White Paper

How DMVs can Help Prevent Fraud and Improve Public Safety

Verify and Authenticate Identities before Issuing a Driver's License or State Identification Card.

February 2015

LexisNexis®

Risk Solutions
Government

For the majority of Americans, a state-issued driver's license is the form of identification they use most often. Once viewed simply as a document granting authority to operate a vehicle, driver's licenses are now predominantly used to verify the identification of an individual. Once obtained, a license can be used to open a bank account, apply for social services benefits, obtain passports or social security cards, or hundreds of other actions. A fraudulent driver's license with the picture of one individual and the identification information of another can easily become the foundation for fraud, deception and other illegal activities.

Fraudulent identifications lead to many concerns – including a serious threat to officer and public safety – and can become the gateway for individuals to go undetected when:

- Driving with a suspended or revoked license
- Evading arrest on an outstanding warrant
- Gaining government-issued benefits such as housing, healthcare or nutrition assistance
- Travelling unabated as a member of a terrorist watch list

State departments or bureaus of motor vehicles work diligently to properly identify individuals applying for a driver's license, as front-line agents in helping to prevent fraud and keep the public safe. However, many state Department of Motor Vehicles (DMVs) do not have the tools they need to verify and authenticate identities. As a result, they are often faced with incomplete, inaccurate or fraudulent identification information.

Did you know?

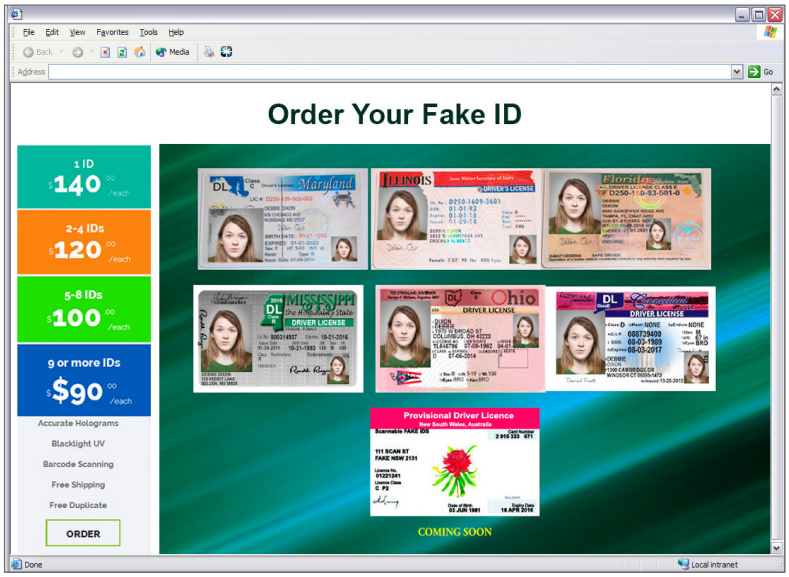
18 of the 9/11 terrorists held fraudulently obtained original driver's licenses issued from multiple states.*

It's a tough job

The U.S. Census Bureau reports that 14.1 percent of the U.S. population, or 44,200,000 people, move every year. This increases the likelihood of duplicate or outdated licenses.**

How are fraudulent licenses obtained?

When a person goes to the DMV to obtain a driver's license, the first step is to substantiate their identity and a permanent address. Fraudsters use easy-to-falsify identity and residency documents such as birth certificates, rental agreements and bank statements to establish their false identities. Unfortunately, these documents can be easily modified and difficult to determine if they are fake, resulting in DMV employees facing an uphill battle, even with the provided equipment and training. In fact, there are numerous services online that tout their ability to create fake documentation that will pass any scanner, black light or other test to prove authenticity.



Adding to the complexity are recently adopted state and federal laws around identification and driver's licenses. For example, the REAL ID Act of 2005 establishes minimum standards for state-issued driver's licenses and identification cards in order to be used as a acceptable ID on federal premises. Additionally, in January 2015, California Assembly Bill 60 (AB 60) went into effect. AB 60[1] requires the California DMV to issue driver's licenses to applicants who are unable to submit proof of their legal presence, but meet other qualifications and can prove residency in California. It is estimated California will issue licenses to 1.4 million undocumented residents over the next three years.[2]

As states continue to address issues of immigration and seasonal workers, DMVs across the nation will be faced with new challenges – and new means for fraudsters to try to obtain false identification documents.

Impacting public safety

Any fraudulent licenses pose a serious safety threat. Perhaps most common is an individual who has a suspended or revoked license due to poor driving or a DUI, and procures a fraudulent driver's license, or even worse, a Commercial License. Even an individual who has not passed an eyesight or driving test puts the safety of pedestrians, law enforcement officers and other drivers in peril every time he/she takes the wheel.

From a more nefarious standpoint, someone with a fraudulent driver's license may also use that license to procure license plates. License plates affiliated with a different identity allows the driver to avoid the notice of law enforcement, avoiding a warrant for an arrest or to transport illicit/dangerous goods – and potentially endanger law enforcement officers should they have to engage with an unknown, criminal driver

Contributing to fraud

A 2012 U.S. Government Accountability Office (GAO) report studied the methods of surrendering a current license from one state and obtaining a new license from a second state. To test the system, GAO created fraudulent driver's licenses and then used the licenses to obtain a new, secondary license from other states. It was determined that of the three states tested, all three of them accepted, and never checked the validity of the surrendered (fraudulent) licenses. The GAO successfully traded a fake for a real license, allowing the fake identity to now "live" on an official government document, and serve as the basis to defraud that same government – a significant flaw in the system.

Over the last 10 years, government programs have become highly vulnerable to this type of fraud. For instance, the Taxpayer Advocate Service, the

Internal threats

Occasionally, DMVs even face threats from within as opportunistic employees may be tempted to sell or falsify information in exchange for a fee. There are numerous stories of former DMV employees being sentenced to prison for involvement in conspiracies to sell official driver's licenses to ineligible individuals. Read real stories on FraudoftheDay.com.

watchdog organization within the Internal Revenue Service (IRS), recently reported that identity theft-related tax refund fraud has increased 650 percent since 2008. Similarly, Unemployment Insurance fraud cost taxpayers an estimated $3.3 billion. Licenses issued under a false identity can help perpetuate these types of fraud. False documents become the foundation for other crimes.

What can be done?

With so many variations in identity documentation and easily falsified residency documents, how are DMVs working to prevent issuing a gateway to criminals and fraudsters? DMVs utilize the Social Security Administration's Social Security Number (SSN) verification system as a first line of defense to determine if an identity is real or fabricated. The SSN ties an individual's name, date and place of birth together to create an identifier that is supposed to be unique. Over the last 10 years, theft and misuse of identity information such as SSN's has become commonplace and, unfortunately, the value of the uniqueness of the SSN is questionable.

In addition, synthetic identities have also become common. A synthetic identity is one where a portion of the identity information is modified allowing the new identity to look like another person, thus creating difficulty in identity resolution. Getting a license for a synthetic identity creates serious issues: who is the real party, where do they live and how can authorities contact them?

DMVs need a system to ensure they know with whom they are interacting ...every time. They need to confidently verify the identity documents represent an actual live person and establish the identity is not fictitious by confirming the date of birth, name and SSN match an actual living person, not a fabricated identity. In addition, they need to be able to authenticate the identity and confirm that the person they are interacting with is the actual owner of that identity. This can be done in real-time using identity proofing solutions prior to issuing any driver's license and any time the individual accesses DMV services, both online or in person.

Identity proofing

Identity proofing technology is the key to overcoming these challenges and helping DMVs detect and prevent driver's license fraud. Identity proofing quickly and efficiently answers two important questions:

1) Is the identity presented real? (Does this person exist?)

2) Does the identity belong to the citizen? (Are you who you say you are?)

The first step in the process is identity verification, which enables the DMV to determine that the identity being presented actually exists. This is

Partnering to fight crime

On a positive note, some organizations and government agencies are working together to share information – helping to reduce instances of fraud and mitigate threats. The American Association of Motor Vehicle Administrators (AAMVA) has a system that verifies credential data against motor vehicle agencies to reduce identity theft and documentation fraud.

A synthetic or fabricated identity:

Using numerous aliases and slightly modified SSNs, criminals are able to obtain multiple IDs that exist under completely different records.

Real full name = Laurence Kevin Benson.

Modifications:
Larry Benson
(123-00-6789)

Lawrence K. Benson
(128-00-6789)

L. Kevin Benson
(123-00-6787).

accomplished by running it through a series of algorithms to determine if the information entered is a valid person. Proper verifications are made possible by analyzing a vast amount of personal data confirmed by thousands of public and private records.

The next step is to authenticate that the person executing the transaction is in-fact the owner of the identity. This can be done through knowledge-based authentication, a quiz that generates random, multiple choice questions for an individual derived from non-wallet based data – information that could not be obtained by simply looking through a wallet – using public, proprietary and the agencies internal databases. The external databases complement those databases typically accessed by DMVs and provide a more complete view of the identity being presented. The advanced quiz engine tailors questions to the individual requesting the driver's license, offering identity verification input options beyond just name, address and SSN, which can be easily falsified. Configuring the quiz to select the types of questions and the number of questions presented, response times and acceptance/decline criteria provides users with a superior interactive experience while allowing the agency to manage the authentication risk.

Unique Identifiers

The underlying component of the identity proofing approach is the establishment of a unique identifier. A unique identifier, using advanced linking technology, will resolve identities based upon different identity characteristics associated with an individual from both traditional agency information as well as how they have represented themselves to organizations outside the DMV.

Augmenting existing files with a unique identifier allows DMVs to:

1) Spot individuals that apply for multiple driver's license or identification card under similar aliases with slightly modified SSNs. By appending a unique identifier they can be resolved to a true, single identity.
2) Identify fraud tied to the use of identities from deceased or incarcerated individuals on a state and national basis.
3) Catch individuals using false residency documents or false SSNs to obtain a license in order to evade law enforcement, gain social services benefits and/or defraud organizations.
4) Protects citizens by limiting exposure to fraud and mishandling opportunities of the individuals SSNs

A unique identifier links and organizes multiple pieces of information quickly and accurately, all while protecting private information such as SSNs and resolving errors that may exist in a system.

The power of LexisNexis

The LexisNexis identity proofing solutions are backed by decades of identity management experience across multiple industries. With access to over 37 billion public records from more than 10,000 data sources powering our identity solutions, DMVs can quickly validate and authenticate identities with confidence, helping stop false identities from entering DMV systems, reducing driver's license fraud and improving overall public safety. LexisNexis securely offers information on 585 million unique identities in the U.S. In addition to the vast majority of current citizens, this also includes the deceased, incarcerated and many foreign nationals.

Using the power of the LexisNexis patented linking technology, LexID®, DMVs can identify, link and organize information quickly with a high degree of accuracy, turning disparate information into meaningful insights. The combination of advanced linking technology, paired with our collection of public records, gives agencies the ability to identifying individuals that are deceased or incarcerated, those that have never lived in the state but hold a license, live at a different address than claimed, claim SSNs that do not match the name of the license holder, claim SSNs that do not exist, list addresses that do not exist, or have identities with multiple associated SSNs to ensure licenses are only issued and used by the actual owner of the identity presented. By leveraging the LexID, agencies gain the most accurate and complete picture of an individual possible while protecting citizens' personal information, reducing fraud and increasing public safety.

Preventing driver's license fraud is a critical component to help ensure the nation's public safety. By identifying fraudsters, DMV employees can help keep citizens safe and keep public assistance going to those who truly meet the requirements.

Sources

1 Assembly Bill (AB) 60 (Chapter 524: Statutes of 2013), http://dmv.ca.gov/portal/dmv/detail/ab60/index?lang=en

2 Parker, Bruce. "Driver's licenses a magnet for immigration fraud in Vermont." Watchdog.org. 22 January 2015

For More Information

Learn more about how states are already using these solutions to prevent fraud. Visit IdentityGov.com/DMVFraud and request a demonstration or contact 888.579.7638.

About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions (www.lexisnexis.com/risk/)is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

LexisNexis®

NXR11051-00-0215-EN-US