Technology

Debix

Fellowes, Inc.

General Services Administration

KPMG

National Institute of Standards and Technology

North American Security Products Organization

Pay By Touch

Telecommunications Industry Association

Underwriters Laboratories Inc.

Members of the Report Drafting Committee

Working Group 1 - Issuance

Mr. James X. Dempsey, Policy Director, Center for Democracy and Technology

Mr. Garland Land, Executive Director, and Mr. Chuck Hardester, Security Contractor, National Association for Public Health Statistics and Information Systems

Mr. Graham Whitehead, Director of Auditing, North American Security Products Organization

Mr. Thomas E. Wolfsohn, Chief Policy Officer, American Association of Motor Vehicle Administrators

Mr. Mark A. Zalewski, Director of E-Standards, American Financial Services Association

and the members of Working Group 1

Working Group 2 - Exchange

Ms. Julie Ferguson, Vice President of Emerging Technologies, Debix

Mr. Jeffrey Friedberg, Chief Privacy Architect, Microsoft

Ms. Susan Grant, National Consumers League

Mr. Bob Pinheiro, Robert Pinheiro Consulting LLC

Mr. Robert Ryan, Vice President, Government Relations, TransUnion LLC

and the members of Working Group 2

Working Group 3 - Maintenance

Ms. Julie Bernard, Senior Manager, Accenture

Mr. Michael O'Neil, Chairman, North American Security Products Organization

Mr. Vladimir Poletaev, Dir., Account Management / Client Services, Europ Assistance USA

Mr. Robert Ryan, Vice President, Government Relations, TransUnion LLC

Mr. Jim Shaffer, Chairman of the Board, ASC X9 Inc, and Senior Security Analyst, ACI Worldwide

Mr. George K. "Chip" Tsantes, EVP and CTO, Intersections Inc.

and the members of Working Group 3

Annex 1 – Panel Charter

Mission

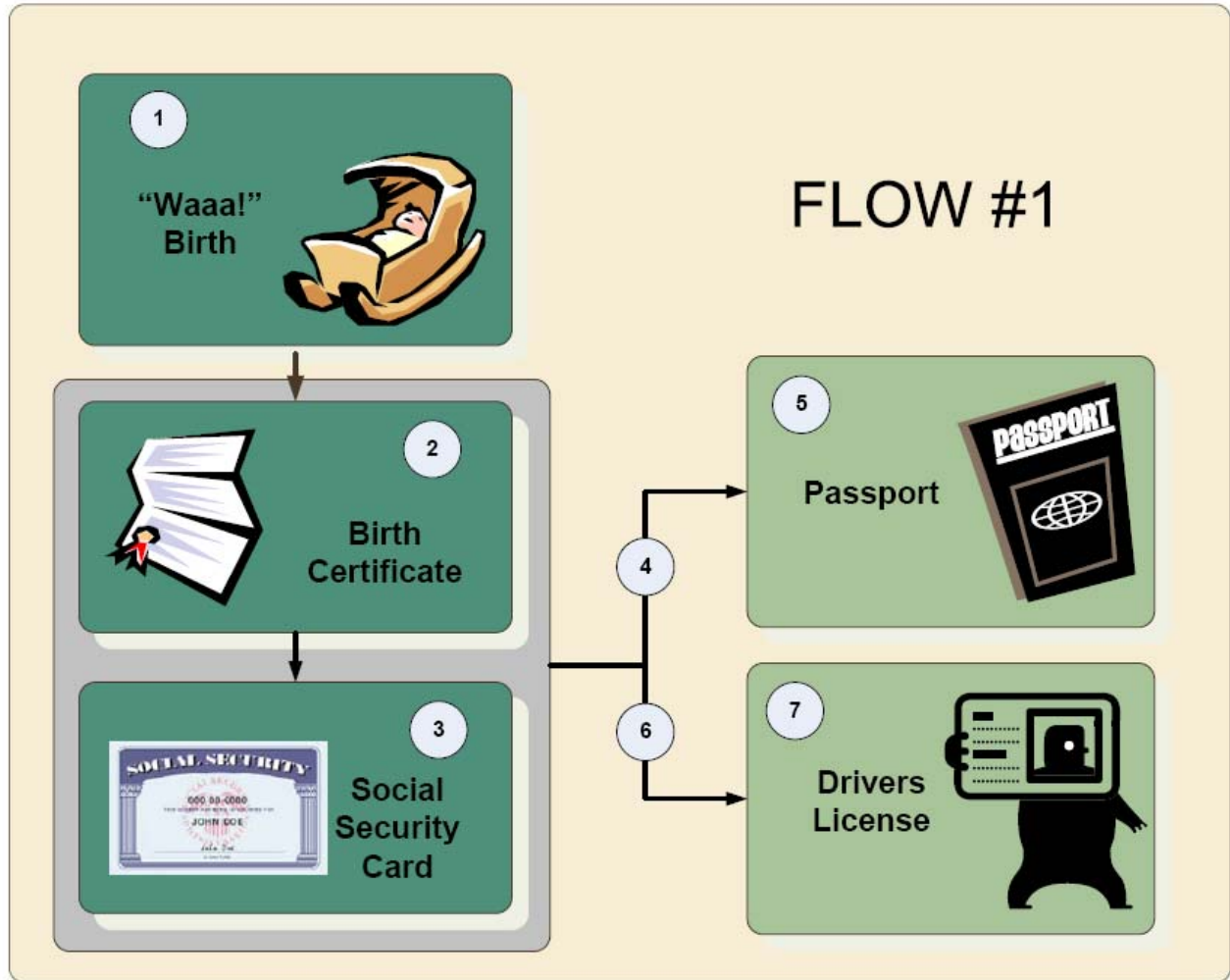
The ANSI-BBB IDSP is a cross-sector coordinating body whose objective is to facilitate the timely development, promulgation and use of voluntary consensus standards and guidelines that will equip and assist the private sector, government and consumers in minimizing the scope and scale of identity theft and fraud. The Panel will be charged with two key goals:

1. Identify and catalogue existing standards, guidelines, best practices and related conformity assessment systems focused on identity theft and fraud, including definitions, threats and identity management solutions as they pertain to identity theft and fraud prevention.
2. Identify areas needing updated or new standards, guidelines, best practices and related conformity assessment systems germane to combating identity theft and fraud which have the potential to further diminish the impact of identity theft and fraud on marketplace trust and commerce.

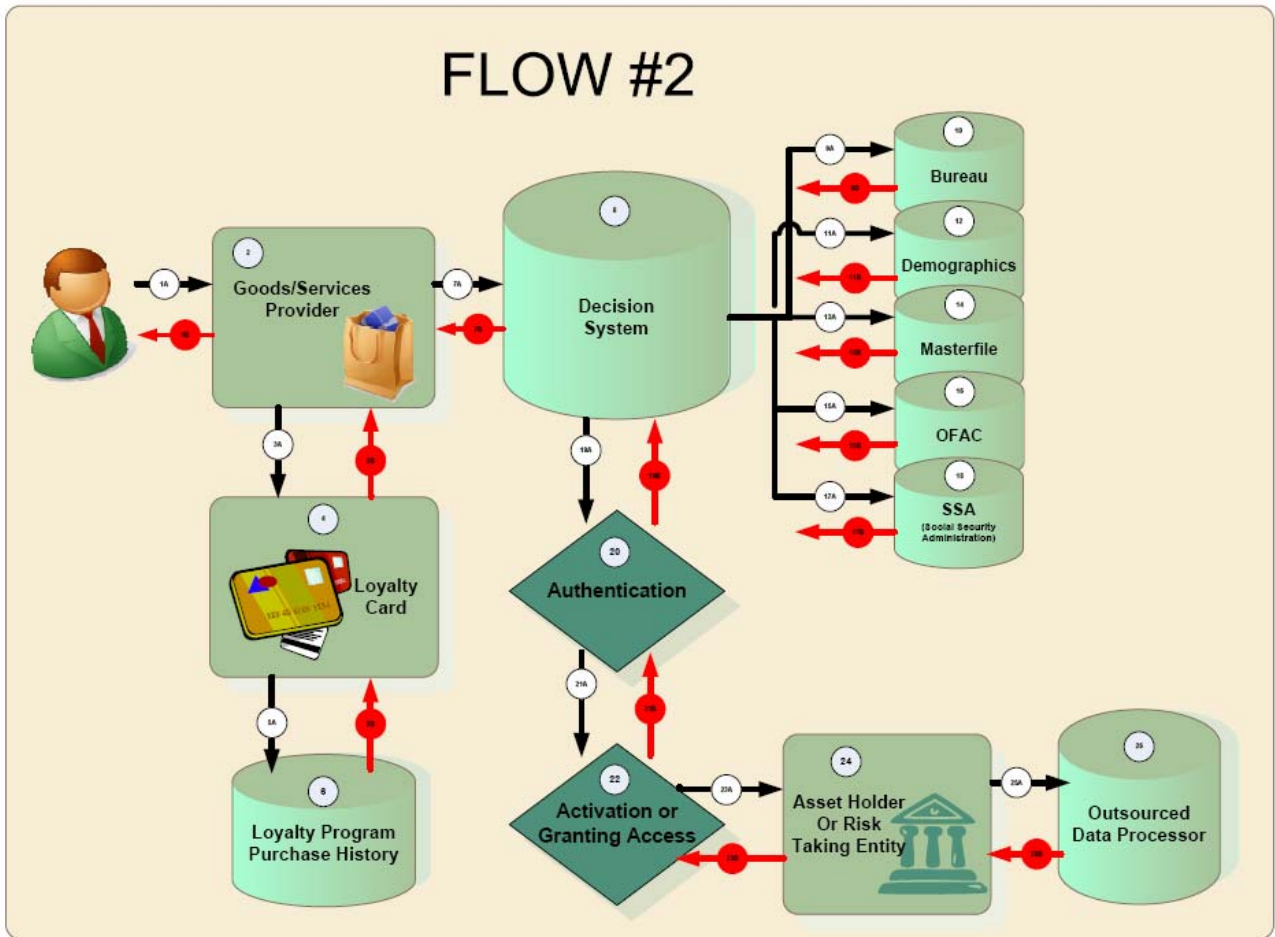
Terms of Reference of Panel

1. Coordinate and provide a highly inclusive forum for industry, non-governmental organizations, standards developing organizations, government, consumers and other participants to identify and define needs, determine work plans and establish priorities for updating standards or creating new standards.
2. As appropriate, coordinate with other national, regional, and international efforts addressing identity-related standards, i.e. Health Care IT Standards Panel (HITSP) and ANSI Homeland Security Standards Panel (ANSI-HSSP).
3. Solicit participation from other identity-related standardization work areas, i.e. Biometrics, Health Care, Security; and work cooperatively to achieve the mission of the ANSI-BBB IDSP.
4. Facilitate and promote cross-sector collaborative efforts between standards developing organizations to establish work plans and to develop joint and/or complementary standards.
5. Produce a comprehensive, cross-sector report describing standards, guidelines and best practices that businesses and other organizations can use to prevent and respond to identity theft and fraud and protect the confidential personal data of their employees and customers.
6. Potentially establish and maintain a database of identity-related standards, accessible from the Internet, and capable of generating updates, alerts, and reports (may require additional funding).
7. Make widely available the results of the ANSI-BBB IDSP work.

Approved by IDSP Steering Committee 16 November 2006



FLOW #2



Flow #1

The first flow illustrates the birth of a US citizen and the subsequent identity stages that occur.

1. Birth.
2. Issuance of birth certificate.
3. Issuance of Social Security card.
4. The process of issuance of a US Passport includes birth certificate and Social Security card.
5. The passport document; anti fraud components within the passport document.
6. The process of issuance of a US state drivers license uses birth certificate and Social Security card.
7. The license document; anti fraud components within state documents.

Flow #2

The second flow shows a typical new account establishment procedure. This process could be for a consumer general purpose credit card, private label retail card, mobile phone, insurance, apartment rental, or other situations whereby a good or services provider is taking a risk that the consumer will not repay their debt. This flow begins with an assumption that a consumer has already earned the ID credentials from Flow #1, including driver's license and Social Security card. Each set of process lines includes an 'A' and 'B' line options. A indicates the flow of data from left to right, or top to bottom, and B indicates the opposite flow; usually a response to the initial request.

1. Consumer interacts with a goods/services provider. In this scenario, the consumer is approaching a 'brick and mortar' facility or location. Alternatives Flows can be designed to accommodate web interaction or telephone interaction. These may require acknowledgement for more steps such as internet connectivity and subsequent data transfers and system authentication.
2. The entity, such as a retailer, phone distributor, rental building or other services provider.
3. An optional process where many retailers convince their customers to sign up for their frequent shopper program. This could be an internal or an outsourced process. This stage includes the data transmission from point of application to the loyalty card decision process, but not necessarily the ultimate loyalty card masterfile repository (which is #6).
4. The loyalty card, token, device used to match consumer to loyalty account information.
5. The process of establishing the initial loyalty card account onto the loyalty card masterfile and subsequent purchase history transactions which are sent to the loyalty card masterfile repository (#6).
6. The loyalty card masterfile repository. All consumer identification resides in this location as well as all subsequent purchase information. Such systems may also include consumer behavior models and cross-sell platforms. This environment may be an internally managed or outsourced process. Data may reside locally, centrally, or at an outsource vendor.
7. The inbound and outbound data transfer between point of application and decision system.
8. Decision environment. This may be an internal or outsourced environment. This may be a locally installed software, centrally installed software, or outsourced ASP process which can be either client-dedicated installed or shared environment. This decision environment also performs 'validation' and 'verification' routines. For the purposes of this diagram, 'validation' is the checks for sensibility of data components (i.e., a SSN is 9 digits, numeric only, and within the issued range). 'Verification' is some sort of check to another data source, or comparisons between data components (i.e. SSN is not on the death-master list, or the birth-state or SSA application location listed on application matches the SSA issued ranges for that state).

9. The inbound and outbound data transfer between decision system and contiguous data source.
10. Consumer credit bureau search such as TransUnion, Equifax, or Experian.
11. The inbound and outbound data transfer between decision system and contiguous data source.
12. Search within a non-credit consumer demographic repository, such as LexisNexis or Acxiom.
13. The inbound and outbound data transfer between decision system and contiguous data source.
14. The system of record which contains consumer identifying information and purchase history. This search is usually to check for current customer status to prevent repeated opening of new accounts for current customers. This search also serves to check for prior negative experience with the applicant.
15. The inbound and outbound data transfer between decision system and contiguous data source.
16. OFAC search accommodated through a direct link, or more likely through an outsourced vendor. Credit bureaus often fulfill this function in #10.
17. The inbound and outbound data transfer between decision system and contiguous data source.
18. SSA search. The Social Security Administration provides some diagnostic information to assist during application process. Credit bureaus often fulfill this function in #10.
19. The inbound and outbound data transfer between decision system and an authentication process. This could be the same data transfer #9 if a credit bureau (#10) is the host of the authentication process. This connection should still be distinguished as distinct from #9 since more than connection to credit bureau is needed for most authentication routines. Some bureaus accommodate this through standard credit bureau interaction, and some use alternative connection methods.
20. Authentication decision process. Authentication is the step beyond verification and must include interactive questions, also called 'knowledge based authentication' or KBA. Solutions commonly use 'in-wallet' and 'out of wallet' question types which may use sources from credit bureaus, demographic data bureaus, prior purchase history, map/location software and shared-secrets.
21. The inbound and outbound data transfer between authentication system and activation and account establishment process.
22. The activation process. Examples include credit cards where the token or card is 'activated' through a separate process. Telecommunications employs a process of activation when the consumer initiates the phone service on a new handset. Other processes, such as face-to-face transactions may not include such a step.
23. The inbound and outbound data transfer between activation process and asset-holder's main interface.
24. Asset-holder or risk-taking entity. This is the main interface with the organization ultimately. granting the application's approval, and taking the risk for requested products or services according to the terms on the application. This step may comprehensively include the following steps of #25 and #26.
25. The inbound and outbound data transfer between the asset-holder's main interface and any outsourced data management organization.
26. Outsourced Data Processor. Some asset-holders may outsource account management and purchase history transactions. To provide an example that is most comprehensive, these subsequent steps have been identified separately to accommodate examples where the asset-holder maintains a CRM (customer relationship) repository, and may outsource subsequent purchase and billing transactions.

Annex 3 – Standards Culled from the Inventory

The table that follows contains examples of existing laws, regulations, standards, guidelines, best practices, etc. with a rationale for how they relate to one or more of the problem areas identified by the IDSP Working Groups (WGs). A summary key to the problem areas is provided below, with a fuller description provided in the cited section of this report.

Problem Identifier Key

<u>Identifier</u>	<u>Issuance (WG1)</u>
I1	New Account Creation / Enrollment Government Context (Sections 9A, 9B) -- foundational creation (birth certificates, Social Security cards) -- subsequent credentials (driver's licenses, ID cards, passports) Commercial Context (ATM cards, credit cards, on-line banking, etc.) (Section 9C)
I2	Security Security of the issuance process (Section 9D) Credential security (Section 9E) -- Tokens, documents, user ids / passwords, certificates
<u>Exchange (WG2)</u>	
E1	Fraudulent use of "perceived" secret information (Section 10A) -- secrets aren't really secret (SSN) -- shared secrets can be replayed -- consumers get tricked / bad habits / inaction
E2	Inadequate validation of credentials (Section 10B) -- by consumer and relying party -- failure of creditors to verify requestor is person entitled to credit
E3	Attacks on special populations (Section 10C) -- fraudulent use to open new accounts -- special victims: kids / elderly / deceased / military
E4	Security freezes (Section 10D)
<u>Maintenance (WG3)</u>	
M1	Intentional information systems breach (Section 11A)
M2	Mismanagement (Section 11B)
M3	Excessive data collection / retention / access (Section 11C)
M4	Security breach notification (Section 11D)
M5	Interface with the consumer / remediation (Section 11E)

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
A1	HHS Privacy Rule	This Rule sets national standards for the protection of health information, as applied to the three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct certain health care transactions electronically. By the compliance date of April 14, 2003 (April 14, 2004, for small health plans), covered entities must implement standards to protect and guard against the misuse of individually identifiable health information.							X	X			
A2	HHS Security Rule	This Rule complements the Privacy Rule. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with the Electronic Protected Health Information (EPHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical. For each of these types, the Rule identifies various security standards, and for each standard it names both required and addressable implementation specifications.								X			
A3	Final Rule: REAL ID, Minimum Standards for Drivers' Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; announced January 11, 2008	The Department of Homeland Security has established minimum standards for State-issued drivers' licenses and identification cards that Federal agencies would accept for official purposes on or after May 11, 2008, in accordance with The REAL ID Act of 2005. This rule establishes standards to meet the minimum requirements of The REAL ID Act of 2005. These standards involve a number of aspects of the process used to issue identification documents, including: information and security features that must be incorporated into each card; application information to establish the identity and immigration status of an applicant before a card can be issued; and physical security standards for facilities where drivers' licenses and applicable identification cards are produced.	X	X		X							
A4	FTC's Financial Privacy Rule	This Rule requires institutions to give their customers privacy notices that explain the financial institution's information collection and sharing practices. In turn, customers have the right to limit some sharing of their information. Also, financial institutions and other companies that receive personal financial information from a financial institution may be limited in their ability to use that information.								X			

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
A5	Identity Theft Red Flags and Address Discrepancies under the FACT Act	<p>On October 31, 2007, the federal financial institution regulatory agencies and the Federal Trade Commission sent to the Federal Register for publication final rules on identity theft “red flags” and address discrepancies. The final rules implement sections 114 and 315 of the Fair and Accurate Credit Transactions (FACT) Act of 2003. The final rules are effective on January 1, 2008 and covered financial institutions and creditors must comply with the rules by November 1, 2008.</p> <p>The regulations that the agencies are jointly proposing would require each financial institution and creditor to develop and implement an identity theft prevention program that includes policies and procedures for detecting, preventing, and mitigating identity theft in connection with account openings and existing accounts. The proposed regulations include guidelines listing patterns, practices, and specific forms of activity that should raise a “red flag” signaling a possible risk of identity theft. Under the proposed regulations, an identity theft prevention program established by a financial institution or creditor would have to include policies and procedures for detecting any “red flag” relevant to its operations and implementing a mitigation strategy appropriate for the level of risk.</p>			X	X							
A6	USA PATRIOT Act -- Section 326 Customer Identification Program (CIP) Regulation	The USA PATRIOT Act in this instance requires reasonable and practical risk-based procedures to verify the validity of an applicant's identity. The legislative intent of Section 326 of the PATRIOT Act was not to force wholesale changes in the manner in which financial institutions identify and verify accountholders, but rather to ensure that the industry will continue to have adequate policies and procedures and follow best practices. This approach by Congress and the Administration is based on the view that financial institutions by-and-large already have sufficient policies and procedures for account opening.			X	X	X						
A7	FCC Privacy Rules to Prevent Pretexting	Prohibits telephone and mobile phone carriers from releasing customer records over the phone without a password in an effort to protect against the practice of pretexting. Also requires carriers to notify customers immediately when there are changes to their accounts, such as a new password, a new address or an online account opened.			X								X
A9	FTC's Disposal Rule	Requires businesses and individuals to take appropriate measures to dispose of sensitive information derived from consumer reports. Any business or individual who uses a consumer report for a business purpose is subject to the requirements of the Disposal Rule, a part of the Fair and Accurate Credit Transactions Act of								X			

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
		2003 (FACTA), which calls for the proper disposal of information in consumer reports and records to protect against “unauthorized access to or use of the information.” The standard for the proper disposal of information derived from a consumer report is flexible, and allows the organizations and individuals covered by the Rule to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology.											
A10	FTC Final Rules on FACTA Identity Theft Definitions, Active Duty Alert Duration, and Appropriate Proof of Identity	The Federal Trade Commission issued these final rules under the Fair and Accurate Credit Transactions Act (FACTA) regarding further definition of the terms “identity theft” and “identity theft report”; the duration of active duty alerts; and the appropriate proof of identity needed by consumers to block fraudulent trade lines in their consumer reports, place or remove fraud or active duty alerts, or truncate their Social Security Number in their file disclosures.											X
A11	FTC’s Safeguards Rule	<p>The FTC’s Safeguards Rule applies to a wide variety of “financial institutions” that are not subject to the jurisdiction of other federal or state authorities under the GLB Act. Among the institutions that fall under the Safeguards Rule are non-bank mortgage lenders, loan brokers, some state-regulated financial or investment advisers, tax preparers, providers of real estate settlement services, and debt collectors. The FTC’s regulation applies only to companies that are “significantly engaged” in such financial activities.</p> <p>Like the Interagency Security Guidelines, the Safeguards Rule requires financial institutions to develop a written information security plan that describes their procedures to protect customer information. Further, the Rule requires covered entities to take certain procedural steps, including: (1) assigning employees to oversee the program; (2) conducting a risk assessment; (3) designing and implementing an information safeguards program; (4) contractually requiring service providers to protect customers’ information; and (5) evaluating and adjusting the program in light of relevant circumstances. However, given the wide variety of entities (large and small) that are covered, the Rule mandates a data security plan that accounts for each entity’s particular circumstances, including its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.</p>							X	X			

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
A12	Fair Credit Reporting Act (FCRA) as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA)	For E1: Requiring regulators to devise a list of red flag indicators of identity theft, drawn from the patterns and practices of identity thieves. Regulators will be required to evaluate the use of these red flag indicators in their compliance examinations of financial institutions, and impose fines where disregard of red flags has resulted in losses to customers; For E2: As it relates to the nationwide system of fraud alerts for consumers to place on their credit files.			X	X							
A13	Family Education Rights and Privacy Act (FERPA)	This Federal law protects the privacy of student education records. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level.							X	X			
A14	The Financial Modernization Act of 1999, "Gramm-Leach-Bliley Act"	<p>The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions.</p> <p>The GLB Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to "financial institutions," which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities. Such non-traditional "financial institutions" are regulated by the FTC.</p> <p>GLB also deals with compliance on opt-out laws during the collection of information (and the sharing of it).</p>			X				X				

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
A15	The Health Insurance Portability and Accountability Act (HIPAA)	<p>Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the US health care system.</p> <p>HIPAA is listed under M3 but, which is Excessive data collection, but it is more related to M5 Interface/remediation, as it provides patients with the right to know how their information can be used; the right to examine and obtain a copy of their own health records and request corrections; the right to control certain uses and disclosures of their health information (SEC. 264). It is also applicable to M2 Mismanagement, as it requires adoption and implementation of privacy procedures for practice, hospital, or plan; limits release of information to the minimum reasonably needed for the purpose of the disclosure; requires training of employees so that they understand the privacy procedures; requires designation of an individual to be responsible for seeing that the privacy procedures are adopted and followed and holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights (SEC. 1176. ; SEC. 1177.).</p> <p>It may be also applicable to M1: Information system breach, as it addresses Security and confidentiality policies, Technical practices and procedures (such as individual authentication of users; access controls; audit trails, physical security and disaster recovery, protection of remote access point, protection of external electronic communications, software discipline and systems assessment (SEC. 1173.).</p>							X	X	X	X	X
A16	Intelligence Reform and Terrorism Prevention Act	Among other things requires the establishment of security standards for birth certificates. The regulations will be published for public comment in the spring of 2008.	X	X									

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
C2	State data breach notification laws	39 states have passed some sort of data breach notice law. Requires businesses and state agencies to alert state residents if an unauthorized user gains access to their unencrypted or unredacted personal data; some state laws cover paper records as well as computerized data; some laws contain a risk of harm threshold, which requires a covered entity to give notice to a person whose data is breached only "where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to the person"; some have penalties and fines, as well as grounds to seek damages.										X	X
C3	State credit freeze laws	39 states and the District of Columbia have enacted some sort of credit freeze law. Allows individuals to place security freezes on their credit records; some limit the availability of credit freezes to victims of identity theft who have filed a police report when others allow any consumer to request a credit freeze, regardless of whether they have been an identity theft victim (but for a fee); Most bills require credit bureaus to put a credit reporting freeze into effect within five business days of receiving a request from an individual; Most if not all laws include some provision allowing consumers to request a temporary lift of a credit freeze, and a requirement to honor such requests within three business days.				X		X					X
C4	State Laws and Model State Vital Statistics Act and Regulations	All states have laws and regulations governing birth certificates. Each state law is somewhat unique, but they are patterned after the model vital statistics law. There are also model vital statistics regulations that states have adapted.	X										
E2	HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information	This guidance document has been prepared with the main objective of reinforcing some of the ways a company may protect EPHI when it is accessed or used outside of the organization's physical purview. In so doing, this document sets forth strategies that may be reasonable and appropriate for organizations that conduct some of their business activities through (1) the use of portable media/devices (such as USB flash drives) that store EPHI and (2) offsite access or transport of EPHI via laptops, personal digital assistants (PDAs), home computers or other non corporate equipment.			X					X			

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
E4	Common Risks Impeding the Adequate Protection of Government Information, July 2007	To make the federal government’s identity theft awareness, prevention, detection, and prosecution efforts more effective and efficient, the President’s Identity Theft Task Force issued “Combating Identity Theft: A Strategic Plan.” The strategic plan instructed the Office of Management and Budget and the Department of Homeland Security to develop this paper identifying common risks (or “mistakes”) and best practices to help improve agencies’ security and privacy programs. Each risk is associated with selected best practices and important resources to help agencies mitigate and avoid these risks.								X			
E6-7	FFIEC Guidance on Authentication in an Internet Banking Environment and FAQs	The authentication guidance, which applies to both retail and commercial customers, specifically addresses the need for risk-based assessment, customer awareness, and security measures to reliably authenticate customers remotely accessing their financial institutions’ Internet-based financial services. The FAQs are designed to assist financial institutions and their technology service providers in conforming to the guidance by providing information on the scope of the guidance, the timeframe for compliance, risk assessments, and other issues.	X			X							
E8	Interagency Guidelines Establishing Information Security Standards Small-Entity Compliance Guide	This Small-Entity Compliance Guide is intended to help financial institutions comply with the Interagency Guidelines Establishing Information Security Standards (Security Guidelines). The guide summarizes the obligations of financial institutions to protect customer information and illustrates how certain provisions of the Security Guidelines apply to specific situations. The appendix lists resources that may be helpful in assessing risks and designing and implementing information security programs. Although this guide was designed to help financial institutions identify and comply with the requirements of the Security Guidelines, it is not a substitute for the Security Guidelines. Moreover, the guide only addresses obligations of financial institutions under the Security Guidelines and does not address the applicability of any other federal or state laws or regulations that may pertain to policies or practices for protecting customer records or information.								X			
E10	FTC's Protecting Personal Information: A Guide for Business	The FTC provides guidance to businesses on how to safeguard sensitive personal information of customers and employees. This guide outlines five key guidelines involved in a sound data security plan.								X			

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
E11	FTC Safeguards Rule: Education & Guidance	The FTC provides guidance on how to comply with the Safeguards Rule under the Gramm-Leach-Bliley Act. Under this rule, financial institutions must have a security plan to protect the confidentiality and integrity of personal consumer information.							X	X			
E13	2003 Revisions to the U.S. Standard Certificates of Live Birth and Death and the Fetal Death Report	This report describes the evaluation to prepare the 2003 U.S. Standard Certificate of Birth, the Standard Certificate of Death, and the Standard Report of Fetal Death. It describes the work of the Panel to Evaluate the U.S. Standard Certificates, brought together by the National Center for Health Statistics (NCHS), and presents the Panel's recommendations.	X										
E14	ANSI/NIST - ITL 1-2007, Data Format for the Interchange of Fingerprint Facial, & Other Biometric Information	This standard defines the content, format, and units of measurement for the exchange of fingerprint, palmprint, facial/mugshot, scar mark & tattoo (SMT), iris, and other biometric sample information that may be used in the identification or verification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, related descriptive and record data, digitized fingerprint information, and compressed or uncompressed images. This information is primarily intended for interchange among criminal justice administrations or organizations that rely on automated fingerprint and palmprint identification systems, or use facial/mugshot, SMT, iris, or other biometric data for identification purposes.	X										
E16	FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors	<p>This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems.</p> <p>The standard contains two major sections. Part one describes the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive 12 (HSPD-12), including personal identity proofing, registration, and issuance. Part two provides detailed specifications that will support</p>		X									

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
E17	NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems	<p>technical interoperability among PIV systems of Federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard. The interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in Special Publication 800-73, Interfaces for Personal Identity Verification. Similarly, the interfaces and data formats of biometric information are specified in Special Publication 800-76, Biometric Data Specification for Personal Identity Verification</p> <p>This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help organizations to better manage IT-related mission risks.</p> <p>In addition, this guide provides information on the selection of cost-effective security controls. These controls can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and carry this information.</p> <p>Organizations may choose to expand or abbreviate the comprehensive processes and steps suggested in this guide and tailor them to their environment in managing IT-related mission risks.</p>							X				
E30	OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, dated May 22, 2007	<p>The US Office of Management and Budget (OMB) has issued new guidance to federal agencies for safeguarding sensitive information and responding to a data breach if one occurs. The May 22 memo from OMB Deputy Director Clay Johnson is an updated version of earlier guidance that the OMB issued in June 2006 and comes on the heels of the release of the President's ID Theft Task Force Strategic Plan in April and several data breaches at federal agencies in 2007. The guidance requires agencies to develop a data breach notification policy and plan within 120 days and includes steps that they can take to reduce the risks related to a data breach. It also includes recommendations to reduce the use of Social Security Numbers, including eliminating the unnecessary use of the SSN and exploring alternatives to agency use of SSNs as a personal identifier.</p>								X	X	X	

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
E31	OMB Guidance – Protection of Sensitive Agency Information, June 2006	<p>In addition to the recommendation that all departments and agencies use the checklist for protection of remote information provided by National Institute of Standards and Technology (NIST), four other actions are recommended in an effort to properly safeguard information assets while using information technology. These four actions are:</p> <ol style="list-style-type: none"> 1. Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing; 2. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access; 3. Use a “time-out” function for remote access and mobile devices requiring user reauthentication after 30 minutes inactivity; and 4. Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or it’s still required. 								X			
E33	President's Identity Theft Task Force: Combating Identity Theft, a Strategic Plan and, Volume II, Supplemental Information	<p>The strategic plan is the result of an unprecedented federal effort to formulate a comprehensive and fully coordinated plan to attack this widespread and destructive crime. The plan focuses on ways to improve the effectiveness of criminal prosecutions of identity theft; enhance data protection for sensitive consumer information maintained by the public sector, private sector, and consumers; provide more comprehensive and effective guidance for consumers and the business community; and improve recovery and assistance for consumers.</p> <p>Among other things, the plan calls for the establishment of national standards that require private sector entities to safeguard the personal data they compile and maintain and to provide notice to consumers when a breach occurs that poses a significant risk of identity theft.</p> <p>Guidance from the plan relevant to IDSP problem areas includes:</p> <p>Strategic Plan M4 and M5: Appendix A, Identity Theft Task Force’s Guidance Memorandum on Data Breach Protocol</p> <p>Volume II, Supplemental Information M2: Part B, Enforcement Actions Relating to Data Security M1 and M2: Part C, Guidance for Businesses on Safeguarding Data M4: Part D, Guidance for Businesses on Data Breaches</p>							X	X		X	X

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u> M5: Part P, Current Remediation Tools Available to Victims	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
E34	Social Security Administration's Death Master File	The SSA Death Master File is used by leading government, financial, investigative, credit reporting organization, medical research and other industries to verify identity as well as to prevent fraud and comply with the USA PATRIOT Act.				X	X						
E37	US Postal Service In-Person Proofing at Post Offices Program	The IPP Program is an operation by which the USPS conducts In-Person-Proofing of customers nationwide for physically authenticating an individual's identification at a post office before that individual is issued a digital certificate.			X	X							
E38	Mailing Standards of the US Postal Service Domestic Mail Manual	Contains standards for domestic mail, including requirements regarding mail receptacles, conditions of delivery and other Recipient Services found in Section 508		X									
F1	Australian National Smartcard Framework	The National Smartcard Framework is intended to become an essential reference guide for agencies introducing smartcard technology. It will facilitate the specification by these agencies of secure and interoperable credentials and will be fundamental to the delivery of better connected government services. The Framework will be used by agencies across all levels of government to ensure that, where necessary, smartcard implementations are mutually compatible and conform to industry standards.		X									
F3	Canada's Key Steps for Organizations in Responding to Data Breaches and Privacy Breach Checklist	The guidelines outline some of the key steps in responding to a breach, such as containing the breach, evaluating the risks associated with it, notifying the people affected and preventing future breaches.								X		X	X

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
G1	AAMVA DL/ID Security Framework	A package of decisions based on best practices, standards, specifications and recommendations to enhance driver's license administration and identification security. Addresses business requirements; business and systems security; initial customer identification; record and document creation; record and document use.	X	X									
G2	AAMVA Personal Identification -- AAMVA International Specification -- DL / ID Card Design (2005)	The intent of the specification is to improve the security of the DL/ID cards issued by AAMVA's members and to improve the level of interoperability among cards issued by all jurisdictions.		X									
G3	AAMVA Fraudulent Document Recognition Training Recognition	AAMVA, with the assistance of entities such as the Secret Service forensic document lab, developed this fraudulent document recognition training curriculum which is used to train state and provincial MVA personnel.		X									
G4	American Bankers Association Industry Resource Guide, Identification and Verification of Account Holders, January 2002	The American Bankers Association and its Account Opening Best Practices Group have devised these options for financial institutions to consider in developing customer identification processes.	X		X	X							
G8	Anti-Pretexting Working Group Best Practices for Authenticating Requests from Purported Customers Related to Call Detail Records	Anti-Pretexting Working Group's Best Practices for authenticating customers in an effort to prevent pretexting of customer call records. This Working Group is made up of telecom companies that volunteered to share their best practices and develop strategies for preventing consumer fraud and protecting the privacy of customers.			X	X							

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
G9	ANSI/ARMA 5-2003, Vital records programs	<p>ANSI/ARMA 5-2003 sets the requirements for establishing a vital records program. It includes requirements for identifying and protecting vital records, assessing and analyzing their vulnerability, and determining the impact of their loss on the organization. It does not apply to records that have migrated from vital status to other functional value.</p> <p>It provides guidance for identifying those organizational records and information that are deemed vital and provides standards for methods of protecting them.</p> <p>This standard should be used to point out and reference the critical nature of protecting certain types of records, data and information in general, but with specific reference to our current initiative of personal identifiable information.</p> <p>Chapter 7 of the Standard discusses Vital Records Identification; and while this traditionally addresses those records (or information) that would be needed to “restart” a business or process, there is much related to “What records are necessary to protect assets, protect legal and financial status of the organization, and preserve rights and obligations of employees, customers, stockholders, and citizens”.</p> <p>Chapter 8 of the Standard discusses Protection Methods and presents about 10 different approaches to this topic.</p>							X	X			
G14	ANSI X9.8 Banking – Personal Identification Number (PIN) management and security, Part 1: PIN Protection Principles and Techniques for Online PIN Verification in ATM & POS Systems	<p>Part 1 of this two part standard specifies the basic principles and techniques which provide the minimum security measures required for effective international PIN management. These measures are applicable to those institutions responsible for implementing techniques for the management and protection of PINs. PIN protection techniques applicable to financial transaction card originated transactions in an online environment and a standard means of interchanging PIN data. These techniques are applicable to those institutions responsible for implementing techniques for the management and protection of the PIN at Automated Teller Machines (ATM) and acquirer-sponsored Point-of -Sale (POS) terminals.</p>	X										

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
G22	X9.49-1998, Secure Remote Access to Financial Services for the Financial Industry	<p>The American National Standard X9.49 is designed to define a minimum level of security requirements for a secure and protected exchange of information between a user and a financial service provider. The standard is intended for use by banks and other payment system groups to implement controls that reduce operational risks in remote access-based financial systems. When implemented the protection offered will:</p> <ul style="list-style-type: none"> • Provide integrity for a message during transmission; • Provide for secrecy of the message during transmission; <p>Identify the correct user and financial service provider to and during data transmission; and</p> <ul style="list-style-type: none"> • Prevent repudiation of a message or transaction by user and service provider. <p>The level of protection provided depends upon the sensitivity of the information exchanged, and could vary among applications.</p>		X					X	X			
G35	X9.99-2004, Privacy Impact Assessment Standard	<p>This American National Standard recognizes that a Privacy Impact Assessment (PIA) is an important management tool that should be used within an organization or by third parties to identify and mitigate privacy issues and risks associated with processing consumer data using automated, networked information systems. This PIA Standard scope:</p> <ul style="list-style-type: none"> • provides references to educate the reader on privacy topics and financial privacy in particular • describes the privacy impact assessment activity, in general • defines the common components of a PIA regardless of business system affecting financial institutions, and • explains how to improve the quality of business-system specific PIAs <p>A privacy impact assessment (PIA) is different than a privacy compliance audit institutions. This standard provides a privacy impact assessment structure.</p>								X			

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
G42	BBB Security & Privacy - Made Simpler™	Manageable Guidelines to help protect customer's security and privacy from identity theft and fraud. In Chapter 8 it talks about payment card security requirements for collection and storage of credit card info: www.visa.com/cisp It also discusses point of sale payment software that has been validated compliant with Payment Application Best Practices.								X	X		
G43	Guidelines for Extended Validation Certificates, October 20, 2006	These Guidelines for Extended Validation Certificates ("Guidelines") describe certain of the minimum requirements that a Certificate Authority (CA) must meet in order to issue Extended Validation Certificates ("EV Certificates"). Organization information from Valid EV Certificates may be displayed in a special manner by certain software applications (e.g., browser software) in order to provide users with a trustworthy confirmation of the identity of the entity that controls the website they are accessing. EV certificates are an important manner for sites to authenticate themselves to users. They are used by several browsers including Internet Explorer 7 and Opera, and are also utilized by Windows CardSpace.			X	X							
G48	Document Security Alliance Recommendations for Driver License Security and The REAL ID Act	Addresses data capture; identification verification; secure ID production; secure ID credentials, authenticating IDs.	X	X									
G100	ICAO Doc 9303. Machine Readable Travel Documents	ICAO Doc 9303 has 3 parts: Part 1 covers Machine Readable Passports; Part 2 covers Machine Readable Visas, and Part 3 covers "Size 1 and Size 2 Machine Readable Official Travel Documents." The Sixth Edition of Part 1 was published in September 2006, in two volumes. Volume 1 sets forth the specifications for a machine readable passport (MRP), characterized by a visual inspection zone and a machine readable zone (MRZ) containing essential identification and document details in OCR-B typeface. Volume 2 sets forth the specifications for biometric enhancement of the MRP to become an "e-Passport". U.S. passports comply with ICAO.	X	X		X							

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
G109	ISO 9798-1, Entity Authentication, Part 1: General	Entity authentication - Part 1: General This International Standard specifies entity authentication mechanisms which use security techniques. These mechanisms are used to corroborate that an entity is the one that is claimed. An entity to be authenticated proves its identity by showing its knowledge of a secret. The mechanisms are defined as exchanges of information between entities, and where required, exchanges with a trusted third party. The details of the mechanisms and the contents of the authentication exchanges are not specified in this part but in the Parts 2-6 of this multi-part International Standard.			X								
G126	ISO/TR 13569: 2005, Banking and related financial services -- Information security guidelines	ISO TR 13569:2005 provides guidelines on the development of an information security programme for institutions in the financial services industry. It includes discussion of the policies, organization and the structural, legal and regulatory components of such a programme. Considerations for the selection and implementation of security controls, and the elements required to manage information security risk within a modern financial services institution are discussed. Recommendations are given that are based on consideration of the institutions' business environment, practices and procedures. Included in this guidance is a discussion of legal and regulatory compliance issues, which should be considered in the design and implementation of the programme.							X	X			
G131	ISO/IEC 18013, ISO compliant driving licenses, Part 1: Physical characters and basic data set	Part 1 of ISO/IEC 18013 establishes guidelines for the design format and data content of an ISO compliant driving license (IDL) in regard to both visual human-readable features and ISO machine-readable technologies. It creates a common basis for international use and mutual recognition of the IDL without impeding individual national/community/regional motor vehicle authorities in taking care of their specific needs. The design approach of the IDL ISO ID-1 size card and accompanying booklet with sleeve insert pocket is intended to replace the international driving permit (IDP) paper document. The basis of document design premises includes <ul style="list-style-type: none"> • a minimum common mandatory data element set; • a common layout for ease of recognition; • minimum security requirements. 	X	X									

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
G132	ISO/IEC 18013, ISO compliant driving licenses, Part 2: Machine Readable Technologies	Part 2 of this International Standard establishes guidelines for the design format and data content of an ISO compliant driving license (IDL) with regard to ISO machine-readable technologies. It creates a common basis for international use and mutual recognition of the IDL without impeding individual countries/states to apply their privacy rules and national/community/regional motor vehicle authorities in taking care of their specific needs.	X	X									
G133	ISO/IEC 18043:2006, Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection systems	<p>ISO/IEC 18043:2006 provides guidance for an organization that decides to include an intrusion detection capability within its IT infrastructure. It is a "how to" for managers and users who want to: understand the benefits and limitations of IDS; develop a strategy and implementation plan for IDS; effectively manage the outputs of an IDS; integrate intrusion detection into the organization's security practices; and understand the legal and privacy issues involved in the deployment of IDS.</p> <p>ISO/IEC 18043:2006 provides information that will facilitate collaboration among organizations using IDS. The common framework it provides will help make it easier for organizations to exchange information about intrusions that cut across organizational boundaries.</p> <p>ISO/IEC 18043:2006 provides a brief overview of the intrusion detection process; discusses what an IDS can and cannot do; provides a checklist that helps identify the best IDS features for a specific IT environment; describes various deployment strategies; provides guidance on managing alerts from IDSs; and discusses management and legal considerations.</p>							X	X			

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
G138	ISO 22857, Health Informatics -- Guidelines on data protection to facilitate trans-border flows of personal health information	ISO 22857:2004 provides guidance on data protection requirements to facilitate the transfer of personal health data across national borders. It does not require the harmonization of existing national standards, legislation or regulations. It is normative only in respect of international exchange of personal health data. However, it may be informative with respect to the protection of health information within national boundaries and provide assistance to national bodies involved in the development and implementation of data protection principles. The standard covers both the data protection principles that should apply to international transfers and the security policy which an organization should adopt to ensure compliance with those principles.							X	X			
G146	ISO/IEC 27002:2005, Information technology -- Security techniques -- Code of practice for information security management (ISO/IEC 17799:2005 has been renumbered as ISO/IEC 27002:2005)	ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains best practices of control objectives and controls in the following areas of information security management: <ul style="list-style-type: none"> • security policy; • organization of information security; • asset management; • human resources security; • physical and environmental security; • communications and operations management; • access control; • information systems acquisition, development and maintenance; • information security incident management; • business continuity management; • compliance. The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.		X					X	X	X		

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
G217	ANSI/NASPO SA v3.OP-2005, Security Assurance Standards for the Document Product Security Industries	This American National Standard identifies broad areas of security risks and specifies what must be done to reduce them to an acceptable level by high (Class I), medium (Class II), and basic (Class III) security operations. The Standard addresses the protection of security technologies and products by providing a framework to certify that suppliers and brand owners form secure operations and supply chains – from suppliers to producers to distributors to consumers. It serves as a comprehensive guide for the specification of security risk management requirements that are essential to establishing and maintaining the effectiveness of security technologies and products used as countermeasures against document, identity and product fraud.		X		X			X	X		X	
G223	OpenID 2.0 Specification	OpenID is a community-developed manner of doing Web single-sign-on (SSO) using URLs as identifiers for people. OpenID providers currently use username/password to log in their users, and are subject to automated phishing attacks. The OpenID community is considering using Information Cards and other phishing-resistant methods to mitigate these threats.	X										

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
G225	PCI Data Security Standard, version 1.1	<p>The PCI Data Security Standard version 1.1, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis.</p> <p>The PCI DSS covers these areas:</p> <p>Technical Foundation/Requirements: The standard details technical requirements for the secure storage, processing and transmission of cardholder data.</p> <p>Testing Methodologies: The standard provides for common auditing procedures and scanning procedures, and a common security Self-Assessment Questionnaire.</p> <p>The PCI Data Security Standard is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.</p> <p>The PCI Data Security Standard is comprised of 12 general requirements designed to:</p> <ul style="list-style-type: none"> • Build and maintain a secure network; • Protect cardholder data; • Ensure the maintenance of vulnerability management programs; • Implement strong access control measures; • Regularly monitor and test networks; and • Ensure the maintenance of information security policies. 							X	X			
G227	Privacy Rights Clearinghouse Prevent Identity Theft with Responsible Information-Handling Practices in the Workplace	These are PRC’s recommendations for the implementation of responsible information-handling practices by employers to prevent identity theft.											X

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
G232	The US-CCU Cyber-Security Checklist, Final Version 2007	This check list is intended as a comprehensive survey of the steps that corporations and other organizations should take to reduce their vulnerability to cyber-attacks. The vulnerabilities and counter-measures have been sorted according to six easy-to-distinguish categories of information system components: 1) hardware, 2) software, 3) networks, 4) automation, 5) humans, and 6) suppliers.							X	X			
I3	Document Security Alliance White Paper: Formulation and Definition of Birth Certificate Minimum Standards	The DSA white paper is focused on the birth certificate document itself; hence there is a lot of detail that is not relevant to issuance fraud per se. On the other hand it is directly relevant to identity theft and readers may find it thought provoking to read through the sections that discuss the issues and analysis of birth certificate fraud.	X	X									
I4	Document Security Alliance White Paper on Formulation and Definition of Minimum Card Security Standards for the Social Security Administration, April 4, 2006	Recommendations for improving Social Security card security.	X	X									
I6	NAPHSIS White Paper: Recommendations for Improvements in Birth Certificates	This white paper identifies nine specific areas in which improvements are recommended. These areas represent challenges in both resources and time required to accomplish the tasks. These recommended improvements along with the amount of security and fraud risk that will be alleviated, the ease of implementation, the resources required, and the need for coordination with other entities outside the vital records community are outlined.	X	X									
J1	BITS Financial Institution Shared Assessments Program	<p>The Financial Institution Shared Assessments Program was created to develop a standardized approach to obtaining consistent information about a service provider's information technology practices, processes and controls. As part of the program, and consistent with ISO 27002, ten areas of information security management have been used as the foundation for two complementary tools designed to document the service provider's ability to actively manage information security controls.</p> <p>Standardized Information Gathering Questionnaire (SIG): Developed by BITS members to leverage the BITS IT Service Providers Expectations Matrix and address the control areas covered in ISO 27002:2005, the SIG can be used to obtain required documentation and establish a profile on operations and controls for each of the control areas to obtain verifiable information for each control area. When used as a standalone</p>							X	X			

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
		document, the questionnaire provides information the financial institution needs to evaluate the security controls the service provider has in place.											
		Agreed Upon Procedures (AUP): Developed by BITS members with the Big 4 accounting firms acting as technical advisors, the AUPs provide objective and consistent procedures that will be performed on each of the control areas. Procedures address control objectives in security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, information security incident management, business continuity management, and compliance. Procedure outcomes enable organizations to view results in the context of industry risk management and regulatory requirements.											
J2	ICFE's Certified Identity Theft Risk Management Specialist™ (CITRMS) educational and certification testing program	The ICFE has developed the "Certified Identity Theft Risk Management Specialist™" (CITRMS) educational and certification testing program. The main purpose is to comprehensively prepare and equip law enforcement professionals, financial planners and CPA's, resolution advocates, notaries, lawyers, credit and debt counselors, with the knowledge and skills necessary to help consumers and businesses fully assess and minimize their risk of credit and identity theft.							X	X			
J3	NASPO Certification to ANSI/NASPO SAv3.OP-2005, Security Assurance Standards for the Document and Product Security Industries	Each NASPO member must maintain a set of consensus standards and operational protocols. This is to ensure that any brand owner, product manager, or customer needing graphic security products or services can ascertain that a NASPO member company is certified to operate within its classification. Members will be certified on an annual basis by NASPO qualified auditors, who will conduct on-site certification at the members' facilities.		X		X			X	X		X	

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
		The intent of NASPO goes beyond preserving the quality of the graphic security products industry; it also includes having its members recognized as a professional group of the highest integrity. What NASPO accomplishes is to join together individual qualified security product providers with a common goal; to provide brand owners, product managers and customers, an organizational structure and recognized level of security for the North American security products industry. This in turn creates an environment to lessen the economic and criminal impact of fraud at every level.											
J4	PCI Data Security Standard, version 1.1 Security Audit Procedures	PCI Security Standards Council maintains a companion document to the PCI Data Security Standard called the PCI DSS Security Audit Procedures. This is basically the auditor's assessment program, and contains a matrix of control objectives and guidelines for obtaining documentary evidence.							X	X			
J5	Visa USA Payment Application Best Practices (PABP)	Visa CISP (Visa USA) has a voluntary assessment program for software vendors, called the "Payment Application Best Practices (PABP)" assessment. This program uses 3rd party assessors to "prove" the application is compliant with the standard. The document is in matrix form to use as an auditor's guideline and requirements document.							X	X			
L34	ASTM E1869-04, Standard guide for confidentiality, privacy, access, and data security principles for health information including electronic health records	This guide covers the principles for confidentiality, privacy, access, and security of person identifiable health information. The focus of this standard is computer-based systems; however, many of the principles outlined in this guide also apply to health information and patient records that are not in an electronic format. Basic principles and ethical practices for handling confidentiality, access, and security of health information are contained in a myriad of federal and state laws, rules and regulations, and in ethical statements of professional conduct. The purpose of this guide is to synthesize and aggregate into a cohesive guide the principles that underpin the development of more specific standards for health information and to support the development of policies and procedures for electronic health record systems and health information systems. This guide does not address specific technical requirements. It is intended as a base for development of more specific standards.							X	X			

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
L76	ISO/IEC TR 18044:2004, Information technology - Security techniques - Information security incident management	<p>ISO/IEC TR 18044:2004 provides advice and guidance on information security incident management for information security managers and for information system managers.</p> <p>ISO/IEC TR 18044:2004 provides information on the benefits to be obtained from and the key issues associated with a good information security incident management approach (to convince senior corporate management and those personnel who will report to and receive feedback from a scheme that the scheme should be introduced and used); information on examples of information security incidents, and an insight into their possible causes; a description of the planning and documentation required to introduce a good structured information security incident management approach; a description of the information security incident management process.</p> <p>Quick, coordinated and effective responses to an information security incident require extensive technical and procedural preparations. Information security incident responses may consist of immediate, short- and long-term actions. Any actions undertaken as the response to an incident should be based on previously developed, documented and accepted security incident response procedures and processes, including those for post-response analysis.</p>							X	X			

<u>Row #</u>	<u>Designation / Title</u>	<u>Rationale</u>	<u>I1</u>	<u>I2</u>	<u>E1</u>	<u>E2</u>	<u>E3</u>	<u>E4</u>	<u>M1</u>	<u>M2</u>	<u>M3</u>	<u>M4</u>	<u>M5</u>
L79	ISO/IEC 27001:2005, Information technology -- Security techniques-- Information security management systems -- Requirements	<p>ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations).</p> <p>ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. It is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.</p> <p>ISO/IEC 27001:2005 is intended to be suitable for several different types of use, including the following:</p> <ul style="list-style-type: none"> • use within organizations to formulate security requirements and objectives; • use within organizations as a way to ensure that security risks are cost effectively managed; • use within organizations to ensure compliance with laws and regulations; • use within an organization as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met; • definition of new information security management processes; • identification and clarification of existing information security management processes; • use by the management of organizations to determine the status of information security management activities; • use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization; • use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons; • implementation of business-enabling information security; • use by organizations to provide relevant information about information security to customers. 							X	X			



Final Report – Volume I: Findings and Recommendations

January 31, 2008



AMERICAN NATIONAL STANDARDS INSTITUTE

Headquarters
1819 L Street, NW
Sixth Floor
Washington, DC 20036

Operations
25 West 43rd Street
Fourth Floor
New York, NY 10036

General Information
212.642.4900

Telefax
212.398.0023

On the Internet
www.ansi.org/idsp



BETTER BUSINESS BUREAU

Headquarters
4200 Wilson Blvd
Suite 800
Arlington, VA 22203

General Information
703.276.0100

Telefax
703.525.8277

On the Internet
www.bbb.org
