REPORT TO THE NATION

AN ANALYSIS OF NATIONAL DOCUMENT SECURITY VULNERABILITY

Table of Contents

DSA
DOCUMENT SECURITY ALLIANCE

EXECUTIVE SUMMARY

Crime based on identity theft and document fraud permeates many aspects of our society, injuring government, business and individuals alike. Today, the collective annual cost in the United States is hundreds of billions of dollars. The cost is not solely monetary. As the events of 9/11 revealed, even seemingly minor problems can quickly become national in scale. Fraud damages consumer confidence and erodes the ability of business, academia and government to provide vital services. Citizens directly impacted by these crimes are not only outraged; they look to government agencies and business organizations for solutions.

Document security impacts everything from prescription drug fraud to counterfeit driver's licenses and illegal immigration. Government officials at federal, state, and local levels whose documents and credentials are vulnerable to attack have an obligation to take action that will deter fraud and make it easier for law enforcement to detect fraudulent documentation.

To support the efforts of government and business, the Document Security Alliance (DSA), a not-for-profit organization with members from government, the private sector and academia, has developed this *Report to the Nation* to highlight significant problems involving document security.

This report provides facts, suggestions and recommendations to guide legislatures, executive management, program offices, and procurement officials in establishing a protective envelope for our citizens.

By understanding how a document can be attacked, document originators can design it to be more secure. Though there is no one silver bullet in today's document security arsenal, the security industry has proven technologies and tools to counter fraud and deter counterfeiters. DSA is ready to assist both the public and private sectors in examining specific challenges to document security and providing expert guidance to fashion and implement efficient and effective solutions.

Identity Documents

Almost everyone carries a means of personal identification: driver's license, government-issued identification (ID) card, student or employee ID. Yet, most of these IDs were never intended to be secure identity documents. They were intended to enable individuals to drive a vehicle or gain access to their school or place of work.

To strengthen economic security and public safety, DSA recommends the adoption of uniform standards for personal identification.

Specifically:

- Upgrading the security of birth certificates and other breeder/source documents that we use to acquire passports, driver's licenses and other day-to-day means of identification:

- Implementing electronic verification of breeder/source documentation as required by the REAL ID Act;
- Providing funding to improve the states' Vital Records operations;
- Issuing driver's licenses and identification cards from secure facilities;
- Standardizing document security requirements for state driver's licenses and identification cards;
- Ensuring that more stringent security is compatible with protecting each individual's privacy rights;
- Upgrading issuance, authentication and verification processes;
- Enabling cross-jurisdictional authentication of ID documents and implementing capabilities for cross-database application verification, and
- Establishing systems for facial recognition and other biometric verifications.

Other Government Documents That Support Identity

Other documents issued at the federal, state and local level show identity, provide proof of ownership, entitle citizens and non-citizens to rights and benefits, and provide proof of compliance with laws and regulations. When these documents are falsified, counterfeited, altered, or copied, individuals and the community bear the costs of their misappropriation and misuse.

Though driver's licenses and birth certificates have generated the most concern, fraudulent documentation plays a significant role in motor vehicle theft and odometer mileage fraud. To reduce such losses, DSA recommends increasing the security of motor vehicle titles through the use of overt and covert devices to thwart counterfeiters and expose fraudulent titles.

Non State-Issued Breeder Documents

Every day millions of Americans use documents to gain access to privileges, information, benefits and restricted areas. Examples include employee IDs, academic IDs & transcripts,. To strengthen the security of these documents, DSA recommends:

- Federal personal identification verification (PIV) standards be extended to enhance the security of employee and student IDs;
- Academic transcripts be required to use anti-counterfeit technologies that make illegal copying or reproduction difficult and facilitate the verification of legitimate transcripts; and
- Bank checks be required to contain sophisticated overt and covert anti-counterfeit features to thwart illegal reproduction or alteration.

Prescription Fraud

Prescription fraud enabled by fraudulent laser printed and written prescriptions and illegally used patient ID cards costs the U.S. healthcare system billions of dollars each year. Furthermore, abuse of prescription medication creates serious problems for communities and businesses nationwide. Some states have already added security technology requirements to written prescriptions and thereby eliminated millions of dollars in fraud.

DSA recommends that all prescription pads be uniquely numbered and contain document security technologies that prevent illegal duplication or copying. Furthermore, we encourage continued adoption and implementation of electronic systems that enable pharmacists to validate each prescription and authenticate the identity of the physician who wrote it.

Security Assurance and Risk Mitigation

It is in the interest of all government agencies to procure products and services that meet modern security standards. To this end, DSA recommends that procuring agencies and procurement officials utilize the DSA glossary as a reference to guide security feature selection and require that vendors comply with national security assurance standards.

Next Steps

This *Report to the Nation* is a call to action for government agencies nationwide. The Document Security Alliance recommends that agencies undertake a critical examination of ID documents they now generate and the means they currently use to authenticate applicants for these documents.

DSA

Security must be integrated into the processes and technologies that agencies use to establish an individual's identity. Agencies must also be able to verify the data presented to support the individual's use of identification and supporting legacy documents to gain benefits, access, funds or privileged information.

To ensure the success of these efforts, DSA is committed to providing in-depth expertise, a regularly updated glossary of security features and counsel to assist agencies in their selection and implementation of secure processes and technologies to strengthen document security.

STUDY & RECOMMENDATIONS

As our nation is now well into the 21st century, the challenges inherent in creating, issuing and authenticating secure documents have become more difficult:

- Pew Research estimates more than 245 million individual driver's licenses and identification cards are in use in the U.S.
- The U.S. Government Accountability Office has documented the use by criminals of counterfeit driver's licenses to purchase firearms.
- The National Association for Public Health Statistics and Information Systems (NAPHSIS) estimates that 57 jurisdictions using 6,400 locations issue more than 14,000 different documents purported to be certified copies of birth certificates.
- The U.S. Department of Homeland Security, Immigration and Customs Enforcement, states that millions of illegal immigrants have used fraudulent documents to obtain rights and privileges accorded to citizens and lawful residents.
- State attorneys general and state medical associations estimate that prescription fraud enabled by fraudulent prescription pads, misuse of Medicaid cards and other illegal means costs the U.S. healthcare system more than $5 billion annually.

This report addresses a wide range of challenges faced by federal, state and local governments to protect documents that convey important information, value and authority. It examines known problems, presents ideas and offers recommendations to guide legislatures and executive agencies to strengthen document security.

1. CATEGORIZING DOCUMENT FRAUD

In general, document fraud tends to fall into four principal categories:

1) Theft of legitimate documents and raw materials.

   a) Partial - Unauthorized acquisition of raw materials, like a hologram, that might facilitate production of a counterfeit;

   b) Pre-Issue - Theft of a ready-to-use document before issuance;

   c) Post Issuance - Theft of an authentic document from its intended holder.

2) False Issuance of legitimate documents.

   a) Malfeasance – Knowingly issuing an item under false pretenses;

   b) Illegal Production – Unauthorized use of authentic equipment by outsiders;

   c) Nonfeasance – Generating a legal document without following protocols

   d) Diversion - Use in an unintended market or application, or one specifically prohibited by law or agreement.

3) Alterations of legitimate documents.

   a) Deletion - Removing legitimate information;

   b) Insertion - Adding false information.

4) Counterfeits

   a) Clone – A reproduction employing the same base components and manufacturing technologies as the original;

   b) Facsimile – A reproduction employing base components or manufacturing technologies that differ from the original;

   c) Dissimilar Representation – An instrument known to exist, such as a license or check, that has little or nothing in common with the authentic item;

   d) Fictitious Item – A fantasy item where no legitimate counterpart is known to exist.

An act of fraud often entails multiple categories. A stolen document could, for example, contain altered data as well as a counterfeit addition.

By understanding how a document might be attacked, document originators can design security into the document and its validation processes right from the start.

No single silver bullet exists in today's document security arsenal. However, the security industry has depicted fraud protection and counterfeit deterrence technologies in the DSA glossary of security features that a designer can use to layer security features within each document. Layering involves the application of multiple technologies:

- Level 1 technology is easily identified without the use of auxiliary tools;
- Level 2 requires simple tools such as a magnifying glass or ultraviolet light; and
- Level 3 requires the use of sophisticated equipment to validate an overt or covert security feature.

2. IDENTITY DOCUMENTS

Almost everyone carries a means of personal identification. These identity documents must address two key factors: an acceptable level of certainty that a person is who they claim to be and the intended use of privileges. Generally, the higher the risk the more resources, information and intrusiveness are required to establish or authenticate an identity. Some people carry multiple identity documents – typically as cards – each associated with a specific set of permissions. Some may be used to gain physical access to a school or workplace; others provide logical access to data in a computer or personal account at a financial institution.

In what has become common practice, individual privileged documents (such as a driver's license, social security card, etc.) are often accepted as proof of identity. However these do not possess acceptable levels of certainty for higher use requirements.

Though offered and often accepted as proof of identity, these privileged documents are more appropriately understood as tokens of identity. They are but one of the three basic building blocks to authenticate a person's identity. The three blocks are:

1) What a person has in his or her possession, such as a passport, driver's license or birth certificate,

2) What a person knows, such as a Personal Identification Number (PIN) or elements from personal or family data that outsiders would be unable to determine,

3) What a person is or does, including personal or behavioral characteristics as varied as fingerprints, retina or iris images or the dynamic pattern recorded when someone walks or pens a signature.

These building blocks serve to reinforce personal identity and reduce the risk that an imposter will succeed in usurping an individual's identity. When a document such as a driver's license is structured with all three building blocks, it protects both the person who carries the document and those who rely on the document to authenticate the individual.

An overarching problem with many of the documents used to assert identity is that they were issued originally with relatively little thought to security. Birth certificates are completed by hospitals or birthing centers and filed with local or state officials within their jurisdiction. Certified copies of birth records filed within their jurisdictions are issued by local or state officials. Social Security cards provided individuals with a number to record their contributions to Social Security and, ultimately, to apply for benefits under the program. Over time, these credentials have become accepted to verify identity when the individual applies for a driver's license or passport.

2.1 Vital Records: Birth Certificates, Death Certificates and Electronic Verification of Vital Events (EVVE)

Vital Records capture key elements of personal identity: name, birthplace, birth date, and parents' names. These documents are used by issuers in the public and private sectors to establish the individual's identity when new documents are created and issued.

Birth certificates are often called breeder or source documents since they facilitate the acquisition of additional identity documents. Starting with the birth certificate, one can "breed" other documents, such as a Social Security card, driver's license or passport. Most birth certificates are certified copies or abstracts of the actual birth record, which is filed and maintained in the local jurisdiction of birth.

Currently, 16 states allow various levels of open access to birth records at the state or local level or release informational copies to anyone who requests them. Imposter and identity fraud often begins through such access.

In 2005, NAPHSIS recommended cross-matching birth and death records to reduce identity fraud. Many vital records offices lack the automation resources to perform this match in a timely fashion, creating loopholes that are exploited by criminals. While some states have an inter-jurisdictional exchange program to exchange birth and death records, not all states have appropriated the funding necessary to take full advantage of the system.

NAPHSIS has developed the Electronic Verification of Vital Event (EVVE) system to provide government-to-government verification of birth and death information. The system is currently available in 53 states and territories.

Given the public's concern about identity theft and the misuse of personal information, legislators and government officials will need to ensure that broader exchanges of identity information are not compromised.

Though Congress enacted the Real ID Act in 2005, implementation has stalled. Some states have, in fact, passed resolutions opposing the act or ignoring certain of its provisions. While this is being played out in Congress and state legislatures, there are improvements that can be made in birth certificate documentation and those steps in the issuance process that are potentially vulnerable to fraud. DSA is prepared to provide agencies with recommendations to improve the issuance process as well as the physical security of documents.

DSA recommends that federal and state governments embrace the importance the birth record serves in the identity chain and address improvements to its physical security and the issuance process. All U.S. birth certificates should incorporate overt and covert anti-counterfeiting and authentication technologies to increase the security of the document against counterfeiters.

2.2 State-Issued Driver's Licenses and Identity Documents

Driver's licenses and identification documents issued by state motor vehicle agencies are the personal ID of choice for most people throughout North America. Today, people routinely use their driver's license to board commercial airlines, enter secure buildings, and apply for specific programs and benefits. Organizations in both the public and private sectors use these documents to ascertain the identity of persons seeking physical or logical access to facilities or accounts.

Because driver's licenses are immediately recognized as official government ID cards, their authenticity is accepted by most organizations. Each card contains a facial image, signature, physical description and demographic information about the holder as well as a variety of security features, such as tamper-evident substrates that make visible any effort to alter data on the card.

Once issued, these ID cards become source documents that allow individuals to obtain additional documents, benefits, and services. If you have a driver's license, it is usually accepted as sufficient proof that you are who you say you are.

Identity theft is a serious crime that is costly both to the individuals victimized and to the banks and commercial institutions that suffer financial losses. Counterfeit identity documents are a financially lucrative business for organized crime. They have been used to create false identities for illegal immigrants. Terrorists have used them to travel freely within countries they have targeted. Phony driver's licenses also play a role in underage drinking, highway fatalities and tobacco use.

Following the events of 9/11, efforts to improve U.S. identity systems intensified when it was discovered that all but one of the hijackers had acquired authentic ID documents, such as driver's licenses and airline employee IDs, which they used to board commercial flights, rent cars, and operate freely within the U.S.

Congress passed the REAL ID Act to establish minimum security standards for state-issued driver's licenses and personal ID cards that individuals use to identify themselves when boarding airliners or seeking access to buildings and other areas that come under federal jurisdiction.

DSA recommends upgrading the security of breeder documents through the use of cross-jurisdictional authentication, cross-database application verification, and systems for facial recognition. DSA also recommends upgrading issuance, authentication and verification processes.

2.3 Standardization in Driver's Licenses and Identification Cards

State driver's licenses and ID cards are now the most important documents for establishing individual identity. State motor vehicle administrators have long advocated minimum standards for creating and producing driver's licenses and ID cards. The American Association of Motor Vehicle Administrators (AAMVA) issued the first Personal Identification – International Specification for driver's licenses and identification cards design (updated in 2013). Many jurisdictions voluntarily comply with this specification and use it when they procure vendors to create and issue these documents.

DSA strongly supports the use of recognized standards for the creation and issuance of driver's licenses and identification cards to reduce fraud & improve citizen security. This will increase reliability and decrease identification theft while preserving individual privacy.

2.4 Secure Government Documents that Support Identity

Numerous documents issued by government agencies at all levels are used to identify the individual and establish proof of ownership, entitlement to specific privileges or compliance with legal requirements. Automobile titles provide a case in point. Vehicle ownership is typically documented by a title document issued by the state where the vehicle is registered.

Car theft is a profitable criminal enterprise, resulting in insurance claims worth more than $8 billion per year. Before implementation of the National Motor Vehicle Title Information System (NMVTIS), a thief could steal a car, take it over the state line and get a valid title by presenting fraudulent ownership documentation. Alternately, a thief could steal a car, switch the Vehicle Identification Number (VIN) plate for one taken from a junked car, and get a valid title for the stolen car. These activities were possible because the states had no quick and reliable way of validating ownership documentation prior to issuing the new title. NMVTIS inhibits title fraud and auto theft by making it harder to title stolen vehicles. Law enforcement officials can get information on any particular vehicle or title and have access to junk yard and salvage information.

With NMVTIS, jurisdictions can verify the validity of existing documentation before issuing new titles, yet many states still fail to make the investment necessary to support the creation, issuance and documentation of secure titles. As a result, automobile titles today are more secure in some states than others.

To reduce and ultimately eliminate the re-titling of stolen, wrecked and flood-damaged vehicles, DSA recommends requiring increased security of motor vehicle titles, including multiple overt and covert counterfeit deterrent and authentication devices. Some devices should be mandated for use on all titles while others should be customized for specific jurisdictions.

2.4.1 Employee ID cards

Companies today collect, create and hold more sensitive personal information than ever before. At the same time, the need to protect that information is increasing due to constituent concerns and government regulation.

The benefits of proper employee identification are clear. The pitfalls are less understood and rarely studied. Employee ID cards frequently have a photo, full name and other personally identifiable attributes. Although most establishments require government-issued identification to transact, employee identification (coupled with other easily counterfeited documents) can be a source of potential abuse.

The federal government adheres to the National Institute for Standards and Technology (NIST) recommended minimum requirements for secure personal identification verification (PIV) systems in its Federal Information Processing Standards (FIPS 201) publication. FIPS 201 establishes standardized processes and technologies designed to enhance security, reduce identity fraud and protest the personal privacy of those issued government identification.

More companies are providing PIV-interoperable credentials so their employees can enjoy the benefits of these enhanced capabilities. Non-federally issued identity cards include those sponsored by state and local governments (e.g., First Responder, Health Care ID cards), and identity cards issued by other interested entities that need to be interoperable with PIV-compliant systems.

DSA

DSA recommends that the continued support and pursuit of federal PIV-interoperable credentials be extended to the private sector. Certain private sector employees need controlled access to areas in crisis situations to maintain critical infrastructure and provide needed services. Implementation of PIV-interoperable credentials allows the inclusion of necessary members of the private sector and expedites the validation of employment identification and credentials during emergencies.

2.4.2 Academic Credentials

Academic transcripts provide records of performance for students in universities and other educational institutions. Transcrips document student performance levels that make them eligible for employment and higher learning opportunities.

Individuals who employ fraudulent academic credentials dilute the perceived quality of an institution's graduates, may perform poorly in business and demonstrate a willingness to commit fraud for personal gain.

DSA recommends that academic credentials use anti-counterfeit technologies that make illegal copying or reproduction difficult and provide a means to verify legitimate credentials. Furthermore, the issuance of these credentials must be tightly controlled by each educational institution so that electronic verification can be easily conducted on credentials presented for employment.

2.4.3 Paychecks

Check fraud is a longstanding problem. For this reason, many checks contain security features. Checks, especially paychecks, represent more than just the dollar value printed on the check. A paycheck establishes the status of one's employment, provides a rough record of earnings, and in many cases helps to prove the personal identity of the individual.

Many smaller credit-issuing entities, such as car dealerships and paycheck advance services, require nothing more than a single form of government-issued identification and proof of employment (paycheck). For this reason, fraudulent paychecks are a valuable tool for identity thieves.

Current laws protect the individual by making the issuing company a holder in due course for fraudulently cashed checks. However, if a company paycheck is counterfeited or manipulated to falsely issue credit in one's name, thus stealing the employee's identity, it adversely impacts the employee.

DSA recommends that all checks from financial institutions and companies be required to contain sophisticated overt and covert anti-counterfeit features to thwart illegal reproduction or alteration.

3. PRESCRIPTION FRAUD

Prescription fraud under Medicaid has been estimated at more than five billion dollars a year. To combat Medicaid prescription fraud, Congress enacted legislation in 2007 requiring Medicaid prescriptions be written on tamper-resistant pads/paper to be eligible for federal reimbursement.

Some states have taken action to comply with this law by adding security features and technologies to prescription pads. Other states have taken additional actions.

For example, the State of New York has implemented an end-to-end solution that identifies criminal or fraudulent transactions before the prescription drugs leave the pharmacy. This solution saved the state Medicaid program about $140 million in 2007.

DSA recommends that all prescription blanks, forms and pads contain secure and tightly controlled document security technologies that prevent or severely complicate illegal duplication or copying. States can also employ additional technological safeguards that will allow pharmacists to verify the prescription and authenticate the physician who wrote it.

4. SECURITY ASSURANCE AND RISK MITIGATION

When the Intelligence Reform and Real ID Acts were written, their congressional authors were mindful of the importance of addressing both document and issuance fraud. As a result, both laws called for greater issuance security. Moreover, the final rule of the Real ID Act specified numerous actions by issuers to prevent or detect insider fraud.

National security assurance standards address multiple areas of risk that are present within the framework of most organizations, private and public. While outlining the areas of risk that must be addressed, it also provides flexibility in mitigating those risks. By allowing multiple solutions, the standard avoids the creation of fixed barriers that might simplify the challenge to criminals seeking to identify and subvert current security methods.

The principles of security assurance give agencies multiple ways to prevent and mitigate the acts of individuals with dishonest and malicious intent. As a result, agencies such as the U.S. Government Publishing Office (GPO) are making increased use of this standard to specify broad SA requirements in procuring security-sensitive materials and technologies.

Whenever security-sensitive materials or technologies are being procured by government agencies, DSA recommends requiring that vendors comply with national security assurance standards.

5. CONCLUSION

Simple, effective, and economical solutions are available today to reduce the proliferation of fraudulent documents and, in some instances, virtually eliminate them. Yet problems persist, in part, because organizations accustomed to "business as usual" resist examining current practices. Government and business can choose from a wide range of technological tools and processes to issue more secure documents and authenticate the documents they routinely examine in carrying out their mission:

- Businesses have learned that check protections provide a significant return on investment.
- When states reduce prescription fraud, they not only take from the greedy and return to the needy; they recoup tens of millions of dollars in additional program funds without increasing taxes.
- By cross-checking identification credentials, motor-vehicle administrators don't just reject dangerous drivers; they inhibit terrorists from obtaining legitimate IDs.
- When universities and businesses work together to identify fraudulent academic transcripts, they don't just protect their own reputations; they protect society and the economy.

There are a multitude of potential solutions available to attack document fraud. As noted throughout this paper, the challenge is not technology or even cost. The challenge is getting the people and organizations responsible for issuing sensitive documents to take steps to analyze current practices and determine how to improve the security of the documents they generate and use.

The commercial, academic and government members of the Document Security Alliance have teamed together to provide an informative, objective and compelling report to the nation. We maintain a comprehensive glossary of security features and stand prepared to answer questions and provide assistance to help organizations improve the security of their documents.

DSA
DOCUMENT SECURITY ALLIANCE

204 E Street, NE
Washington, DC 20002
Phone: 202/543-5552
Fax: 202/547-6348
www.documentsecurityalliance.org
info@documentsecurityalliance.org

The Document Security Alliance (DSA) is a not-for-profit organization focused on document security at all levels of government to enhance our nation's economic, personal, and homeland security for the 21st century. DSA's goal is to leverage our government and industry members' expertise to identify methods of improving security documents and related procedures to combat fraud, terrorism, illegal immigration, identity theft, and other criminal acts.