



Report Summary

**Excerpt from 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)**

REPORT SUMMARY

Excerpt from Final Report Volume 1: 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

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



Report Summary
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
