IDENTITY DOCUMENTS

THE CONTINUED AVAILABILITY OF FOREIGN SOURCED COUNTERFEIT IDENTITY DOCUMENTS ARE A THREAT TO OUR NATIONAL SECURITY

The commercial, academic and government members of the Document Security Alliance have teamed together to provide an informative summary of the social and technical factors that influence fraud related to Birth Certificates. We now stand prepared to provide assistance and answer questions to help government organizations improve the security of their documents.

Contents

DSA
DOCUMENT SECURITY ALLIANCE

PROBLEM: HIGH QUALITY COUNTERFEITS ARE FLOODING AMERICA

In today's highly connected world, high school children with an internet connection and a small sum of money can easily obtain high quality counterfeit identification from China by accessing websites moderated in the Philippines. Smart criminals can too.

Chinese based counterfeiting operations continue to use off the shelf software along with industrial grade card printers to produce counterfeit driver's licenses and ID cards. Because materials used by these counterfeiters are often the same as those used for state driver's license issuance, counterfeits are increasingly difficult to discern from genuine licenses. Too many state and federal enforcement officers continue to rely on human sight without the assistance of image scanning forensic level devices. The consequence is that counterfeit IDs successfully pass through security inspections in critical day-to-day checkpoints.

Because of upgrades to driver's license security in line with REAL ID Act requirements, including increased state use of identity verification systems such as SSOLV and SAVE, those living or operating under assumed names are increasingly finding themselves blocked at driver's license issuing agencies when attempting to get "valid" identification.

Consequently, imposters seek high quality driver's license counterfeits and counterfeit "breeder documents", such as birth certificates. Criminal counterfeiting rings in China are providing them and the sophistication of their products grows every year. These counterfeits are dangerous, as our security infrastructure relies on our state issued identity documents.

Federal and State Laws Recognize Three Types of "False" Identity Documents:

1. Counterfeit identity documents that emulate the features and characteristics of valid IDs issued by state and federal governments. For decades, the preferred counterfeit ID is a counterfeit driver's license with an unexpired date.

2. Valid identity documents, usually issued in the name of a fictitious or stolen identity, obtained through fraudulent means.

3. Valid identity documents that have been altered after issuance to change a name, photo image, age, or other biographic descriptor.

STUDY & RECOMMENDATIONS

ID Counterfeiters Continue to Find a Ready Market for their Products:

Driver's licenses are the document of choice for identity purposes in the United States.

- A valid driver's license will get someone onto any domestic airline flight within the United States.
- Cursory visual authentication of the driver's license normally requires the inspector to make a quick determination that the features from the document, like the photograph, biographic information, security features, and substrate, are genuine.
- Driver's licenses or passports are required for Brady Gun Checks and by employers using E-Verify. They are also required as proof of identity for listed (controlled) pharmaceutical products such as OxyContin and Methamphetamine.
- Driver's licenses or ID cards are required as proof of identity at any traffic stop and are law enforcement's first line of defense against imposters.

Driver's licenses are used as proof of identity to gain access to age restricted products and facilities, high security federal buildings, and domestic travel. Though offered and often accepted as proof of identity, these cards are more appropriately understood as tokens of identity. They are but one of three basic building blocks to authenticate a person's identity.

Counterfeit IDs Impact National Security, Homeland Security, Public Safety, and the Economy:

National Security:

Jihadist terrorists and homegrown extremists have used counterfeit driver's licenses to rent cars and trucks, to buy chemicals to produce high potency explosive components, and to evade law enforcement detection – as was the case with Timothy McVeigh, for example. The 9/11 Commission Report states unequivocally that for terrorists, "Travel documents are as important as weapons" after determining that the hijackers used over 30 different driver's licenses and ID cards to open bank accounts, hide from police, enroll in flight schools, and board airplanes.

The al-Qaeda training manual instructs terrorists to obtain false identity documents to conceal their identities and terrorists have continued to follow this instruction. For example, the 2012 Burgas Bus bombers held counterfeit Michigan driver's licenses they used as "weapons" to kill 6 people. Khalid Ali-M Aldawsari was convicted for attempted use of a weapon of mass destruction in Texas for his plan to attack nuclear power plants, reservoirs, dams, and New York City streets during rush hour. His "important steps" included obtaining counterfeit and fraudulently obtained identity documents. Aldawsari lacked only a single chemical to complete his explosives before he was arrested by the FBI. A recently recovered laptop belonging to an ISIS operative held an instruction guide on moving from country to country with fake IDs, along with a bomb-building manual. The wife of an ISIS leader was detained in November 2014 as she traveled through Lebanon after she presented a fake ID.

Recommendation: Achieve nationwide state compliance with federal identity document security regulations (REAL ID) so that all documents meet the minimum standards.

Homeland Security:

The Department of Homeland Security is in the third phase of enforcing the REAL ID rules within federal agencies, with further restrictions on accessing federal buildings due on October 10, 2015. That enforcement has incentivized states that had previously refused to strengthen policies and practices regarding verification of documents offered as proof of identity. The press, and consequently the public, is now more aware of the homeland security benefits of the higher standards for identity confirmation. At this date, 22 states and Washington, DC are deemed compliant with the federal security requirements, and a like number are committed to comply. Seven states are on a collision course with DHS, meaning their residents will not be able to use their state's driver's licenses as proofs of identity when boarding aircraft in 2016. The upgrades made at DMVs to comply with REAL ID have made it more difficult to obtain a valid driver's license using fraud, but gaps remain. For example, in 2012, the Government Accountability Office

DSA

obtained fraudulent driver's licenses in three states because the clerks did not recognize that out-of-state birth certificates presented were counterfeits. Particularly of concern was that the fake birth certificates were from adjacent states to the issuing offices, and a cursory comparison to original examples demonstrated the absence of security features. The undercover federal investigators involved in the study used forged birth certificates based on those issued in Ohio and New York and successfully submitted the documents in three different states. The GAO study pointed out that virtually all states across the country are vulnerable to the out-of-state document-fraud issue.

This security vulnerability should not have existed after the provisions of the Intelligence Reform Act of 2004 were set, which mandated issuance of standards for birth certificates, along with rules for state verification of these widely varying documents. Although draft rules were prepared in 2008 by the Center for Disease Control, and subsequently approved by Health and Human Services, the Office of Management and Budget has still not approved issuance of the rules.

Recommendation: The federal rules regarding security and standardization of birth certificates required by the Intelligence and Reform Act of 2004 should be issued for public comment.

Public Safety:

Criminals often use counterfeit documents to conceal their fictitious or stolen identities to commit crimes and/or hide from law enforcement. Underage drinking and habitual DUI offenders use them to stay on the highways. Identity thieves use them to steal checks or obtain fraudulent credit cards in their victims' names. Drug dealers use them for the purchase of controlled substances, such as amphetamines, barbiturates, and narcotics like hydrocodone and oxycodone.

Enforcement of important U.S. laws, as well as our safety and security is threatened, as purchasers of counterfeit IDs use them for purposes beyond underage drinking. Additionally, the federal program for verifying eligible employees (E-Verify) and the National Instant Criminal Background Check System (NICS) used by gun stores to comply with the Brady Handgun Violence Protection Act both depend on the reliability of IDs (usually driver's licenses) presented by those subject to the check.

Silk Road was a dangerous example of almost all of the above. An anonymous online market place, Silk Road was available only through TOR - a type of software that enables anonymous communication by scrambling relays. Silk Road vendors offered anything from fake IDs to drugs to contract killers. Many, perhaps most, of the customers for counterfeit identity documents on the so-called "darknet" were career criminals, seeking higher quality products available through vendors targeting underage drinkers. This marketplace was shut down in 2013 after Immigration and Customs Enforcement (ICE) agents arrested its operator, but many of the fake IDs sold through its international internet bazaar are still in circulation across the world. The operator of Silk Road, Ross Ulbricht, was convicted on February 4, 2015 with narcotics trafficking, distribution of narcotics by means of the Internet, and conspiracy to traffic fraudulent identification documents, as well as participation in narcotics trafficking conspiracy, continuing criminal enterprise, computer hacking conspiracy, and money laundering. Mr. Ulbricht is typical of today's drug dealers who hide their true identities while they sell both illegal and controlled substances.

The newly elected Governor of Massachusetts has expressed concern that the state's Registry of Motor Vehicles requires top down reforms, after a Boston narcotics police task forces determined that local heroin traffickers were using valid driver's licenses issued under assumed names.

Massachusetts is one of the many states where driver's license fraud is a rarely prosecuted misdemeanor offense. Local city, county, and state prosecutors have the option of charging drug dealers under federal criminal law, but rarely do so [18 U.S. Code § 1028, Fraud and related activity in connection with identification documents, authentication features, and information – See Appendix].
A 2011 report indicated that 16% of inmates in federal prisons convicted on forgery and fraud charges have their offenses classified as "drug-induced". Additionally, 39% of those in jail and 42% of those in state and local prisons on convictions of forgery and fraud have their crimes classified as "drug-induced".[1] In nearly all cases, the link occurs because drug addicts can purchase controlled drugs using counterfeit

IDs, especially when combined with counterfeit doctors' prescriptions. State and federal enforcement of controlled substance act requirements is easily overcome by states with weak fraud prevention measures, and by the ease with which high quality counterfeit IDs can be purchased via the internet.

Recommendation: To constrain lawbreakers using counterfeit IDs, an ounce of prevention through rigorous enforcement will enhance public safety and significantly reduce financial losses to federal agencies and institutions. The resources expended to prosecute the providers and users of counterfeit IDs are a fraction of the benefit returned in reducing economic losses experienced by both the federal government and commercial businesses. State use of federal identity fraud laws is critical to stopping the flood of counterfeit driver's licenses.

Off shore Counterfeit ID Vendors are Still Flooding in Counterfeits:

The surge of counterfeit IDs from China began in 2011. That year, custom and Border Protection spokesman Brian Bell attested that, "Since January we have caught about 15,000 IDs. In the past we would see maybe 10 to 15 per year." In July 2011, officers in a Chicago suburb arrested 40 students between the ages of 17-20 for licenses that were hidden inside a game shipped from China. The shipment contained 1,700 fake IDs, according to the Cook County Sheriff's office.[2]

These were likely coming from IDChief, a Chinese counterfeiter responsible for the majority of counterfeit US driver's licenses. When IDChief was shut down in 2012 following an aggressive media and Congressional campaign spearheaded by the Document Security Alliance, a vacuum was left in competition for the remaining counterfeit ID customers. Many new counterfeiting websites based in China sprung up, some purportedly were associates of the IDChief operators. From October 2013 to September 2014, 4,585 Chinese made counterfeit IDs were intercepted at Kennedy International Airport alone. Bell commented again, saying his personnel were tipped off by three or four dollar tea sets being shipped to college towns, hidden deep inside of which are counterfeit IDs.[3] But this only speaks to the thousands that are discovered by the authorities. It's likely that hundreds of thousands of counterfeit IDs are in the hands of consumers in the United States and abroad.

These foreign-produced high-quality counterfeit IDs usually include bar codes that can be scanned by conventional card recognition readers used by bars and nightclubs. They are difficult to discern without the use of technology or people well trained in forensic document analysis using the special tools of the trade. Those states working to comply with REAL ID rules are training DMV personnel and local law enforcement to recognize counterfeit Driver's Licenses, notably Ohio, New Jersey, New York, and Florida. Too many other states, however, provide little or no comparable forensic document training to local law enforcement. There is also very limited use of card scanning technology by state and federal law enforcement or security personnel at ID checkpoints at airports and elsewhere.

Findings of the 2012 GAO Study:

Important GAO conclusions were:

"While most states have taken steps required by the REAL ID Act of 2005 (Act), officials in some states indicated that they may not comply with certain provisions—-such as re-verifying SSNs for license renewals"
"Identity verification procedures have been effective at combating certain kinds of fraud, but vulnerabilities remain"

"Criminals can still steal the identity of someone in one state and use it to get a license in another because states lack the capacity to ...detect such cross-state fraud.

"Officials in many states said they have difficulties detecting forged birth certificates. Verifying date of birth is also required by the Act, and a system exists for doing so, but no licensing agencies are using it because of concerns about incomplete data, among other reasons.

"GAO investigators were able to use counterfeit out of-state drivers' licenses and birth certificates to fraudulently obtain licenses in three states."

"even though relevant national systems are not yet fully operational, DHS has no plans to promote certain alternatives states can use to comply with the Act's identity verification requirements and combat cross-state and birth certificate fraud. Officials in some states indicated they needed direction from DHS in this area."[4]

DSA

THERE ARE SOLUTIONS:

Federal law enforcement by Homeland Security Investigations, U.S. Postal Inspectors, and the FBI result in arrest and conviction of only a small proportion of the criminals who produce and sell counterfeit IDs. To reduce the multiple threats to public safety, the following solutions should be considered:

Train our gatekeepers: Frontline personnel in vulnerable areas of commerce, federal building security personnel and local police should become trained in basic methods of identity document authentication, and have tools available to assist in distinguishing counterfeit IDs from valid IDs. Reference guides to state licenses are essential tools for authentication, as counterfeit driver's licenses are most often used in states other than the state from which the document is counterfeited.

Stronger card security for state and federally issued IDs and Driver's Licenses: There are a variety of effective, easy to verify optical technologies which cannot be easily copied. These can be combined with other level 2 and 3 security features to form a layered approach to security that has proven effective.

- Incorporation of levels 1, 2, and 3 security features into documents.
- Better understanding and usage of advanced authentication technologies.

Specialized and secure card production materials designed to prevent counterfeiting and that are limited in access and costly to obtain.

Provide additional guidance to state driver's license agencies under the authorities of the REAL ID Act.

The REAL ID Act of 2005 provides broad authority to the Secretary of Homeland Security regarding REAL ID rules. In December 2014, that authority was exercised to modify the final rule with regard to certain date constraints pertaining to enforcement. Systems that deliver automated confirmation of the validity of information on identity documents issued by the U.S. State Department, the U.S. Citizenship and Immigrations Services agency, and by other state driver's license agencies are available, but only a handful of states are making regular use of those systems. Similarly, state level electronic death registration systems and the nationally available Electronic Verification of Vital Events (EVVE) system are used only by a handful of driver's license agencies. The Secretary of Homeland Security has routinely supported use of these systems and obtained funding from Congressional appropriations. It is critically important that states increase utilization to prevent fraudulent use of counterfeit driver's licenses and other identity documents, to obtain valid driver's licenses under fictitious or stolen identities.

Use of ID card scanning technology for routine inspections of IDs to detect counterfeits:

- Use of technology that does more than verify bar codes. Because sophisticated counterfeits produce bar codes that are impossible to differentiate from valid IDs, ID readers MUST be able to verify security features AND bar codes.
- Use of software that captures and securely stores images and biographic information that can be subsequently used as evidence when criminal acts occur in conjunction or as a direct result of identity fraud.

Final Recommendations:

We recommend Congress emphasize strong support for enforcement of federal anti-counterfeit, law enforcement task forces.

Congress needs to affirm our national commitment to reduce financial loses and societal harm from ID counterfeiting.

We recommend our Congressional leadership support counterfeit ID prevention in a manner that prioritizes public safety, fraud reduction, and the optimization of collected revenues.

Congressional oversight hearings should challenge the Office of U.S. Attorneys to more actively prosecute criminals who employ identity fraud to commit felony offenses. Law enforcement agencies can use existing federal laws to prosecute and penalize criminals who counterfeit IDs and driver's licenses.

Previously, ICE led counterfeit and fraudulent document task forces across the country. This has been de-emphasized in recent years. Congressional interest in DHS's failure to close down offshore counterfeit ID operations would likely increase ICE's resource allocation and focus on more actively investigating counterfeit identity vendors, and lead to a greater resource allocation by the Department of Justice.

We recommend the continuation of Department of Homeland Security grants supporting forensic document training for local law enforcement.

These grants expand the capability of state and local police to identify those presenting counterfeit documents. Those representing local governments are the first lines of defense against counterfeit identity documents.

DSA

We recommend Congressional committees of jurisdiction request a GAO review of the federal agencies involved in fraud and counterfeit defense to assess and measure their improvements. They should consider adding this requirement to the respective Offices of Inspector General of the federal agencies most at risk of financial loss through crimes enabled by counterfeits.

Existing federal laws to penalize the use of counterfeit IDs are tangential to other fraud statutes – hence these crimes are rarely prosecuted. Additional Congressional Oversight would increase attention to requiring use of federal agencies to identify counterfeit IDs used to access federal buildings.

1. 18 U.S.C. Section 1028(a)(5) B Possession of Document-Making Implements;
2. 18 U.S.C. Section 1028(a)(8) B Trafficking in False Authentication Features;
3. 18 U.S.C. Section 1342 B Using a Fictitious Name or Address;
4. 18 U.S.C. Section 1546 B Fraud & Misuse of Visas, Permits, & Other Documents;
5. 18 U.S.C. Section 371 B Conspiracy;
6. 18 U.S.C. Section 1326(a), (b)(2) B Illegal Alien Found in the U.S. Following Deportation

We recommend law enforcement agencies use existing federal statutes to successfully prosecute crimes.

A 2011 Los Angeles criminal case illustrates how federal statutes were used to prosecute more than two dozen individuals in a massive fraudulent document operation. The ID ring was producing counterfeit driver's licenses for 40 of 50 U.S. states. These counterfeit IDs were used in the "commission of credit and bank fraud, tax fraud, identity theft, and pharmaceutical diversion schemes... the false document manufacturing ring produced raw materials for the manufacture of thousands of documents per month that were distributed in California and across the United States."[5]

CONCLUSIONS:

ID counterfeiting facilitates a wide range of illegal activities. The cost to society far exceeds the naïve popular perception that "Fake IDs" are only for underage kids trying to get into a bar. Transnational criminal gangs operate across the United States counterfeiting driver's licenses, birth certificates, and other identity documents costing consumers, businesses, and government benefits agencies hundreds of millions of dollars annually. ID Counterfeiting has become a major gateway for criminals to steal, injure and, in some cases, terrorize the public. Federal laws sufficient to criminalize ID counterfeiting already exist, as do the agencies authorized to enforce them. As Congress considers how best to reduce the current deficit, it's important to consider that the fraud prevention savings to commerce and society well exceeds enforcement costs. Our nation's commitment to continue to fund identity document protection should not be in question.

Citations:

1. Department of Justice: National Intelligence Center. "Economic Impact of Illicit Drug Use on American Society." April 2011. Pp ix, 56-62.
2. Staver, Anna. Kent Patch. "Kent State Students Reach Plea on Fake ID Charges". 10/6/11.
3. Fliegelman, Oren. New York Times. "Made in China: Fake IDs". 2/6/15.
4. United States Government Accountability Office (GAO): Report to Congressional Requesters: September 2012: Driver's License Security: Federal Leadership Needed to Address Remaining Vulnerabilities: GAO-12-893:
5. Federal Bureau of Investigation. "More Than Two Dozen Identified in Massive Fraudulent Document Manufacturing Operation in Los Angeles".11/3/11.

DSA

APPENDIX:

Important Federal Definitions to Prosecution of ID Counterfeiting Crimes:

TERM	DEFINITION	US CODE
Authentication Feature	the term "authentication feature" means any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with another feature is used by the issuing authority on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified;	18 USC 1028 (d)(1)
Identification Document	the term "identification document" means a document made or issued by or under the authority of the United States Government, a State, political subdivision of a State, a sponsoring entity of an event designated as a special event of national significance, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals;	18 USC 1028 (d)(3)
False Identification Document	the term "false identification document" means a document of a type intended or commonly accepted for the purposes of identification of individuals that-- (A) is not issued by or under the authority of a governmental entity or was issued under the authority of a governmental entity but was subsequently altered for purposes of deceit; and (B) appears to be issued by or under the authority of the United States Government, a State, a political subdivision of a State, a sponsoring entity of an event designated by the President as a special event of national significance, a foreign government, a political subdivision of a foreign government, or an international governmental or quasi-governmental organization	18 USC 1028 (d)(4)

DSA

False Authentication Feature	the term "false authentication feature" means an authentication feature that-- (A) is genuine in origin, but, without the authorization of the issuing authority, has been tampered with or altered for purposes of deceit; (B) is genuine, but has been distributed, or is intended for distribution, without the authorization of the issuing authority and not in connection with a lawfully made identification document, document-making implement, or means of identification to which such authentication feature is intended to be affixed or embedded by the respective issuing authority; or (C) appears to be genuine, but is not	18 USC 1028 (d)(5)
Issuing Authority	the term "issuing authority"-- (A) means any governmental entity or agency that is authorized to issue identification documents, means of identification, or authentication features; and (B) includes the United States Government, a State, a political subdivision of a State, a sponsoring entity of an event designated by the President as a special event of national significance, a foreign government, a political subdivision of a foreign government, or an international government or quasi-governmental organization	18 USC 1028 (d)(6)

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.