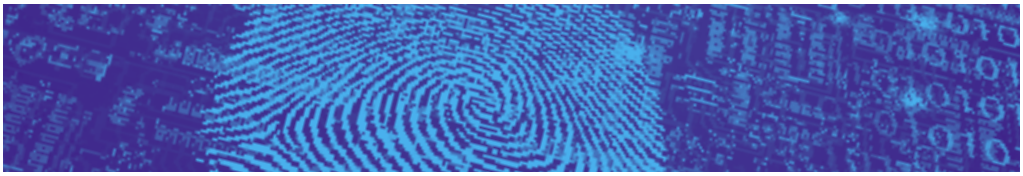
AAMVA

American Association of
Motor Vehicle Administrators

External Fraud
Identity Theft
DMV INVESTIGATORS
Facial Internal Fraud
Recognition
TERRORISM

Best Practices for the Deterrence and Detection of Fraud



March 2015

LAW ENFORCEMENT STANDING COMMITTEE
INTERNAL FRAUD WORKING GROUP, EXTERNAL FRAUD WORKING GROUP

Cover photo credits: “Eye Scan” and “Fingerprint” © Thinkstockphotos.com;
“DMV Investigators” courtesy of New York Department of Motor Vehicles

Contents

Executive Summary

Credentials issued by departments of motor vehicles (DMVs) are extremely valuable. They prove a person's or vehicle's identity, demonstrate the ability to drive safely, and show ownership of vehicles. But for individuals wishing to commit a crime, they can be a golden ticket to riches or anonymity.

Since 9/11, administrators and other stakeholders have come to realize that in addition to highway safety responsibilities, DMVs are on the front lines of national security and identity protection. The need to deter and detect fraud is greater than ever.

An understanding of what motivates fraudsters can go a long way in identifying behavioral risk factors. DMVs need to create environments that endorse ethics and encourage employees to do the right thing at every turn, making the perpetration of fraud as difficult as possible. Anti-fraud messages must be constantly repeated to remind employees that it is a priority for the organization. When fraud is identified, organizations need to take swift and severe action against the fraudsters. Sending such a message will, in and of itself, help deter fraud.

DMVs should regularly review processes throughout the organization and look for weaknesses or areas where fraud or theft could occur. Once identified, changes to reduce the threat should immediately be implemented. Audit and oversight should be a regular part of daily operations. Regular, random, and spot monitoring should take place for all staff. A tip line can help root out fraud by giving employees and the public an anonymous way to report fraud.

In addition to having strong processes and oversight in place, critical to the fight is a sufficiently staffed and properly equipped fraud unit. In addition to investigating fraud, the unit can serve as watch guards and minimize the potential for fraud throughout the organization. The unit can assist with the development of anti-fraud training and can review proposed legislation with an eye on fraud. It can review RFPs and proposals and make recommendations on document security. Investigators with enforcement authorities can access databases that might otherwise be unavailable and make the unit eligible for additional grant funding from federal agencies focused on the fight against fraud.

The benefits of combating fraud far outweigh the cost. Only with the proper staffing, resources, and technologies in place can the DMV be successful in the ever-increasing challenge of fighting fraud.

The reality of fraud may be seen as a negative, but it also comes with opportunity. Opportunities to form effective partnerships, strengthen the organization, garner positive publicity, enhance business practices, reaffirm policies, improve morale, and publicize successes exist while improving an agency's ability to deter fraud.

By publicizing arrests and prosecutions, the visibility and reputation of DMVs are enhanced. The public and the legislature will begin to see the DMV as a force for good and as an agency that is diligent in its responsibilities to protect the information and products for which it is entrusted. The public will feel more confident that their personal data are entrusted

to an agency whose priority is security. Legislators will appreciate the fact that funding dollars to support a fraud unit are well spent.

DMVs should take the opportunity to issue press releases and promote successes in combating fraud without providing investigative tactics or sensitive case details.

The Internal and External Fraud Working Groups realize that the risk of fraud can never be completely eliminated. Those who are sufficiently motivated to override or circumvent them can usually find a way to do so. The mechanisms individuals use to perpetrate fraud are continually evolving, and DMVs must be ever vigilant to keep up with the pace of criminal activity.

Chapter One Background

The implementation of the U.S. Commercial Motor Vehicle Safety Act of 1986 exposed significant security loopholes in driver license (DL) issuance processes throughout the country. Before the Act, individuals had been readily able to obtain multiple DLs and identification cards (DLs/IDs) in either a single or multiple jurisdictions. As a result of such fraud, as well as illegal activities in general regarding identification documents, the American Association of Motor Vehicle Administrators (AAMVA) and its members recognized a need to improve the issuance process for DLs/IDs.

In the early 1990s, AAMVA resurrected and updated the Fraudulent Identification Prevention Program (FIPP), which provided training resources to assist front-line staff in the detection of fraudulent documents, and verification of authentic documents at the time of DL or ID card application. FIPP evolved to today's Fraudulent Document Recognition Program, which is the most widely used training program AAMVA offers. In 1996, AAMVA released a Model Program for Uniform Identification Practices, which included solutions to close many of the identification security loopholes. Components of the program were adopted by some, but not all, DMVs throughout the United States and Canada. In 2000, AAMVA created the Uniform Identification Subcommittee (UID Subcommittee) to update and maintain the work of the Uniform Identification Working Group.

The impact of the use of fraudulently obtained DLs/IDs was highlighted by the events of September 11, 2001. Consequently, the business processes and procedures, as well as the supporting internal controls under which credentials were issued, became the focus of intense scrutiny.

Throughout 2002 and 2003, the UID Subcommittee reviewed the DL/ID issuance and enforcement practices of DMVs, law enforcement agencies, and stakeholder communities. The UID Subcommittee sought information, research, and advice from the private sector; AAMVA members; AAMVA's board of directors; various consultants; federal agencies; and associations such as the International Association of Chiefs of Police (IACP), National Sheriff's Association (NSA), and National Association for Public Health Statistics and Information Systems (NAPHSIS). The UID Security Framework was the resulting product based on recommendations of the many who provided input.

In 2009, at the request of its membership, AAMVA formed the Internal Fraud Working Group. Two deliverables were assigned to the group. The first was to create a *Best Practices Guide* to assist DMV administrators and their staff in considering the implications of internal fraud inside the DMVs. The second was to create a checklist to assist administrators in assessing, deterring, and detecting internal fraud within the DMV environment. Realizing internal fraud is not limited to a single type of transaction or area, the Working Group—with input from the jurisdictions—endeavored to include information regarding the numerous venues by which internal fraud could be perpetrated.

In 2012, AAMVA formed the External Fraud Working Group to develop a best practices document addressing the detection and deterrence of fraud by those doing business with the DMV, whether it is a

partner or a customer. The group reviewed and revised the existing fraud document and added pertinent information regarding external fraud. The result is this single comprehensive document that addresses both internal and external fraud.

In November of 2013, AAMVA's Facial Recognition Working Group met for the first time. The group was chartered to review the methods used by motor vehicle agencies (MVAs) to capture, review, and share facial images, and when appropriate, investigate potential matches and pursue prosecution when fraudulent activity is discovered. The Working Group is slated to release a best practices document related to the capture and utilization of images by August 2015.

Administrators must be ever vigilant toward new methods of committing fraud against the organization. Agencies are encouraged to share their experience and solutions with their peers. Working together is an invaluable tool in the fight against fraud.

Chapter Two Fraud Defined

The *Merriam-Webster Dictionary* defines fraud as: 1) the crime of using dishonest methods to take something valuable from another person, 2) a person who pretends to be what he or she is not in order to trick people, and 3) a copy of something that is meant to look like the real thing in order to trick people. All of these definitions describe methods used to commit fraud against DMVs. In today's environment, the risk of fraud is higher than ever before.

The documents issued by DMVs have tremendous street value for those who wish to commit crime or illegally obtain financial benefits and entitlements. Falsely obtained DMV documents are used to perpetuate identity theft, human smuggling and trafficking, gang activity, financial fraud, illegal immigration, terrorism, and other national security threats, to name a few. Criminals have tremendous incentive, and deep pockets, to tempt DMV staff into issuing genuine documents under false pretenses. They have the means to obtain legitimate-looking documents and use them to apply for genuinely issued credentials.

The reasons individuals commit fraud are vast and should not be underestimated. Someone who would not otherwise ever consider theft or fraud may find him- or herself in a desperate situation and choose to perpetrate a crime.

DMVs are subject to fraud from almost any arena in which they do business—internally by those working for the agency or those serving as agents of the agency, and externally from entities that provide or receive information, as well as those transacting business with the agency. Collusion between internal and external parties is also a risk. Non-DMV entities produce fraudulent identity and vehicle documents that may eventually be submitted to the DMV with the intention of receiving an officially issued credential.

When you think of fraud in the DMV, you likely think of someone who wants a DL for illicit purposes or a person who wants to wash a title in order to sell a damaged or stolen vehicle. In reality, these examples of "external" fraud—fraud solely perpetrated by an outside entity—are only a piece of the fraud problem. The unfortunate reality is that "internal" fraud may be just as big of a problem, if not more so, as the fraud committed by customers or third-party partners. Employees and agents of a DMV who commit fraud may accept bribes for issuing documents in violation of procedures, steal money or indicia, issue credentials without proper documentation, remove tickets or suspensions from a record, fail to report audit violations, swipe inventory, give a test applicant an undeserved passing score, and much more.

External fraud is fraud perpetrated by customers, third-party agents, car dealers, insurance providers, emissions or safety inspection stations, driver training schools, third-party testers, ignition interlock providers, courts, banks, auto auctions, junk and salvage dealers, medical professionals, indicia providers, record providers, armored car companies, and others who do business with the DMV. The ability of individuals associated with these entities to perpetrate fraud can be found in nearly every part of the organization.

The Psychology of Fraudsters

Fraud involves deception, purposeful intent, risk of apprehension, violation of trust, rationalization, and other factors. It is therefore important to understand the psychology that might influence the behavior of fraud perpetrators. We sometimes wonder why people commit fraud, why they steal things, and what goes through their minds in committing illegal acts. The answers to why people commit fraud can be explained by Donald R. Cressey's famous concept, developed in the 1950s. Cressey, a criminologist, came up with a theory to explain the basics of fraud. According to Cressey, there are three elements present in every fraud: motivation, opportunity, and rationalization, referred to as the "fraud triangle." Breaking the fraud triangle is the key to fraud deterrence.

Motive

In this element, a person feels pressure or feels a need to commit fraud. It might be a financial need such as expensive medical bills or other type of debt. Another possibility is the desire for material goods. The individual, a close family member, friend, or acquaintance, may have a gambling, drug, or spending problem. The reasons individuals commit fraud are vast and should not be underestimated. Someone who would otherwise never consider theft or fraud may find him- or herself in what he or she considers a desperate situation and choose to perpetrate a crime.

Opportunity

When there is a need, the fraudster looks for opportunities to commit fraud. Internal fraud may be committed by employees with access to records, documents, or other information that allows them to commit fraud. Internal access, as well as knowledge about what goes on in the organization may make it easier for an individual to commit fraud. Of the three elements, removal of opportunity is most directly affected by a system of internal controls and generally provides the most actionable route to deterrence of fraud.

The majority of tips reporting fraud come from employees of the organization. Agencies need to have mechanisms in place for employees and others to report fraud—and to do so anonymously if they wish.

Rationalization

Fraudsters rationalize their behavior by convincing themselves that committing the crime is okay. They think, "I deserve it," "after this one, I'm done," "they don't pay me enough," "others do it," "I was passed over for a promotion," or "I'll pay it back," among other rationalizations. Fraudsters may also justify their behavior by convincing themselves that they need it more than their employer. Some believe that their personal need is greater than that of the organization. Many do not believe their fraud will have a significant effect.

BEHAVIORAL FACTORS ARE KEY

Some may overlook employee behavior as an indication of possible fraud. As incidences of fraud rise, placing the spotlight on behavioral factors may be an important approach to both fraud detection and deterrence. In its 2014 *Report to the Nation*, the Association of Certified Fraud Examiners (ACFE) estimated that the typical organization loses 5% of its annual revenue to fraud.

According to ACFE, in 92% of cases, the fraudster displayed one of the behavioral flags often associated with fraudulent conduct. In 64% of the cases, two or more behavioral flags were identified. Living beyond means (43.8% of cases), financial difficulties (33%), unusually close association with vendors or customers (21.8%), and excessive control issues (21.1%) were the most commonly observed behavioral warning signs. Occupational fraud is more likely to be detected by a tip than by any other method. The majority of tips reporting fraud come from employees of the organization, so it is important that agencies have

mechanisms in place for employees and others to report fraud.

Fraud is not a new crime. The history of business, and indeed humankind, is littered with misrepresentation for unlawful gain. In their "12th Global Survey on Fraud," Ernst and Young found that bribery, corruption, and fraud remain widespread and that despite the risk, companies are still failing to do enough to prevent bribery and corruption. Previous Ernst and Young surveys found that 85% of the worst frauds were committed by insiders, people who were on the organization's payroll. They also found that more than half of the perpetrators were from management, a one third increase from the previous year. An interesting finding was that although the managers had been with the organization for some time, about half of those who committed fraud had been in a management position for less than a year.

In tough economic times, with budget cuts, layoffs, and furloughs—often a standard part of doing business—internal fraud will almost certainly increase. Employees who experience a reduction in their family income—no matter the reason—will look for ways to make up the loss. When the California DMV was forced to reduce staff throughout the agency because of budget restrictions, it had the wisdom to increase its investigations staff, knowing internal fraud would increase. This insight was proven to be a reality, time and time again, and their foresight paid off.

An Ernst and Young survey found that 85% of the worst frauds were committed by insiders, people on the organization's payroll.

In addition to economic issues, events such as birthdays, the start of school, Christmas, tax time, and medical or unexpected home expenses may be driving factors that result in an increase in fraud. High staff turnover increases an organization's exposure to fraud. Managers should take note of employees who appear to live above their means or have gambling issues, alcohol or drug problems, or personal financial crises, and they should take steps to more closely scrutinize the work of such individuals.

It is difficult to determine who may perpetrate fraud on the DMV. When presented with seemingly identical opportunities and motives, why does one person commit fraud but another does not? There is no clear answer. Some of the factors affecting organizational fraud include:

- The degree to which an employee identifies as being part of the organization
- The perception of detection
- The financial condition of the organization
- Internal accounting controls
- The integrity level of leaders and employees
- Commitment to the organization's value system
- Personal traits and characteristics of executives and employees
- Employee reward systems for ethical behavior
- Organizational culture and dynamics
- Peer pressure
- The swiftness, certainty, and severity of punishment
- Mechanisms available to report fraud

The Demand for Fraudulent Identity Documents

Criminals covet counterfeit or fraudulently issued documents to mask their identities, places of residence, or their criminal activities. False identification documents fall into three categories: borrowed, altered, and fake (fraudulent). The most common form of illegal ID in use today is the borrowed ID. Typically,

these are used by persons younger than 21 years of age who obtain identification from those who can legally drink. The sources may be siblings, friends, or IDs obtained through friends. Altered IDs involve making physical changes to a real ID. This most commonly involves the changing of the birth date or photo. With improved security features on government-issued IDs, the alterations of these documents have become less frequent.

Fake or fraudulent IDs are documents that purport to be a genuine identification document. These documents may appear to be real IDs as issued by a government entity; others may have no similarity to the documents being issued but are designed in such a way that a person may believe it to be a real document. In recent years, an influx of high-quality counterfeit identification documents (primarily driver licenses) has been produced en masse both domestically and internationally. These documents replicate enough security features to enable holders to board an aircraft, enter a federal building, set up a bank account, and establish credit. The documents typically sell for as little as $200 and can be easily purchased online in any identity the recipient wishes to assume. A primary concern of such documents includes reciprocity agreements among DMVs because the individual may potentially purchase a high-quality counterfeit and obtain a genuine DMV-issued identification document from another jurisdiction using the fraudulently issued DL. This represents a threat to both homeland security and highway safety.

Document fraud investigations by Department of Homeland Security's (DHS's) Homeland Security Investigations (HSI) have found previously convicted felons and criminals involved in nefarious activities ordering false identification documents. Included are individuals who were involved in identity theft, drug distribution, money laundering, and other criminal activities. In one case, HSI seized approximately $1.3 million from a website operator who was selling counterfeit DLs domestically and internationally. He was arrested, pleaded guilty, and is currently in prison. One of the recipients of the fake DLs in that case was sentenced to 15 years in federal prison for narcotics distribution. In another instance, forensic examination of the seized computers revealed a group of 30 IDs purchased by one individual. Each of the IDs was in a different name and had a different date of birth, and the IDs were from more than 15 different states. In another instance, a woman purchased approximately 25 IDs for five persons, all adults older than 21 years of age. Each of the IDs was in a different name and date of birth. More than 15,000 fake DLs were produced by the defendant during the course of his criminal activity. The website offered DLs and IDs from every U.S. jurisdiction.

In another case, HSI shut down a document vendor that produced more than 20,000 high-quality fake DLs. The owners and operators of the website were arrested. HSI seized more than $2.1 million, 19 firearms, and thousands of false driver licenses during the investigation.

Criminals have cited avoidance of detection as a primary means of obtaining counterfeit documents or committing identity fraud. Simply stated, criminals understand the need to obtain an additional identity to avoid detection by law enforcement. The criminal threats stem from the fact that the DL is a perfect "breeder" document for establishing a false identity. The use of a false identity can facilitate a variety of crimes, from money laundering to check fraud. False identities also serve to conceal criminals sought by law enforcement.

The Complex World of Vehicle Fraud

Vehicle fraud can take on many faces. A vehicle is one of the biggest purchases an individual will make, and the potential profit to be made by those wishing to cheat the system is considerable.

A common type of fraud related to vehicle titling occurs when information on an existing valid

certificate of title is altered. The most common alterations are made to the odometer reading, odometer status, title issue date, vehicle brand information, and purchase price. Although jurisdictions make extensive efforts to use title documents that resist alteration, alterations continue to be a concern. Although many alterations are amateurish and readily detectable by an experienced and trained title clerk, they are often good enough to fool potential vehicle purchasers. Alterations can be as simple as writing over printed information or scratching or scraping information from an existing title and replacing it with new information. Unfortunately, innocent purchasers often do not become aware of the fraud until they attempt to obtain a new title at the DMV. More sophisticated criminals use a variety of chemicals and other procedures to erase or alter information on a title and add new information where needed. Criminals also make use of high quality color copiers to create or copy vehicle titles, and the copies help to disguise any alterations made on the original title.

Fraud can also take place in private party (non-dealer) purchases. Such fraud may involve only the purchaser, only the seller, or both. Fraud involving only the purchaser most commonly occurs when the purchaser understates the purchase price of the vehicle or records an incorrect purchase date in order to lower the fees or taxes required. A detriment to the jurisdiction in this situation is a loss of revenue through lower taxes and fees. Fraud committed by the seller would most commonly occur through a false odometer disclosure when selling the vehicle. Fraud involving both the seller and buyer could occur when the two parties agree on a false selling price, transaction date, or odometer disclosure.

Although less common, fraud involving third parties, such as dealers, large fleet owners, or auction companies, also occurs. Third-party fraud most commonly involves alteration of information related to odometer reading, odometer status, and brand information. Third parties accomplish document alteration using any and all of the methods described previously.

Vehicle cloning is a highly lucrative crime. Car thieves often travel across state and international borders to sell cloned vehicles at the highest prices. Altering the title to match the vehicle provides the document necessary to transact a sale of the vehicle to an unknowing buyer. And having a document that looks legitimate increases the value of the vehicle for the seller.

Individuals may provide false information to obtain a duplicate title. The applicant indicates that the title was lost, mutilated, or stolen when in fact it is in his or her possession or known to be in the possession of another. This is often done to obtain multiple loans for the same vehicle. The lender learns of the fraud when trying to record the lien.

Examples of Vehicle Fraud

- Wrecker services submit false storage liens to gain ownership of vehicles and then sell them for a substantial profit
- False trades allow for the circumvention of required taxes
- Using counterfeit and stolen titles to transfer ownership for a cloned (stolen) vehicle
- Fictitious identification or Social Security Number is used to apply for title transfers
- Providing false addresses to facilitate titles transferred in a county that does not scrutinize each transaction for authenticity and validity
- Estranged spouses or family members may forge the owner's signature and sell the vehicle while the owner is away or incarcerated
- Fraudulent disclosure of the vehicle purchase price
- Use of minimally repaired salvage vehicles in staged accidents or insurance fraud
- "Paper" vehicles are false advertisements via online services where money is exchanged without physically inspecting the vehicle
- Curbstoning—the repeated, unlicensed flipping of used cars; that may or not be owned by the person doing the selling
- High-dollar vehicles titled or registered in other jurisdictions to avoid fees

Unlicensed individuals or organizations may sell vehicles whose odometers have been altered so the true vehicle mileage is masked. Criminals often target high-mileage vehicles or those that are 10 years of age or older. Such vehicles are often marketed on the Internet and sold to unsuspecting buyers who believe the mileage displayed is true and accurate. Vehicles are subsequently purchased at a price higher than their true value.

Vehicle-related fraud is almost always committed to increase the value of the vehicle. Lowering a vehicle's odometer reading, removing vehicle brands, or changing the odometer status (e.g., changing it from UNKNOWN to ACTUAL) will increase the retail value of a vehicle. It makes the vehicle more valuable to the seller and makes unknowing purchasers more willing to pay a premium price for a vehicle that appears to be "clean."

Fraud and Highway Safety

Fraud has a negative effect on highway safety. Individuals who cheat on a knowledge or skills test or those who collude with a DMV employee to receive a passing score because they do not possess the knowledge or skills to drive safely may be licensed to operate a motor vehicle through fraudulent means. These individuals put others at risk and pose threats to the lives and property of others. Those who use falsely obtained DLs may use their ill-gotten document for criminal activities on our highways, putting others at risk. Individuals may receive a DL for a higher class than they are qualified, meaning they do not have the skills necessary to safely operate the large vehicle. There is also a public safety concern with individuals who are issued driving privileges when they are not medically eligible to drive.

Federal officials have identified a growing trend in which DMV employees use their access to equipment and data to sell genuine DMV-issued identification documents or information. These individuals have access to information, tools, and technology—computers, cameras, production equipment, and paper or card stock—that allows them to issue genuine documents under false pretenses. Criminal and terrorist organizations value high-quality, fraudulently issued documents and are more than willing to bribe a DMV employee to obtain them.

It is not, however, only the criminal element that is intent on perpetrating fraud. Friends and family members can pressure employees to alter or falsify records to help the individual avoid a DL suspension or payment of fees or fines. Internal fraud can be as seemingly harmless as a data entry clerk removing a conviction, changing a date of birth, or modifying other information on a record. An employee may pocket fees, falsify written test results, charge a lesser tax on a vehicle registration, or access information inappropriately.

Administrators cannot assume they have only honest and ethical staff. Although most employees are truthful and forthright, the organization more than likely employs individuals who will commit theft or fraud. Do not assume that because an individual is in a position of responsibility (e.g., auditor, manager, supervisor, team leader, investigator) that he or she is above reproach. Processes need to be put in place to check the checker as well as front-line staff. People often believe that they can get away with fraud because they are smarter than others. Those who commit fraud are likely to be those you least suspect. There are many instances in which DMVs were caught unaware by the fraud going on in their agency.

It is not unusual for those who perpetrate fraud within an DMV to teach other employees how to commit fraud. Let's look at a situation in Maryland as an example. A young man previously employed by the MVA completed a tour in the military and was accepted to the Baltimore Police Department Academy. He was forced to drop out because of a physical injury and returned to the MVA requesting employment. His previous work record showed him to be a reliable employee, and the MVA rehired

him as a front-line clerk in one of its field offices. This seemingly upstanding young man issued more than 200 genuine Maryland ID documents—both commercial and noncommercial DLs—based on counterfeit or nonexistent documents and did so for his own financial gain. He had been drawn into the fraud business by his supervisor. The majority of DL recipients were individuals involved in organized crime and narcotics trafficking. The genuinely issued documents were used to expand their criminal organizations and avoid detection by law enforcement. The U.S. DHS, with the assistance of the MVA Internal Investigations Unit, conducted a multijurisdictional investigation that led to the seizure of more than $1.2 million, along with the arrests and convictions of the MVA employees and leading members of the criminal syndicate. Some members of the conspiracy received 17-year federal prison sentences for their involvement in the scheme.

Chapter Three Fraud Deterrence

Fraud deterrence is the proactive implementation of policies, technologies, and processes to minimize the opportunity for individuals to perpetrate fraud. It is based on the premise that fraud is not a random occurrence; rather, it occurs where the conditions are right for fraud to occur. Fraud deterrence attacks the root causes and enablers of fraud. Analysis of processes, procedures, and systems can reveal potential fraud opportunities. Improving organizational procedures to reduce or eliminate causal factors of fraud is the single best defense against fraud. Fraud deterrence involves both short-term (procedural) and long-term (cultural) initiatives.

Fraud deterrence is not early fraud detection, which can often be a confusing point. In the DMV world, fraud detection can take place at any time during the transaction itself, as well as after the fact through a review of the transaction and supporting documentation. For example, in the case of facial recognition, a one-to-one match may identify fraud at the time of application, or it may be caught through a one-to-many match later in the process. Deterrence involves an analysis of the conditions and procedures that affect fraud enablers, in essence looking at what could happen in the future given the process definitions in place and the people responsible for the process. Fundamentally, deterrence is a preventive measure.

The first step toward eradicating fraud is to identify the greatest risk factors. Top offenders commonly include the failure to split key duties among several employees; inefficient physical and procedural safeguards over cash, other assets, and transactions; inadequate supervision of employees; and lack of mandatory vacations or job rotations for those with financial responsibilities.

There is no area within a DMV that is immune from the risk of fraud. The mail room, field offices, reinstatement processing, driver control, dealer processing, third-party transactions, even audits, are all vulnerable to fraud. As a protector of customer information, keeper of the public trust, and partner in highway safety, the DMV is responsible for ensuring the safety and security of data and the credentials it issues.

The demand for fraudulently obtained jurisdictional-issued credentials is immense, as is the desire for the information printed on the document. Defrauding the DMV is often a building block crime, one committed to facilitate greater crimes. Criminals and others who wish to commit fraud are willing to pay significant dollars for a fraudulently issued genuine DL, vehicle title, or other credential. They will go to great lengths, including bribing a DMV employee, to obtain a genuine document.

> *"The management of third parties is the biggest blind spot for companies today."*—Global Head of Internal Audit, US

It is imperative that agencies constantly look for new and better ways of doing business. The "we've always done it this way" attitude does not work in today's fraud-ridden society. New technologies and constantly evolving schemes—by both staff and criminals—make it imperative that operating under the status quo

is no longer accepted. Do not assume that because something has worked in the past that it will continue to be effective. After changes are made, be diligent by continuing to police processes and procedures. Make changes or enhancements as weaknesses are identified. New or changed laws, regulations, and procedures may change the opportunity or desire to commit fraud. New programs or requirements such as title branding, legal presence requirements, or stricter alcohol laws may result in new types of, or new opportunities to commit, fraud. Agencies must look for gaps that would allow employees to defraud the system. After gaps are identified, immediate steps must be taken to remedy problem areas. As processes are improved and oversight is strengthened, those who wish to defraud the system will also improve their methods, so constant vigilance is required.

Lawbreakers can be adept at fooling us, and the criminals who defraud the DMV are becoming increasingly more sophisticated in their means and methods. They may be successful if existing deterrents do not keep pace. The benefits of fraud are sufficiently lucrative that efforts to commit fraud will continue. Criminal networks are aware of which agencies use effective fraud prevention, detection, and investigative measures and those that do not. Those without an evolving and robust fraud strategy are prime targets for deception. Investigators and others responsible for overseeing processes and procedures and for ferreting out fraud must be part of every DMV.

The reality of fraud may be seen as a negative, but it also comes with opportunity. Opportunities to form effective partnerships, strengthen the organization, garner positive publicity, enhance business practices, reaffirm policies, improve morale, and publicize successes exist while improving an agency's ability to deter fraud.

Establishing or Maintaining the Right-Sized Fraud Unit is Key to Combating Fraud

To avoid becoming a target for fraud, it is imperative that DMVs develop fraud competencies sufficient to provide credible deterrents. In the ever evolving world in which we live, it is often a challenge, both in terms of resources and funding, for DMVs to stay in front of those intending to defraud the agency. Agencies must strive to meet such challenges to successfully foil fraud. By investing in a comprehensive fraud plan, the degree of fraud an agency experiences and the potential negative publicity that results from a casual approach can be averted. Having an active fraud unit sends a message that you are serious about combating fraud.

Since 9/11, administrators and other stakeholders have come to realize that in addition to highway safety responsibilities, DMVs are on the front lines of national security and identity protection. The need to address fraud and to enhance or create functional, stand-alone investigative units is greater than ever. With a sufficiently staffed and properly equipped fraud unit, the DMV will have watch guards keeping an eye on processes. The in-house unit can swiftly identify and address fraud problems and should have the authority to do so. The benefits of combating fraud far outweigh the cost. Only with the proper staffing, resources, and technologies in place can the DMV be successful in the ever increasing challenge of fighting fraud.

Justification for a Right-Sized Fraud Unit

A crucial requirement in the fight against fraud is an appropriately sized and adequately equipped fraud unit. Unfortunately, some agencies are forced to rely on outside law enforcement agencies to assist in the fight. In such situations, the DMV's fight is likely a secondary consideration by the outside enforcement agency because it is understandably focused on its own mission. The competition for resources often leaves the DMV with little to no assistance. An in-house

fraud unit provides the ability to proactively oversee the operation from a focused perspective because its primary mission is the detection and deterrence of fraud. A fraud unit can establish or enhance processes and procedures. It can take swift action when issues are identified. It can provide a unique perspective to legislative reviews and can pinpoint potential areas for fraud opportunities. Failure to focus on the deterrence and detection of fraud can undermine the credential issuance process, harm the reputation of the agency and its management, and even negatively impact the governor's office. It can make the jurisdiction a target for criminal activity and can threaten homeland security. A core competency of the DMV is the issuance of credentials. An equally important core competency should be fighting fraud.

The fraud unit should have oversight and authority to address both internal and external fraud. There is no magic formula to determine the appropriate size of the unit because it depends on the size of the organization, its responsibilities, the number and type of transactions processed, and the number of contractual third parties or partners the agency oversees. The group should be of sufficient size to effectively handle all of the responsibilities for which the unit is charged. Tracking performance and publicizing successes can help justify expansion of the unit when, and if, warranted. When analyzing the impact of new legislation or policies, consideration should always be given to the potential need for additional staff for the fraud unit.

Good, Better, Best

DMVs should strive to implement and maintain at least a "good" fraud program. The table below describes basic tenants that constitute, good, better, and best fraud programs.

Existing Fraud Unit Review

If a fraud unit already exists within a DMV, it is wise to regularly review staffing levels, tools, resources, and accesses to ensure the group is of sufficient size and that it is fully equipped and adequately trained to carry out its mission. A regular review will help ensure the DMV is keeping pace with fraudulent activities and trends. Agencies should include the fraud unit when planning for new legislation or programs to ensure fraud deterrents are in place.

Good	Better = Good +	Best = Good + Better +
Fraud policy, code conduct or ethics in place for all employees	Investigators with previous law enforcement experience	Full-time sworn investigators are dedicated to DMV fraud, and have subpoena and arrest authorities
Protocol for reporting internal or external fraud	Investigators who meet jurisdictional law enforcement accreditation standards	Investigators participate in task forces, fusion centers, and other groups
A fraud unit with investigators and appropriate support staff	Fraud staff involved in development or review of legislation and new processes	Forensic accountant(s) are part of fraud team
Fraud staff with a comprehensive knowledge and understanding of DMV procedures, laws, systems, and processes	Information is actively shared with task forces, fusion centers, and other appropriate groups	
Regular collaboration among fraud, audit, and other units	Investigative staff possess foreign language skills	
Chief of fraud unit reports directly to DMV agency head	Fraud team has access to case management and other pertinent tools	
Background checks are completed as part of the hiring process		
An internal fraud working group meets regularly		

Setting Up a Fraud Unit for the First Time and Managing Change

When establishing a fraud unit for the first time, the scope of responsibilities and authorities of the unit must be identified and planned for before implementation. The responsibilities of the unit should be in alignment with those of the agency. Once established, both the mission and staffing levels of the fraud unit should be regularly reviewed to determine if changes are needed.

Determine how the unit will fit in with existing processes. For example, there may be overlaps between responsibilities of internal auditors and members of the fraud unit. Tasks for each should be spelled out to keep overlap to a minimum while making sure all areas are covered. Determine whether activities currently performed by other parts of the agency should become the responsibility of the fraud unit and proactively manage the changes to ensure all parties buy into the new processes. Determine whether required authorizations exist or whether enabling legislation or regulation is needed.

One area to review is the facial recognition program. Are facial recognition system matches considered part of the issuance process and performed by the driver issuance unit, or should this be a responsibility of the fraud unit? Perhaps a combination of efforts by the two groups?

The culture of the organization will change with the establishment of a fraud unit, and such change must be proactively managed. Instituting change is often difficult when long-standing processes and procedures are affected. Affected personnel should be involved in discussions to ensure they are aware of and that they buy into new processes.

Responsibilities of the Fraud Unit

Management must determine what the unit will investigate. Facial recognition "hits," title and odometer fraud, dealer regulations, DL fraud, identity theft, and DMV tax fraud are just a few of the areas of potential responsibility of the unit. Determine whether they will conduct general investigations, vehicle inspections for assembled and homebuilt vehicles, or investigate mistakes on credentials. Determine whether the investigators are responsible for the investigation from its inception through to the arrest or if they will work with local enforcement.

The fraud unit should have the authority to conduct covert operations (such as observing third-party commercial driver license [CDL] testing or translated tests), as well as overt operations. Understanding what is said during the translated tests is important, so foreign language skills (or access to foreign language–speaking staff) are necessary. A fraud unit needs access to legal advice. It may not be necessary to have an attorney on staff within the unit, but there should be provisions for the unit to obtain legal advice as needed. The fraud unit should have a role in contributing to or reviewing procedures to better prevent or detect fraud. The unit should provide regular "lessons learned," which may prompt changes in policies, procedures, and training or input to legislative proposals.

The fraud unit can monitor DMV "tip lines" for leads and initiate investigations as appropriate. Investigators can attend intelligence briefings with other law enforcement agencies. They should be encouraged to actively discuss DMV cases and to network with other law enforcement agencies to combat fraud and other crime on a widespread basis. Sharing of resources among agencies is important in the fight against fraud. When other law enforcement agencies see the benefit of working with the DMV fraud unit, they can help promote the unit to the public and to the legislature and can provide valuable information to the unit.

Investigator Qualifications, Authorities, and Tools

Investigators should have law enforcement experience. Ideally, they will be sworn law enforcement officers with arrest authority. Former local, state, and federal criminal investigators bring with them a wealth of knowledge and experience in conducting complex criminal investigations. Such individuals can hit the ground running and minimize training costs for the agency. Individuals with foreign language skills can be beneficial in the investigative process.

To maximize success, it is important that fraud investigators have law enforcement authority enabling access to data, information, and intelligence available only to certified enforcement officers. Such information can prove critical in conducting investigations. It also allows investigators to obtain search warrants and provides greater credibility in dealings with law enforcement agencies, prosecutors, and third parties such as financial institutions. Developing the essential partnerships with federal, state, and local law enforcement agencies is more challenging if the fraud investigator(s) lacks law enforcement authority. Agencies whose investigators have law enforcement authority are eligible for grants, data access, and reimbursements from federal and state agencies.

Investigators with arrest authority are able to more efficiently conduct investigations because they do not have to coordinate with outside entities to make an arrest. Having the ability to make arrests assures cases will be handled in a timely manner because they are not dependent on someone else's workload or priorities. Successful convictions will increase as the DMV will not have to rely on outside entities to testify about DMV matters with which they are less familiar. The authority to arrest wrongdoers serves as a deterrent to others that wish to circumvent legitimate processes in place at DMVs.

The investigative process is considerably streamlined if the DMV investigator can issue subpoenas and eliminate the red tape that might otherwise be involved. For those who require legislative action to provide administrative subpoena or law enforcement authorities, Appendix A provides statutory language from Kansas, California, and New York.

Additionally, DMV investigators need the ability to use a full array of investigative techniques to ensure a successful outcome. These can include the authority to write and execute search warrants, conduct surveillance, place wiretaps on target telephones, interview witnesses, develop confidential informants, transport and interview arrestees, and present investigative findings to prosecutors and grand juries.

Having the right equipment to safely and effectively conduct everyday operations is critical. Proper attire, including clearly identifiable marking(s) as a law enforcement officer, is necessary when conducting search and arrest warrants. This alleviates confusion and reduces the chances of harm to both the investigator and the subject(s) of the investigation. Investigators should have the authority to carry a firearm during the course of duty. Such authority requires mandatory firearms training and regular qualifications with agency-approved firearms. Unmarked vehicles equipped with radios and other necessary gear is essential. Such vehicles allow investigators to conduct surveillance and other vital functions throughout the course of the investigation. Self-defense training and the ability to work in pairs when visiting suspects help ensure the safety of investigators when faced with a threatening situation.

In addition to traditional law enforcement equipment, essential tools of the trade include black lights, magnifiers, flashlights, binoculars, smartphones, audio and video recorders, onboard diagnostic (OBD) tools, bar code readers, still and video cameras, and ID checking guides. Access to DMV records, facial recognition or other biometric systems, social media, conventional websites, databases maintained by law enforcement agencies, public record aggregators, vital records offices, court records, skip tracing data, and tax records is necessary to do the job; to confirm credentials were issued to the right person; and ultimately, to solve cases.

Support Staff Experience and Authority

Although investigators are critically important to the fight against fraud, they cannot do the job alone. Adequate support staff is a fundamental need for any good investigative team. Analysts, auditors, fraud examiners, and forensic accountants play a key role in the deterrence and detection of fraud. These positions do not necessarily need to be part of the fraud unit, but they should certainly exist within the organization and should work collaboratively with the fraud unit. Just as investigators should have law enforcement experience, the individuals who fill support staff positions should have relevant experience along with the appropriate professional accreditation. Experience or training in using data mining and database software is essential for the support team. Employees of the unit should have access to ongoing professional training and professional accreditation opportunities.

It is extremely beneficial for support staff to have driver licensing or motor vehicle experience because their understanding of the processes will allow them to better identify and detect potential fraud. Investigative training should be afforded to support staff to help ensure success. Existing DMV staff who show an aptitude for critical thinking can be trained to investigate fraud schemes. Front-line DMV employees are often more aware of vulnerabilities within the agency than those in supervisory or management positions and may be good candidates for the fraud unit.

Support staff can be extremely valuable in the investigative process. They can obtain background information, which allows the investigator to focus on the investigation itself and on tracking leads. Forensic accountants, auditors, and analysts can investigative leads, obtain and analyze data, identify emerging trends, connect the dots, obtain DMV records from other jurisdictions, and run various behind-the-scenes database queries.

Support staff conducts the day-to-day research and completes analysis on potential fraud cases. They can help determine whether fraud occurred and whether a case should be investigated administratively or criminally. They provide a critical and unique viewpoint during the investigation. They analyze collected data to discern the scope of the fraud, identify potential conspirators and witnesses, determine associations, and spot trends and patterns. They can provide link charts, attend meetings with prosecutors, conduct evidence reviews, and handle other tasks essential to any investigation. Best-case practices suggest analysts be involved "early and often."

Support staff can develop reports that identify potential fraud such as pass/fail comparisons among third-party testers, multiple high-end vehicles with clear titles registered to one individual, multiple people residing at a single location, and so on. They can also perform risk assessments to analyze procedures and processes within the agency to identify weaknesses that might enable fraud to occur. Risk assessments can help identify methods the agency can use to detect and deter fraud that may be taking place. During risk assessments, system weaknesses where data elements necessary for fraud identification or investigation are not being tracked or collected may be identified.

Forensic accountants are skilled at conducting detailed financial audits and discovering trails when investigating fraud cases that extend beyond an individual (e.g., organized crime). They may develop a nexus to additional crimes being perpetrated by the same individuals. Forensic accountants are useful for tracking the money, which can often be the most complex part of any investigation. Fraud schemes can generate enormous profits for criminals. Seldom are illicit proceeds kept in obvious places such as a bank account under the criminal's own name. A forensic accountant has the skills to track funds throughout a complex maze of on-shore and off-shore accounts, as well as illegitimate or legitimate businesses set up to launder proceeds. A primary goal of any investigation should be to recover as much of the illicit proceeds as possible.

Auditors play an especially important role in an investigation because they are responsible for verifying the "checks and balances" within the DMV. Auditors

monitor and analyze transactions of DMV employees to identify potential fraud problems and emerging trends. Auditors also help examine records obtained by investigators to determine the scope and impact of the fraud. Often, they are the first ones to notice inconsistencies in transactions, accounting processes, and other areas.

Some staff need access to sensitive or restricted data to identify and flag possible fraudulent activity or anomalies an investigation has started. This proactive approach can help identify fraud without having to wait for tips to be received or informants to come forward. Staff will likely require access to multiple DMV systems; external databases; and other online tools, including social media. Captured data must include the elements that can identify fraud. Often, useful data are kept in databases or formats that are either difficult to access or are not captured or stored electronically. The information technology (IT) unit must cooperate with the fraud unit and help staff learn how to best access the data.

The combination of experienced law enforcement personnel, support staff, and DMV employees will greatly enhance the overall investigative efforts of the agency.

The Right Tools Are Crucial

Equipping the team with the tools necessary to conduct an effective investigation is just as important as having the proper skill sets on the team. DMVs maintain a tremendous amount of information about identities, vehicles, and addresses through their normal operations. Tools that can extract data from DMV are essential for the detection, investigation, and prevention of fraud. Automated software can randomly pull a certain percentage of all transactions and a higher percentage of "at-risk" transactions (overrides, gratis, and so on) and can be used to monitor staff activity and identify potential abnormalities. The creation of a separate reporting system made available only to investigators is vital to maintain the integrity of ongoing investigations. Such a system can maintain written reports, investigative findings, and other information deemed necessary.

Data search products can be useful in locating a person's past or present residences, phone numbers, relatives, and so on. Data searches can identify information such as full names and aliases, address history, phone numbers, employment history, business associates, professional license information, death records, financial history, credit history, and other information helpful in an investigation. Such data are updated on a near continuous basis from numerous public and proprietary databases such as the Social Security Administration (SSA) or state vital record death files, tax rolls, state business regulation agencies, Secretary of State offices, phone records, credit bureaus, and so on.

Effectively managing a caseload is difficult without a case management system. Investigators are required to work cases simultaneously because case information requested from other sources takes time to receive. As investigators are waiting for information, they need to maintain up-to-date notes on every case so they can pick up where they left off when the information is received. Case reports and exhibits are important to maintain for future retrieval when administrative hearings and court dates are scheduled.

The ability to retrieve facts about cases, both open and closed, is a vital piece of the fraud management program. Calls from complainants, legislators, media, law enforcement, other DMV staff, and victims require an efficient way to retrieve information. A case management system can provide such capabilities. The case management system should also incorporate a function to provide data from each case that can be used to identify fraud trends and to evaluate both the program and individual investigators' successes or areas needing improvement.

Regular communication and coordination should be established among the business units responsible for regulating entities such as driving schools, dealerships, and so on and the fraud unit so that when anomalies

or suspicious activities are identified, an investigation is initiated and appropriate action is taken on an ongoing basis.

Non-investigatory Benefits of a Fraud Unit

In addition to handling investigations and addressing fraud challenges, investigators can provide valuable assistance in many other areas. They can provide analysis for proposed legislation and offer input for fiscal notes. They can provide input to improve policies, processes, and training and identify areas of vulnerability. They can assist with internal audits, provide undercover testing (both internally and with third parties), and assist with development and analysis of requests for proposals. They can provide input and feedback on equipment purchases.

Investigators can assist and provide valuable insight into the overall design and security features of DLs/IDs during the Request for Proposal/Information (RFP/RFI) process. The experience of fraud investigators can be a significant benefit when deciding what is necessary for the security of an identity document. The insight gained from investigations and identifying vulnerabilities in the current system can ensure that vendor proposals adequately address areas of concern and that potential problems are minimized moving forward. Obtaining the input of the fraud unit, initially and throughout the process, can prevent unnecessary expense while providing a measure of security to make documents harder to counterfeit and to illegally obtain.

Investigators can share their findings to improve DMV functionality. They can work with human resources in developing employee hiring standards and work with the IT division to modernize existing databases. Many DMVs are working with aging computer systems that were designed without consideration of the information that may be needed to track, identify, and investigate fraud. As these systems are replaced, the unit can provide input into what elements should be recorded and tracked. They can work with auditors to show potential vulnerabilities both inside and outside the organization. Investigators can conduct background checks and help develop ethics training. They can speak to and train staff on DMV fraud. Investigators can teach fraud detection to other law enforcement agencies. They can work with prosecuting attorneys and can provide expert testimony on DMV records and processes. With identity theft being a significant problem today, the fraud unit can serve as a resource for outside law enforcement agencies and prosecutors to obtain records, root out fraudulent records, and stop titles and licenses from being issued to known criminals.

For all of the reasons stated here and many more, a fraud unit can greatly benefit the agency, the jurisdiction, and the country. Administrators are encouraged to engage the unit in other areas of the agency as a proactive approach to combat fraud and to make the agency more secure and steadfast overall.

Alternatives if Establishing a Fraud Unit Is Not Possible

If it is not possible to obtain funding or authorization to establish an "in-house" fraud unit, that should not prevent the agency from being proactive in the fight against fraud. DMV administrators should regularly meet with the director of the jurisdiction's public safety or state police agency and discuss how the agencies can partner in the deterrence and detection of fraud. Sharing information among agencies can provide insight into how DMV fraud can lead to other crimes such as vehicle theft or cloning, identity theft, financial crimes, sex offenders hiding under false identities, sex trafficking, minors obtaining alcohol, insurance fraud, odometer fraud, drug offenses, and many more.

Get your attorneys involved in prosecuting those who commit fraud against the DMV, whether action taken is administrative or criminal. Meet with prosecutors and judges and explain fraud issues, the repercussions of fraud, and activities taking place to counteract fraud.

Fraud Deterrence Best Practices

Fraud can be costly, and it can be found in any organization. With no end in sight for the losses that organizations suffer, the question turns to what administrators can do to combat losses. Many organizations focus on improving their internal controls and ignore the fact that there is more to fraud deterrence and detection than a strong set of internal controls. Codes of ethics, hotlines, job rotation, audits, and internal work groups are cost effective ways that are often overlooked when considering how to detect and deter fraud.

Following are some things an organization can do to detect and deter internal fraud.

Implement a Zero Tolerance Policy

Let your employees know right up front that the department has zero tolerance for fraud. Reiterate that policy on a regular basis. Post notices regarding your program and let employees know what action they can take if fraud is suspected.

Develop a Code of Ethics

Fraud deterrence can be built directly into an organization's code of ethics or code of conduct. Many codes already cover instances of fraud. Statements covering conflicts of interest, compliance with applicable laws and regulations, compliance with company policies, and reporting of individuals in violation of the code of ethics all relate to fraud deterrence. Codes of ethics should be clearly communicated to every employee. Each employee should be given a copy of the code of ethics and should sign a statement to acknowledge that he or she has received and understands the code. Management needs to remain active in administering the code of ethics through employee training and posting visible copies of the code where employees can read them. An annual review and signing of the code of ethics during the employee's performance review is a best practice. The administrator may wish to speak to new employees during their orientation and stress how important the code is to the agency. And just as important, management needs

Let your employees know that fraud will not be tolerated. Providing a confidential way to report fraud will increase and improve reporting.

to enforce the code by taking corrective action when violations of the code are discovered. Appendix B provides examples of codes of ethics.

By establishing codes of conduct and ethics, along with the policies and procedures to help enforce them, you set clear expectations for your staff and can prevent unacceptable behavior from occurring.

Fraud Working Group Provides Essential Support

Establishment of a fraud working group is a must for any organization dedicated to combating fraud. The group should consist of subject matter experts who hold positions that allow them to observe and report on potential areas of fraud. At a minimum, representatives from audits, investigations, operations, driver services, vehicle services, IT, and accounting

should be included. Consider including representatives from other entities, such as state police or third-party partners, as ad hoc members.

The working group should meet regularly and be challenged to modify or develop policies, procedures, and technology recommendations using a multidisciplinary approach. The group should report directly to the administrator, who should place a high level of focus on the information and recommendations proposed by the group. Swift action should be taken to address vulnerable areas.

Behaviorally Oriented Solutions for Fraud Risk Factors

- Behavioral approaches and solutions to the fraud risk factors include:
- Sound tone at the top, with management "walking the talk."
- Align incentive structures within the organization in a way that does not encourage fraud perpetration.
- Task an active audit board or committee with overseeing management performance and activities (as well as the work by external and internal auditors).
- Nurture a culture of integrity and ethics, supported by an organizational code of conduct.
- Conduct periodic ethics audits and enforcement of noted violations of the code.
- Maintain an ethics or whistleblower hotline.
- Explicitly reward good behavior.
- Conduct routine background checks for new and experienced hires, as well as for senior leadership appointments (human resources needs to lead this effort).
- Take swift, decisive action in response to incidents of fraud so employees and others are aware of the organization's serious commitment to dealing with fraud issues head on.
- Require fraud awareness training, perhaps delivered by internal audit professionals or outside consultants, and include information on the ethics hotlines and guidance on what to do when fraud is encountered.
- Conduct self-assessments that consist of process owners performing risk and control mapping (and include fraud risk considerations in such exercises).

Conduct Background Checks

Conducting background checks on all DMV employees is a best practice. Background checks may include financial, state and federal criminal history, and driver record checks and should be based on the individual's role and accesses in the organization. Criminal history checks can be run with fingerprints or name only, and both should be completed. Credit histories can identify financial problems, such as delinquent bill payments and gambling habits. Annual background and financial checks are a good idea, especially for those in key positions. Background checks should be a condition of employment.

Implement Clear Internal Policies and Procedures

Ethics policies should clearly detail what the agency considers to be illegal, improper, and fraudulent behavior. On an annual basis, employees should receive and sign statements that delineate what they can and cannot do. The best policies and procedures will not work, however, if management does not support them, if employees do not know about them, or if they have no teeth. Educate existing and new employees, including executives, about the use of such policies and the penalties for defying them and update training annually.

Information Technology Security Awareness

Good IT security practices are necessary to protect the confidentiality, integrity, and availability of personal information. IT security awareness should be reinforced through regular security awareness training and communication. IT security awareness training not only provides employees with new information relative to laws and internal policies and procedures regarding access to systems and dissemination of information but also serves as a reminder of the importance of adhering to mandates and penalties for failure to do so. Failure to complete training within a specific time frame should result in termination of system access until completed.

Establish Hotlines

Because whistleblowers expose a large percentage of frauds, 24-hour tip lines encourage the reporting of potential offenses. Publicize the confidentiality and anonymity of fraud-prevention hotlines. Studies show that witnesses to fraud prefer to remain anonymous when reporting wrongdoing. Keeping employees and the public abreast of such reporting mechanisms demonstrates the agencies intolerance for fraud. Hotlines allow employees, customers, vendors, and others with whom the agency deals to report suspicious activity in an anonymous and secure reporting environment. This helps to ensure that suspicious activity witnessed by anyone inside or outside the agency is reported. Hotlines can range from a voice mail box in an organization's phone system accessed by management to a fully outsourced, fully staffed, 24-hour service.

"Advertise" Your Attention to Fraud

Placing posters and other announcements about the agency's focus on fraud will help serve as a deterrent to both employees and customers. DHS has made posters available to DMVs, and many have found them to be an effective deterrent. In addition, frequent messages about fraud in employee newsletters and other regular communications remind the staff that fraud is a critical priority to the agency and will not be tolerated.

Placing posters such as this one provided by DHS can help deter DMV fraud.

Blow the Whistle

It is impossible to completely eradicate fraud in your agency. You can, however, minimize its damage and take appropriate actions to prevent it. Whether you choose to publicize fraud in your organization or not, make it clear that you will find and fire fraudsters and prosecute them to fullest extent of the law.

Separate Duties

It is critical to separate financial tasks among several employees. The person who signs checks, for example, should not make bank deposits. Unfortunately, budgetary cutbacks and downsizing sometimes result in the same person handling multiple procedures such as taking payments and documenting transactions. This should be avoided whenever possible.

Implement Job Rotation

According to a report by the ACFE, job rotation and mandatory vacations resulted in the second highest reduction (61%) in losses from fraudulent activity. Many types of occupational fraud require the perpetrator to actively conceal his or her scheme through false records. By requiring job rotation and mandatory vacations for employees responsible for handling the organizations funds, other individuals perform those job responsibilities. If fraud is occurring, job rotation and mandatory vacation may provide an opportunity for these actions to come to the attention of management and others. It is easier to successfully commit fraud or theft when the person is in the same job, at the same place, every day. In addition to countering fraud, job rotation could result in improved customer service, increased efficiency, and higher employee satisfaction.

Conduct Audits

The Institute of Internal Auditors defines internal auditing as an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Internal auditors play an important role in evaluating the effectiveness of control. As an independent function reporting to top management, internal audit is able to assess the internal control systems implemented by the organization and contribute to

ongoing effectiveness. As such, internal audit often plays a significant monitoring role. To preserve its independence of judgment, internal audit should not take any direct responsibility in designing, establishing, or maintaining the controls it is charged with evaluating. Audit staff should only advise on potential improvements to be made.

All sensitive transactions should be audited on a random basis. Audit processes must be evaluated—or in some cases, developed and implemented—and constantly reviewed and updated. Do not forget to audit the auditors, supervisors, managers, and others in positions of authority. When deficiencies are identified, take immediate and applicable action, which may include retraining, progressive discipline, or legal action.

Electronic audits can automatically identify potential fraud. Access to work or sensitive areas during off hours and unusual (unauthorized or high-volume) transactions can easily be identified via automatic electronic review.

Third parties conducting critical DMV services such as CDL third-party testers, county or municipal agents, AAA offices, driver training schools, and others who conduct transactions on behalf of the DMV must be monitored regularly. Onsite auditing provides a "hands-on" review of the program and may identify areas of weakness or concern. In combination with headquarters' monitoring, onsite monitoring allows the agency to determine if the third party is in full compliance with DMV rules and regulations. Swift and appropriate action should be taken to address any findings. Review processes to determine if changes need to be made to strengthen the program. Covert observation of activities (especially testing) can provide information on compliance with DMV requirements that is not available any other way.

The California DMV created an "Eagle Eye Award" to provide recognition by the Investigations Division to Field Office Division employees for direct referrals that result in Investigative intervention. The awards recognize and highlight exceptional observations made by Field Office personnel that rises above and beyond their daily course of duty and responsibilities. Objectives of the program include creating a collaborative effort between the two divisions, generating more referrals for investigative intervention, fostering new behaviors of Field Office personnel as they begin to see acute and keen observations as part of their responsibility, increasing motivation of Field Office personnel to become more observant of documents submitted to the department, providing a forum for a greater sense of involvement, ownership, and accountability by encouraging staff to show initiative and individual growth.

Recognize Employees Who Contribute to the Fight

Provide recognition to employees who make contributions toward the deterrence and detection of fraud, including transaction or case referrals or identifying a previously unknown weakness that could be exploited to commit fraud. Such programs can encourage others to be on the look out for instances of fraud or for weaknesses in the process and increase the likelihood of identifying fraud.

Chapter Four Partnerships

Forming partnerships with other state and local entities can provide additional resources in the fight against fraud. Partners can bring resources, expertise, and database access that the DMV likely does not possess. Partners can also provide information on related cases or trends that would otherwise be missed. Forming partnerships is a win-win for all involved. It should be noted that in some cases, it may be necessary to first educate potential partners on the impact that fraud can have to the agency, society in general, affected individuals, and homeland security.

Partnerships with Federal, State, Provincial, and Local Law Enforcement

Fraud is a challenge the DMV cannot solve alone. Partnerships are critical in confronting the problem. State, local, and provincial law enforcement, prosecutors, other state agencies, and federal agencies all play a key role in combating fraud perpetrated against the DMV. To form partnerships, key players from the various agencies should sit down, talk about the problem, and identify solutions. All should agree to open and honest dialog. Once established, discussions between the DMV and its partners should take place on a regular basis.

Although they are important for every agency, partnerships can be especially crucial for DMVs without investigators and for those that have investigators without peace officer authority. Non–law enforcement personnel are unable to access law enforcement–sensitive information, make arrests, and obtain search warrants. Most investigators who lack law enforcement authority do not have the authority to issue subpoenas. DMVs without law enforcement officers find it difficult to file criminal charges without the help of outside law enforcement agencies.

It should be noted that partnerships with law enforcement can be a two-way street. Depending on a jurisdiction's laws and regulations, law enforcement officials may be able to access DMV records, including facial recognition systems, in their investigations. Outside enforcement entities should be required to follow any departmental policies in accessing or using DMV records, including adherence to confidentiality requirements. You may wish to consider establishing a Memorandum of Understanding (MOU) for this purpose.

Examples of successful partnerships between the DMV and other agencies can be found throughout the country. A few illustrations follow and help solidify the reality that partnerships are the key to success

California's "Trap Door Operation" and "Avoid 14"

In an effort to curb underage drinking and deter the use of counterfeit driver licenses and ID cards, the California DMV Investigations Division participates in "Trap Door Operations" with the Los Angeles Police Department (LAPD) and the University of Southern California (USC) Department of Public Safety at local CVS stores. The goals of the operation are to detect, deter, educate, and bring into compliance individuals who are in violation of the law. Additionally, attempts are made to gain valuable intelligence on counterfeiting "mills" operating in the Los Angeles area.

In the "Avoid 14" effort, a Law Enforcement Task Force on Underage Drinking was established by

the San Diego County Police Chief's and Sheriff's Associations to proactively address the public health epidemic of underage drinking. The mission of the Task Force is to provide a forum to bring law enforcement within San Diego County together to ensure active, region-wide cooperation and consistency of enforcement of alcoholic beverage statutes and to establish community partnerships. California DMV Investigators have been vital and valued participants in this Task Force since 2002. Since 2006, DMV Investigators and the 20 or more law enforcement agencies involved have conducted more than 75 operations and made more than 2,200 arrests.

Delaware Department of Motor Vehicles and Local Law Enforcement Agencies

The DMV Fraud/Investigations Unit holds bimonthly meetings with members of the Delaware law enforcement community and other state agencies to discuss numerous issues, including fraud. The meetings provide a forum in which agencies can network and share information and resources. The goal of these bimonthly meetings is to establish a greater working relationship between DMV and other agencies and to foster higher cooperation among agencies.

Oregon Driver and Vehicle Services and Local Law Enforcement Agencies

Oregon holds quarterly meetings with law enforcement partners. Meetings are organized by the DMV administrator, and in addition to key individuals from the DMV, representatives from the Oregon Association of Chiefs of Police, the Oregon State Sheriff's Association, the Oregon District Attorney Association, and representatives from local law enforcement agencies are in attendance. The meetings provide a forum for sharing information, including potential legislation, new DMV initiatives, changes to policies and procedures, and information received for driver or vehicle withdrawal actions.

Maryland Partnerships in Fusion Centers and Auto Theft

The MVA teams with two regional auto theft task forces serving the Baltimore Washington Metropolitan Area (RATT and WAVE). These organizations provide intelligence and law enforcement support during undercover purchases from unlicensed car dealers. As part of the partnership with the auto theft task forces, the MVA has a full-time investigator performing post-transaction inspections of foreign titles submitted to the MVA for authenticity and alterations. The investigator started work in October 2012 and during the first year referred more than 40 suspected title fraud cases to the either a regional task force or to a law enforcement agency.
The MVA Investigations and Internal Affairs Division is a member of the Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN). MAGLOCLEN is one of six Regional Information Sharing System (RISS) Centers across the country. This organization provides valuable intelligence information regarding local crime trends related to counterfeit and fraudulent IDs. MAGLOCLEN also provides training to MVA investigators, at little or no cost to the MVA.

Nebraska Facial Recognition Data Sharing Partnership

The Nebraska DMV established a facial recognition data sharing partnership in July 2012. The first step of the initiative was to add current and historical jail photos from every enforcement agency in the state to the DMV's facial recognition database. A daily feed of new jail photos was then instituted.

A "one-to-many" match process occurs each evening, resulting in a list of suspected fraud cases. DMV investigators review the hits and determine which are potentially fraudulent. If the DL photo is believed to be false, the DMV investigators pursue the investigation. If the DL photo is believed to be the true identity, the arresting agency is advised of the

potentially false name. It is expected that results of a facial recognition match will never be used as sole evidence for arrest or charges.

Electronic access to the facial recognition database is provided to the Nebraska State Patrol and police departments in Lincoln and Omaha for investigative purposes only. Providing access to the facial recognition database to law enforcement partners was another step the DMV implemented in the fight against fraud.

New York Underage Drinking Enforcement Partnership

The New York State DMV Field Investigation unit uses a grant from the NYS Governors Traffic Safety Committee (approximately $140,000) to assign investigators to participate in underage drinking enforcement across the state. Sites identified as "last drink" locations for individuals arrested for DWI under 21 years are targets of the campaign. In one year, investigators recovered more than 1,500 counterfeit or altered driver licenses. In the first seven years, the New York DMV collected more than 15,000 fraudulent driver licenses from underage drinkers. In addition to the traffic safety impacts, the DMV was able to identify security features that were easy to duplicate, as well as features that were difficult to reproduce. The intelligence gathered allowed the DMV to modify security features during their next DL contract renewal.

Oklahoma Partnership on Identity Theft and Fraud

The Oklahoma Driver License Services (DLS) and the Oklahoma Highway Patrol (OHP) Identity Verification Unit (IVU), divisions of the Oklahoma Department of Public Safety, work in conjunction to combat identity theft and fraud. The IVU is composed of civilian employees and is used as a clearinghouse between the DLS and OHP Investigations, which investigates complaints of DL/ID theft and fraud and all other law enforcement agencies with concerns of DL/ID theft.

Washington Partnership on Facial Recognition

The Washington Department of Licensing (DOL) and the Washington State Patrol (WSP) partnership on facial recognition began after a meeting between the two agency heads in which facial recognition processes were discussed. The DOL, having no sworn enforcement investigators, had been sending certified mail to individuals found to have multiple identities advising that their licenses had been cancelled. Information on the cases was also forwarded to the State Fusion Center. The DOL had never received feedback from the fusion center on any action it may have taken as a result of the information received from DOL. The WSP chief quickly realized that without conducting criminal investigations and pursuing prosecution as appropriate, offending individuals would be free to continue their fraudulent practices in other jurisdictions. The chief immediately offered WSP investigative assistance. However, recognizing the WSP lacked the investigative resources to take on every instance of potential fraud identified, an agreement was reached whereby the DOL began triaging and sending the "worst of the worst" to WSP for investigation. Multiple investigations, arrests, and prosecutions have subsequently taken place.

The director and chief also recognized an opportunity not only to reduce fraud and improve homeland security but also to eventually grow the investigative capacity of both agencies. By collecting data and educating the state legislature as to the scope of the problem and how much of the problem is not even being investigated because of resource limitations, it is envisioned that additional resources can eventually be legislatively allocated to address this issue in the longer term.

Making a Case for Federal Partnerships

There are many advantages to partnering with federal law enforcement agencies in the fight against fraud. Grants, sharing of seizure proceeds, reimbursement of equipment, and overtime are a few of the advantages such a partnership provides. The ability to file federal charges is another significant advantage. Federal penalties tend to be tougher than state or local penalties, and federal sentences carry no chance of parole.

Federal law enforcement agencies routinely conduct document and identity fraud investigations. Federal agents bring specialized expertise and can provide resources such as manpower and equipment to DMV investigations, which generally ensures a successful outcome. The combination of DMV investigator knowledge and federal agencies resources results in high conviction rates for those involved in DMV fraud.

Intelligence sharing is another reason to establish federal partnerships. Federal agents frequently receive tips through confidential informants, federal prosecutors, and other law enforcement agencies regarding fraud schemes at DMVs to which DMVs might not otherwise be privy. Federal agencies are often willing to work with DMV investigators to uncover and explore fraud schemes. By working with federal agencies, DMV investigators develop strong partnerships to ensure that investigations are comprehensive and more efficient.

Federal agencies have task forces dedicated to the investigation of identity and benefit fraud. The task forces act as force multipliers and bring resources together more cohesively throughout the investigation. In recent years, a concerted effort has been made to include DMV investigators on such task forces. The benefits of participation on federal task forces for the DMV include asset sharing, overtime pay for investigators, vehicle fleet usage, intelligence sharing, use of office space, and the ability to network with numerous agencies on a daily basis.

Asset sharing can be a significant inducement for working with federal agencies. A majority of federal investigations, including those related to DMV fraud, often results in significant asset seizures. Federal agencies are allowed to keep only a small portion of recovered assets and proceeds, and the remainder is shared with agencies that significantly contributed to the overall investigation.

Advantages of partnering with federal agencies

- Access to grants
- Equipment and overtime reimbursement
- Proceed sharing from seizures
- Ability to file federal charges
- Vehicle fleet usage
- Intelligence sharing
- Use of office space
- Ability to network with numerous agencies on a daily basis

Following are descriptions of some of the federal agencies that can assist the DMV in their fight against fraud.

Department of Homeland Security

The DHS' HSI has taken a lead role in investigating internal (employee) and external (counterfeit documents) fraud schemes that affect the integrity of DMV processes. Efforts include identifying the fraud facilitators (DMV employees, document producers, and operators of illegal websites), conducting extensive criminal investigations, tracing and seizing of illegal funds derived through fraud schemes, and arresting perpetrators of such crimes. Many of these investigations are accomplished through the use of the HSI-led Document and Benefit Fraud Task Forces (DBFTF), whose focus is on the investigation of document and benefit fraud schemes. HSI investigates document fraud schemes in all 50 states through 21 DBFTF's offices located throughout the United States.

U.S. Marshal's Fugitive Task Force

The U.S. Marshals have established task forces across the country that work closely with local, state, and federal law enforcement agencies in apprehending fugitives. Several DMV investigative units have developed relationships with these tasks forces and have obtained grants for overtime or equipment. The Marshals have also assisted in dealing with some of the multiple identity cases generated by facial recognition, especially when one of the subjects has an outstanding warrant.

Federal Bureau of Investigation's Facial Identification Scientific Work Group

The Federal Bureau of Investigation (FBI) has established a scientific work group that is developing "best practices" for using facial recognition in different venues, including MVAs. Access to the website http://www.FISWG.org is free for government agencies and provides access to white papers, supporting documentation and information. The FBI's Biometric Center is an active participant with the group and can also provide expert testimony when needed for facial recognition or identity theft cases.

U.S. Secret Service Electronic Crimes Task Force

The U.S. Secret Service (USSS) has established task forces across the country to assist with identity theft cases, counterfeit IDs, and credit card fraud. Several DMV investigation units across the county work with USSS task forces and receive grants for equipment or overtime.

Department of Justice and Treasury Equitable Sharing Grants

The U.S. Department of Justice (DOJ) and U.S. Treasury Department offer equitable sharing programs for law enforcement who assist in federal investigations and prosecutions. Numerous DMV investigation units with sworn officers have obtained funds as a result of participation in criminal cases. Grants or claims obtained in this manner can be used for law enforcement purposes only and have been used across the country for updates to offices, equipment, and computer upgrades for investigative staff. This has allowed agencies to divert funds to other areas of the agency.

Agencies that do not have investigators with law enforcement authority but that assist in investigations may receive restitution or reimbursement from any pleas or settlements that are reached.

Homeland Security Investigations Forensic Laboratory

Since its creation as the Forensic Document Laboratory in 1978, the DHS HSI Forensic Laboratory (HSI-FL) is the only U.S. crime laboratory specializing in the scientific authentication and research of travel and identity documents and related issues. The HSI-FL provides a broad range of document and latent print-related forensic, intelligence, and investigative support services for HSI, ICE, DHS, and other U.S. and foreign law enforcement agencies. The lab is a resource for forensic, research, training, and law enforcement issues related to travel and identity documents.

The HSI-FL Reference Library contains an extensive collection of more than 280,000 documents, including exemplars of genuine, altered, and counterfeit travel and identity documents from more than 200 countries. The library also contains identification and civil documents from all U.S. states and territories. These documents are used in comparative examinations of suspect documents submitted by ICE and other federal, state, and local law enforcement officers.

U.S. Secret Service Forensic Lab

The USSS is home to an advanced forensic laboratory, which includes the world's largest ink library. USSS forensic analysts examine evidence, develop investigative leads, and provide expert courtroom testimony.

Forensic examiners analyze questioned documents, fingerprints, false identification documents, credit cards, and other related areas of forensic science. Examiners are responsible for coordinating photographic and graphic production, as well as video, audio, and image enhancement services. Much of the technology and techniques used by examiners is exclusive to the USSS.

The forensic services used by the USSS include a number of specialties, including:

- **Identification:** The USSS has access to a full range of fingerprint-related services using the most up-to-date chemical and physical methods, including the utilization of state-of-the-art equipment for the development of latent prints. Specialists provide technical expertise and training in all fingerprint-related matters to the USSS field offices and other law enforcement agencies. They also provide expert testimony in federal, state, and local courts.
- **Forensic automation:** Forensic automation analysts provide advanced automated or computer support to all USSS protective and investigative elements, as well as for outside requests that have originated within USSS field offices. This responsibility is computer intensive and uses internal and external networks to identify fingerprints, handwriting, counterfeit identity documents, and financial documents when other investigative leads have been exhausted.
- **Questioned documents:** The primary goal of analysts is to support field investigations by providing expert forensic analyses of evidence developed during investigations, writing reports of the scientific findings, and providing subsequent expert testimony in court proceedings. Examiners also provide training to investigators on subjects related to forensic analysis and participate in crime scene search teams.

Federal Bureau of Investigation Lab

The FBI Laboratory has specialized units that respond to incidents and collect or facilitate the collection of evidence in the field. The Evidence Response Team Unit supports Evidence Response Teams in all 56 FBI field offices. The Photographic Operations and Imaging Services Unit and the Special Projects Unit provide expertise on forensic facial imaging.

The Forensic Analysis Branch (FAB) is the destination for most items of evidence submitted to the laboratory for analysis. This unit analyzes evidence and will assist with forensic document examination, threatening letters, suspicious packages, and other threats to government agencies.

Examples of Federal Partnership Successes

Partnerships between the DMV and federal agencies are mutually beneficial. Some examples of successful partnerships follow.

Kansas

A group of foreign nationals from Central Asia committed DL fraud when they stepped in line at the DMV to have their photo placed on another person's license after the other person (co-conspirator) was processed at the counter. With their fraudulently obtained DLs, the criminals registered businesses, opened bank accounts, and operated a human trafficking ring in 14 states, all under identities belonging to people who had departed the United States. The group recruited foreign nationals from Central Asia, Eastern Europe, the Philippines, Jamaica, and the Dominican Republic. The crime group also brought foreign nationals, originally from Central Asia and living across the United States, who had overstayed their visas, to Kansas to fraudulently obtain DLs. As the DL fraud investigation evolved into a larger organized crime investigation, the Kansas Department of Revenue's Office of Special

Investigations partnered with DHS Investigations, the U.S. Department of Labor Office of Inspector General's Office, the FBI, and IRS Criminal Investigations. The investigation led to the conviction of 11 individuals, including six from Uzbekistan, two from Moldova, and three Americans. It marked the first time that human trafficking charges were part of a larger RICO (Racketeer Influenced Corrupt Organizations) indictment in the United States. The case exemplifies how DL fraud is often a building block crime that allows criminals to commit a series of other crimes.

New York

The New York State DMV partners with a variety of federal agencies, including the U.S. Marshal's office, DHS Security, HSI, and the USSS. The NYS DMV's participation with federal agencies has allowed it to claim reimbursement for overtime and equipment. These partnerships allow DMV investigative staff to get involved with federal cases, and they allow the DMV to obtain assistance from federal agencies in DMV fraud cases, identity theft complaints, and facial recognition cases. In one recent year, more than 750 arrests made by NYS DMV investigators were made in conjunction with federal law enforcement officers.

Tennessee

A joint investigation by the ICE HSI Resident Agent in Charge office in Chattanooga, Tennessee and the Tennessee Highway Patrol Criminal Investigations Division (THP CID) exposed a sophisticated identity theft and fraudulent document manufacturing organization based in Tennessee. An investigation identified three corrupt Tennessee DMV DL examiners who were unlawfully issuing Tennessee DLs/IDs in exchange for cash or services. Over the course of the investigation, agents determined that several fraudulent document vendors were using a "middle man" to broker the sale of genuine Tennessee DLs through corrupt DMV employees. Fraudulent document vendors and customers from Alabama, Georgia, Tennessee, Florida, and New York used corrupt DMV employees to unlawfully obtain DLs/IDs. The investigation resulted in the seizure of 45 identity documents and 17 criminal arrests. All of the DMV examiners, as well as several document vendors, were arrested, and the DMV examiners were terminated.

Prosecutor and State's Attorney Partnerships

Prosecuting entities should be included in the agency's efforts to fight fraud. Prosecutors are responsible for taking the case before the court, and getting them involved early in the process will strengthen the likelihood of a successful outcome. Following are examples of successful partnerships between DMVs and prosecutors or state attorneys.

Iowa

To enhance enforcement efforts in combating motor vehicle dealer consumer fraud in Iowa, the Iowa DOT Bureau of Investigation & Identity Protection formed a partnership with the Iowa Attorney General's Office of Consumer Protection. Investigators were trained on motor vehicle consumer credit code regulations by the Attorney General's Office legal and investigative staff. Training included hands-on exercises reviewing dealer records to better equip investigators on detecting irregularities in consumer credit transactions while conducting dealer audits. Over the course of one year, the Iowa Attorney General's Office collected $313,332 from eight Iowa dealers and returned the money to 538 victimized consumers.

Kansas

A Houston school teacher was victimized by an imposter in Kansas, who used the victim's name and ruined the victim's credit history. The victim contacted the Kansas U.S. Attorney's Office for assistance. The U.S. Attorney's Office reached out to the Kansas Department of Revenue's Office of

Special Investigations (OSI). OSI's investigation revealed that the perpetrator used a fraudulently obtained Kansas DL in the victim's name as part of a scheme that involved complete identity theft. The perpetrator opened bank accounts, secured credit, registered vehicles, filed taxes, and secured a mortgage on a house. When confronted with the problem by employers, financial institutions, and government agencies, the perpetrator continually insisted she was the true victim. She even went so far as to put the victim's name on her newborn's birth certificate. The hospital bill went unpaid. OSI arrested the perpetrator, and part of her guilty plea called for her to be deported to Mexico after completion of her sentence.

Partnerships with Fusion Centers

Fusion centers were created after the events of 9/11 to share information among local, state, and federal law enforcement entities to protect homeland security. Fusion centers provide statewide threat coordination and strategic overview while working in collaboration with partners at the federal, state, local, private, and tribal levels to protect the citizenry and critical infrastructure of the state and to provide strategic threat analysis. They also provide valuable intelligence information regarding local crime trends.

Fusion centers are composed of law enforcement personnel and analysts from a variety of local, state, and federal agencies. Their purpose is to share intelligence, correlate information, and identify threats. They partner with state intelligence departments to provide assistance to the DMV and vice versa. Fusion centers and intelligence departments can help "connect the dots" in looking for connections between the DMV fraud case and other cases. Following are examples of successful DMV and fusion center partnerships.

California

The California DMV provides a full-time Investigations Division employee for analytical participation in the California State Threat Assessment Center to establish the cooperative effort and partnership among the California Highway Patrol, California Emergency Management Agency, and California Department of Justice to the state designated fusion center. California DMV Investigations Division, and all its Peace Officers are members of the Western States Information Network (WSIN). The WISN is one of the six RISS Centers across the country.

Iowa

The Iowa Bureau of Investigation & Identity Protection staff have long been members of the Iowa Law Enforcement Intelligence Network (LEIN) and actively participate in Fusion Center projects. Shortly after the events of 9/11, the FBI conducted a search warrant in Detroit, Michigan on an investigation of subjects suspected of being involved in terrorist activities. The identity of a fugitive wanted by the U.S. Secret Service for ID counterfeiting was found inside an apartment during the search. Featured on the TV program *Americas Most Wanted*, this fugitive was on the run and the subject of a large-scale manhunt. The investigation led to Cedar Rapids, Iowa, where the USSS was running out of leads. A visit to the DL station by USSS agents turned out to be a game changer when a DL clerk recognized the fugitive's photo from a recent driving test. Bureau investigators examined drive test records and identified a subject being pursued by the bureau on another investigation. Records were examined along with DL photos, and the fugitive's identity was found under a new alias and found to be associated with the subject being investigated by the bureau. The bureau provided this information to the USSS, who located and arrested the fugitive in Cedar Rapids. Bureau staff continues to enhance this information sharing partnership and they continue to be a vital resource for law enforcement fusion centers.

Maryland

In the spring of 2010, the director of the Maryland Coordination and Analysis Center (MCAC) contacted the Maryland MVA and requested that a full-time MVA investigator be assigned to the MCAC as part of the plan to enhance the capability of the nation's first fusion center. The original role of the MVA investigator has evolved into the individual serving as MCAC's Identity Crime Program Manager. This individual serves as a valuable liaison for law enforcement and identity theft victims. The MVA's partnership with MCAC allows the center to access MVA databases that are not routinely available to law enforcement while providing the MVA with the ability to work closely with more than two dozen law enforcement entities. The criminal and intelligence analysts at the MCAC have assisted the MVA during several external fraud investigations. They have provided flow charts of unlicensed sales organizations and have shared valuable information regarding individuals who have unlawfully obtained Maryland DLs or registrations for their vehicles.

Solicit Feedback from Law Enforcement Partners

One challenge when forming partnerships with external entities is finding ways to improve the relationships. After a partnership is established, it is important for DMVs to follow up with the law enforcement agencies to identify ways to improve communications, ensure that information is provided in the most useful manner, and identify other areas for improvement.

An example from Oregon provides a good example of why feedback is important. The DMV has non–law enforcement personnel serving in the role of investigator. Oregon law requires that identities caught through the Facial Recognition System (FRS) be forwarded to law enforcement for action. The DMV provides case files to the Oregon Department of Justice, which reviews the cases, shares them with federal law enforcement agencies, and then forwards them to the appropriate local jurisdiction for further action.

After the files are out of the DMV's hands, the DMV typically does not hear from law enforcement as to the outcomes of the cases, including any successes in identifying identity fraud or other crimes. The DMV did not know if law enforcement understood the information provided or even if the case files contained sufficient information for law enforcement to conduct investigations.

In January 2011, the DMV Fraud Prevention Section worked with the Department of Justice Criminal Justice Division to survey state and law enforcement agencies about its experiences working FRS cases. The survey also provided information on what agencies should be doing with the case files they receive. It was sent to more than 100 law enforcement partners.

Survey responses made it clear that many agencies found value in investigating FRS cases. The DMV's purpose in sending these cases is to encourage law enforcement to initiate further investigation into identity theft, benefit fraud, and other crimes. The survey process was beneficial in educating local law enforcement jurisdictions about handling case files. As a result of the survey, the DMV provided additional training to law enforcement and improved the working relationship with its partners.

Publicize Successes

By publicizing arrests and prosecutions, the visibility and reputation of the DMV is enhanced. The public and the legislature will begin to see the DMV as a force for good, an agency that goes after, and gets, the bad guy. The public will feel more confident that their personal data is entrusted to an agency whose priority is security. Legislators will appreciate the fact that funding dollars to support a fraud unit are well spent. Take the opportunity to issue press releases and promote your successes in combating fraud, without providing investigative tactics or sensitive case details.

When partnering with other agencies, notify them early in the partnership that you would appreciate coordinating any press releases that result from the investigation and be sure the DMV is mentioned as a party to the investigation. Regularly communicate with your leadership, including the governor's office, on fraud issues and what you are doing to address the challenges posed by fraud.

The announcement of arrests and prosecution serves as means to deter fraud. Announcements can also instill confidence in the DMV by others as they perceive the agency as being proactive in the fight against fraud.

Grant Opportunities

A variety of federal agencies offer grant opportunities and sharing programs that can provide support for investigative units.

The USSS operates an Electronics Task Force that works with local and state agencies that are involved with investigations related to fraud, facial recognition, and identity theft. It offers work space, access to specialized equipment, and overtime for participating agencies. The Electronics Task Force also participates with cases when needed.

The U.S. DHS Document Benefit Task Forces are set up around the country. They work closely with DMV investigative unit across the country and provide staff and equipment when needed. They also offer periodic grant opportunities for projects and system enhancements.

The U.S. Marshals have regional task forces that are set up across the country and work closely with many DMV investigation units. They can provide overtime reimbursement as well as staff and equipment to assist investigations.

The RISS Network has regional divisions that are used by DMV investigative units across the country. Members can access a variety of databases and can borrow specialized tools and investigative equipment when needed.

Federal Motor Carrier Safety Administration offers annual grant opportunities for agencies looking to make enhancements to its CDL license issuance process.

Chapter Five Tools in the Fight Against Fraud

DMVs are not on their own in the fight against fraud. Numerous tools, including standards and electronic systems, can provide assistance. The following table provides a list of tools that can be used. A detailed description of each program follows the table.

Drivers	Vehicles	Both Drivers and Vehicles
• Card Design Standards • Secure Card Design Principals • Commercial Skills Test Information Management System (CSTIMS) • Commercial Driver License Information System (CDLIS) • Digital Image Exchange • Driver License Data Verification (DLDV) • Electronic Verification of Vital Events Records (EVVER) • National Driver Register (NDR)/ Problem Driver Pointer System (PDPS) • Report Out of State Results (ROOSTR) • Social Security On-Line Verification (SSOLV) • State-to-State Verification • U.S. Passport Verification (USPass) • Verification of Lawful Status (VLS)	• Electronic Lien and Title (ELT) • National Motor Vehicle Title Information System (NMVTIS) • National Insurance Crime Bureau NCIB/ISO • National Odometer and Title Fraud Enforcement Association (NOTFEA) • Third party vehicle history providers	• Courtesy Verification Program (CVP) • Document ID databases • AAMVA's Fraud Alert Site • AAMVA's Fraudulent Detection and Remediation Program (FDR) • National Law Enforcement Telecommunication System (NLETS) • Regional Information Sharing System (RISS) • Third-party data brokers

Card Design Standards

AAMVA's DL/ID Card Design Standard (CDS) was developed by the Card Design Standard committee, whose representatives are jurisdictional and federal government employees. The CDS provides for the design of DLs/IDs, and its intent is to improve the security of the DLs/IDs and the level of interoperability among cards issued by all North American jurisdictions. AAMVA believes ID security will help increase national security, improve highway safety, reduce fraud and system abuse, increase efficiency and effectiveness, and achieve uniformity of processes and practices.

The CDS provides a standard for the design of DLs/IDs issued by AAMVA member jurisdictions. The intent of the standard is to improve the security of DLs/IDs issued by AAMVA's members and to improve the level of interoperability among cards issued by all jurisdictions. AAMVA respects the fact that each jurisdiction's laws and regulations determine its DL issuance processes and associated card requirements. As a result, the intent of the CDS document is to provide guidance on DL/ID design standards in order to provide a reliable source of identification and at the same time reduce a cardholder's exposure to identity theft and fraud.

Review a copy of the CDS at http://www.aamva.org/DL-ID-Card-Design-Standard/.

Commercial Driver License Information System

The Commercial Driver License Information System (CDLIS) is a nationwide computer system that enables state driver licensing agencies (SDLAs) to ensure that each commercial driver has only one DL and one complete driver record. SDLAs use CDLIS to complete various procedures, including:

- transmitting out-of-state convictions and withdrawals
- transferring the driver record when a commercial DL holder moves to another state
- responding to requests for driver status and history

CDLIS was established under the Commercial Motor Vehicle Safety Act (CMVSA) of 1986 and is based on the Federal Motor Carrier Safety Regulations (FMCSRs) in 49 CFR 383 and 384.

Learn more at http://www.nationaldriverregister-forms.org/ndr/information/commercial driver_s_license_information_system_cdlis.html or http://www.aamva.org/CDLIS/.

Commercial Skills Test Information Management System

The Commercial Skills Test Information Management System (CSTIMS) is an internet-based tool that provides a consistent way to track the scheduling and entry of test results for commercial skills tests by jurisdiction and third-party examiners.

CSTIMS enforces jurisdiction-defined rules to manage CDL skills testing and alerts various parties when circumstances are encountered that may require investigation to determine if fraud has occurred. Additionally, CSTIMS produces reports that can be reviewed for patterns of potential fraud.

Learn more at http://www.aamva.org/CSTIMS/.

Courtesy Verification Program

The Courtesy Verification Program (CVP) provides an effective and no-cost way for AAMVA members to determine if their DL/ID cards conform to the applicable AAMVA standards and specifications. This program is available for the review of MVA documents using machine-readable technologies. Just as compliance with these standards and specifications is voluntary, participation in the CVP is also voluntary.

AAMVA strongly encourages its member jurisdictions to regularly take advantage of the CVP. Even though AAMVA has published best practices, standards, and specifications covering DLs/IDs and the bar codes for other documents for years, inconsistencies in the implementation of those guidelines continue to occur. Such inconsistencies adversely impact the interoperability that is the main goal of AAMVA standards and specifications. A primary objective of the CVP is improving the consistency of implementation across all jurisdictions choosing to follow AAMVA standard and specifications. Information gained from the testing of jurisdictions' DLs/IDs and other documents is not only used by jurisdictions to improve their issuance systems but is also used by AAMVA to make improvements to the standards and specifications it publishes.

AAMVA recommends that its members consider submitting DLs/IDs and other documents on three occasions. The most important of these occasions is the introduction of a new configuration or design for the document. Many problems can be avoided if they are discovered before the actual issuance begins. Similarly, a jurisdiction may choose to have documents tested as part of its selection process when choosing a contractor. Finally, AAMVA strongly recommends regular, periodic retesting of documents at least annually. This last recommendation is based on the fact that we have discovered that unintentional changes to the format and content of issued documents sometimes occur after implementation.

The process for submitting documents is simple. The necessary forms and instructions are contained in the CVP application form.

Learn more at http://www.aamva.org/DL-ID-Card-Design-Standard/ (Courtesy Verification Program tab).

Digital Image Access and Exchange

The Digital Image Access and Exchange (DIA) program is one of many examples of AAMVA working cooperatively with jurisdictions to design and develop solutions that meet jurisdictional needs while continuing to focus on front-line staff and customer service and support. Leveraging existing functionality and proven technology, the DIA program has ensured that previous Problem Driver Pointer System (PDPS) and image-related investments are protected and new capabilities are easier to implement.

Benefits include improved customer service and support, enhanced public safety and security, reduced incidence of DL fraud, and acting as a building block to support Real ID Act mandates.

Learn more at http://www.aamva.org/Digital-Image-Access-and-Exchange/.

Driver License Data Verification

DLs, driving permits, and IDs issued by U.S. jurisdictions are regularly used as proof of identity; however, these documents can be counterfeited or altered. The Driver License Data Verification (DLDV) Service allows an organization that is presented with a DL or ID to verify that the data on the card matches the data held by the jurisdiction that issued the document.

DLDV provides users with immediate verification of identification document data. DLDV users submit data on a license, and the service returns a flag for each data element that indicates if the element matches the data on file with the issuing jurisdiction. Users interact with the service via a web-service call.

Learn more at http://www.aamva.org/DLDV/.

Document Identification Databases

AAMVA has partnered with several of our associate members to provide jurisdictions with a valuable online tool, the Genuine Document Reference (GDR) database, which can be used in conjunction with AAMVA's Fraudulent Detection and Remediation Program (FDR) training program for detecting fraudulent documents. The GDR provides an electronic guide to the DLs/IDs currently being issued by AAMVA members as well as past versions of their documents. This tool provides a quick overview of the overt security features that can then be validated in the MVAs or at the roadside.

Learn more at http://www.aamva.org/Fraud-Prevention-and-Detection/. Select the ID Document Databases tab.

Electronic Lien and Title

The ELT system provides the capability to electronically exchange lien and title information between a lienholder and a jurisdiction's MVA.

Jurisdiction Benefits

- Improved data accuracy resulting from the electronic exchange of data (reduction in typographical errors)
- Improved timeliness of data exchange (no more waiting for the mail)
- Reduction in the use and control of secure forms (paper costs)
- Reduction in mailing and printing costs
- Improved data and forms security

Lienholder Benefits

- Potential staff reduction in areas associated with filing, retrieval, and mailing of paper titles
- Reduction of storage space needed for filing and storing paper titles
- Ease of processing for dealer transactions

Information That Can Be Exchanged

The ELT system includes transactions that allow the jurisdiction to send electronic messages to the lienholder. For example, a jurisdiction can use the Lien Notification transaction to notify the lienholder that the lien has been recorded on the jurisdiction's title record.

The ELT system also includes transactions that allow the lienholder to send electronic messages to the jurisdiction. For example, a lienholder can use the Lien Release transaction to notify the jurisdiction when a lien is paid off. After processing, the jurisdiction creates and mails a paper title to the owner. In another example, a lienholder can use the Request for Paper Title to obtain a paper copy of the title but not release interest in the vehicle.

Learn more at http://www.aamva.org/ELT/.

Electronic Verification of Vital Events Records

The Electronic Verification of Vital Events Records (EVVER) system allows an MVA to verify information on a birth certificate presented by a DL applicant. EVVER verifies birth certificate information against vital records provided by the National Association for Public Health Statistics and Information Systems (NAPHSIS). The NAPHSIS is an association of public health officials concerned about vital records and health statistics. The NAPHSIS makes vital records available to organizations such as the SSA.

After receiving the birth certificate information from the MVA, the NAPHSIS routes it to the issuing jurisdiction's vital records agency, which matches the birth certificate to its records to verify data on the birth certificate. The issuing jurisdiction's vital records agency responds to NAPHSIS, which processes the response and routes it to the requesting jurisdiction MVA with the results of the verification.

Learn more at http://www.aamva.org/EVVER/.

Fraud Alert Site

AAMVA Alert Site was developed as a means of sharing document intelligence alerts issued by the DHS with driver licensing authorities. In 2014, the Alert Site was expanded to include both United States and Canadian federal, jurisdictional and provincial alerts and updates including vehicle alerts, lost or stolen materials and equipment, and document updates. The site provides:

- Images and information on both U.S. and Canadian fraudulent travel and identity documents
- Images and information on both U.S. and Canadian genuine travel and immigration documents
- Genuine and fraudulent document security features
- Detection points and methods that can be used
- Points of contact

The information disseminated is intended to raise the awareness of front-line counter employees on the use of fraudulent travel and identity documents such as passports, drivers licenses, visas, Social Security cards, vehicle titles, vehicle registrations and employment authorization cards which employees may encounter in the credentialing process. Managers and directors are encouraged to update and inform employees on those alerts pertaining to their daily job duties at the beginning of each shift. In the event employees encounter fraudulent documents in the DL issuance process, they should follow their jurisdiction's policies and procedures regarding such documents.

In an effort to maintain the integrity and security of the Alert Site, jurisdictions are limited in the number of users that may have access to the site. Users must have their administrator's approval before access can be granted.

Contact AAMVA to learn more.

Fraud Detection and Remediation

AAMVA's FDR e-learning program is the most widely used of AAMVA's tools and provides training on detecting fraud of all types. The program's core curriculum provides the basic techniques of document examination that front-line staff can use without the need for expensive forensic tools. By providing in-depth examples and explanations of the types of security features in circulation today, and most important, how to identify them, the course provides the tools needed to flag documents for review that may have otherwise been accepted at face value as genuine.

In addition to this core curriculum, the FDR program has expanded significantly in recent years to cover subjects far beyond physical documents only. With training modules and supplements that address such topics as people and actions, imposter fraud, internal fraud for managers, National Motor Vehicle Title Information System (NMVTIS) investigation tools, and many others, FDR provides fraud training and resources to a wide variety of staff far beyond the license counter, including investigators, managers, and administrators.

The training is broken into fully narrated, manageable modules addressing more than 25 specific fraud topics. You can use as many or few of the modules as you wish, allowing for complete customization of your training for students with differing job duties. Generally, each module requires approximately 30 to 45 minutes to complete and includes a downloadable job aid and knowledge assessment. The program can be implemented in many ways, including classroom deployment, computer-based training, and even installed on Learning Management Systems. FDR is free of charge to jurisdiction and law enforcement members.

Learn more about this highly acclaimed training resource at http://www.aamva.org/FDR-Training/.

National Driver Register/Problem Driver Pointer System

The National Driver Register (NDR) system is a computerized database of information about drivers who have had their licenses revoked or suspended or who have been convicted of serious traffic violations such as driving while impaired by alcohol or drugs. NDR also maintains the PDPS, a central database of drivers whose privilege to drive has been revoked, denied, cancelled, or suspended, as well as drivers who have been convicted of specific highway traffic safety violations. Each jurisdiction populates its own segment of the PDPS database with pointer information on its problem drivers. When a person applies for a DL, the DMV runs an electronic check to determine if the name is in the database. If a person has been reported to NDR as a problem driver, his or her license may be denied.

Learn more at http://www.nhtsa.gov/Data/National+Driver+Register+(NDR).

National Insurance Crime Bureau/ISO

The National Insurance and Crime Bureau (NICB) gathers and stores data from property and casualty insurance companies, self-insured organizations, and motor vehicle manufacturers from across the United States. The NICB has a partnership with insurers and law enforcement for the purpose of facilitating the identification, detection, and prosecution of those who commit insurance fraud. This information is invaluable for DMVs and law enforcement because it provides vehicle and accident history information and aids in the identification and location of property and people related to investigations. The NICB provides access to ISO Claimsearch, which is the leading organization and tool in the analyzing of insurance claim information for fraud fighting and is the mechanism used by law enforcement to electronically access insurance claim, people, and vehicle information.

Learn more at https://www.nicb.org/about-nicb or http://www.iso.com/.

National Law Enforcement Telecommunication System

The National Law Enforcement Telecommunication System (NLETS) is an interstate justice and public safety organization whose purpose is to exchange data among law enforcement entities internationally. Data exchanged include motor vehicle and driver and ID data, criminal history records, driver and ID photos, and booking photos. Members include law enforcement from the United States, U.S. territories, and federal agencies with a justice component. This data exchange network is a valuable resource for law enforcement to gather intelligence and facts regarding people, property, and locations.

Learn more at https://www.nlets.org/.

National Motor Vehicle Title Information System

NMVTIS is a system that allows the titling agency to instantly and reliably verify the information on the paper title with the electronic data from the jurisdiction that issued the title. NMVTIS is designed to protect consumers from fraud and unsafe vehicles and to keep stolen vehicles from being resold. NMVTIS is also a tool that assists states and law enforcement in deterring and preventing title fraud and other crimes. Consumers can use NMVTIS to access important vehicle history information.

NMVTIS was created to:

- Prevent the introduction or reintroduction of stolen motor vehicles into interstate commerce
- Protect states and consumers (individual and commercial) from fraud
- Reduce the use of stolen vehicles for illicit purposes, including funding of criminal enterprises
- Provide consumers protection from unsafe vehicles

Learn more at http://www.aamva.org/NMVTIS/.

National Odometer and Title Fraud Enforcement Association

The National Odometer and Title Fraud Enforcement Association (NOTFEA) was formed in 1980. NOTFEA's purpose and mission is to deter odometer, rebuilt or salvage, and other auto fraud through promoting and encouraging cooperation and fostering a working relationship among law enforcement and consumer protection agencies, licensing and motor vehicle departments, the automotive industry (including manufactures, dealers, leasing companies, and auctions), and individuals interested in deterring such fraud by developing a network of those persons and organizations.

Learn more at http://www.notfea.org.

Regional Information Sharing Systems

The RISS Program—*A Proven Resource for Law Enforcement*™—is a nationwide information sharing and investigative support program that serves thousands of local, state, federal, and tribal law enforcement and public safety agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, England, and New Zealand. Officers, analysts, and other criminal justice partners rely on RISS for its proven and secure information sharing capabilities, as well as its professional, innovative, and critical investigative support services. RISS serves as a force multiplier, effectively and efficiently aiding agencies in tackling crime problems in their areas. RISS consists of six regional centers as well as a technology support center. The six RISS Centers are:

- Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network® (MAGLOCLEN)
- Mid-States Organized Crime Information Center® (MOCIC)
- New England State Police Information Network® (NESPIN)
- Rocky Mountain Information Network® (RMIN)

- Regional Organized Crime Information Center® (ROCIC)
- Western States Information Network® (WSIN)

RISS developed and continues to maintain the RISS Secure Intranet (RISSNET™). RISSNET is a secure Sensitive But Unclassified (SBU) law enforcement sharing cloud provider. RISSNET houses and provides access to millions of pieces of data, offers bidirectional sharing of information, connects disparate systems, and acts as the communications infrastructure for a number of critical resources and investigative tools. More than 85 systems are connected or pending connection to RISSNET, and more than 350 resources are available to authorized users. RISS has developed a number of information sharing resources available via RISSNET, including the RISS Criminal Intelligence Databases (RISSIntel™), the RISS Officer Safety Event Deconfliction System (RISSafe™), the RISS Officer Safety Website, the RISS National Gang Program (RISSGang™), and the RISS Automated Trusted Information Exchange (ATIX™).

RISS provides law enforcement agencies and officers a variety of investigative support services to enhance and improve their ability to detect, apprehend, and successfully prosecute criminals. These services include analytical, investigative support and research, equipment loans, confidential funds, training and publications development, field services support, and technical assistance.

Learn more at http://www.riss.net/.

Report Out-of-State Test Results

Report Out-of-State Test Results (ROOSTR) is an Internet-based application that allows jurisdictions to share skills test results for out-of-state applicants electronically and securely to their home jurisdiction. Electronic notification and data submittal from the testing jurisdiction allow the licensing state to retrieve trusted data directly from ROOSTR, eliminating the need to rely on paper forms and reducing opportunities for fraud.

Learn more by contacting the AAMVA Help Desk.

Secure Card Design Principles

This is a companion to the CDS—the Secure Card Design Principles (SCDP)—and sets out to address those issues that cannot easily be addressed by DL/ID standard. The SCDP whitepaper is intended to lay out a set of principles and guidelines that can help maximize the probability of developing and maintaining a DL/ID that will be more resistant to compromise. Where the CDS provides the "building blocks" for designing a secure DL/ID card, the SCDP companion paper further describes a process for how to use those "blocks." There are many considerations to keep in mind beyond just the physical document and the particular security features it may contain.

Learn more at http://www.aamva.org/Best-Practices-and-Model-Legislation/.

Social Security Online Verification

The U.S. Social Security Administration, which currently provides a Social Security Number (SSN) batch verification service to government agencies, has expanded its service to allow online SSN verification.

Jurisdiction DMVs are now authorized by the SSA to obtain SSN verification information either in batch or online mode. Online support allows a jurisdiction to verify an individual's SSN during the DL issuance or renewal process while an applicant is still at the counter. Note that the SSA only verifies information transmitted by a DMV (i.e., whether or not the DMV information did or did not match the SSA information); it does not disclose other data.

AAMVA has developed a Social Security Number Online Verification (SSOLV) package to assist jurisdictions in implementation. The package includes:

- SSA/State Memorandum of Agreement: The legal agreement between an interested MVA and the SSA
- SSOLV Application System Specifications: Requirements for implementing the verification service
- SSOLV Application Structured Test Plans: Structured testing procedures and test cases for testing with AAMVA and SSA

Learn more at http://www.aamva.org/SSOLV/.

State-to-State Verification

The State-to-State (S2S) Verification Service is a means for states to electronically check with other participating states to determine if the applicant currently holds a DL/ID in another state. State participation in S2S is voluntary.

Participation in S2S does not commit a state to be in compliance with the federal REAL ID Act. However, if a state chooses to be REAL ID compliant, S2S can be part of its compliance plan.

The key business requirements include:

- Limit a person to one DL/ID: Enable a state to determine if a person holds a DL/ID in another state.
- Enable a state to send a request to another state to terminate a DL/ID.
- Provide information on all state issued DLs/IDs nationwide: Enable states to verify DL/ID cards presented as a form of identification.
- For states wanting to be compliant with REAL ID, limit a person to one REAL ID card (whether DL or ID): Enable a state to determine if a person holds a REAL DL or REAL ID Card in another state.

In October 2012, AAMVA was awarded a contract from the Mississippi Department of Public Safety under a grant from the U.S. DHS to develop the S2S Verification Service leveraging the modernized CDLIS system architecture, Network Control Software (NCS), and Unified Network Interface (UNI). In addition to the legacy AMIE method, a National Information Exchange Model (NIEM)–compliant Web Service access method will also be developed.

These changes and the associated rollout will be spread over two major phases:

1. Pre-pilot phase (system development and deployment): October 2012 to March 2015
    - The pre-pilot phase consists of all the tasks that are required to build the different system components necessary to begin the pilot activity with participating states. This phase includes the development of system specifications and other documentation needed by the pilot states to develop their applications; the Central Site upgrade, along with development of the associated UNI and Web Service access methods; and a new user interface to generate reports.
    - AAMVA is scheduled to begin structured testing with the pilot states in March 2015. The Central Site Production go-live is scheduled for July 2015.
2. Pilot phase (implementation: pilot states): March 2015 to March 2017
    - The pilot phase consist of tasks that are required to execute the pilot with participating states. This phase includes training and structured testing with the pilot states.
    - As states successfully complete the structured testing, they will be certified to move into production. Eleven states are scheduled to move into go-live between July 2015 and June 2016.

Learn more at http://www.aamva.org/State-to-State/. (See the roadmap on the Documentation tab.)

Third-Party Data Brokers

To conduct a successful investigation and to provide tools in the validating of information, it is important to have access to data from as many sources as possible. Third-party data providers garner information from a variety of public sources that can be searched and analyzed in a multitude of ways and techniques. This information can link vehicles, people, addresses, and businesses together, providing leads and validating or invalidating information provided. Access to one or more of these sources of information will prove to be a valuable resource in fraud fighting, prevention, and deterrence.

Third-Party Vehicle History Providers

Several private companies provide services in the collection and reporting of vehicle histories. As vehicles move across North America and the world, it can be challenging to locate history information, and DMVs are not the only source for this information. These third-party vehicle history providers gather vehicle information from DMVs and from a variety of other sources, including repair facilities, border inspections, safety and emission inspection facilities, and toll facilities, to name a few. When researching vehicle histories, it is important to have as much information as possible, and these companies can be a helpful asset.

Verification of Lawful Status

The Verification of Lawful Status (VLS) application provides a solution to two requirements encountered by state MVAs:

1. Fake and altered immigration documents may be presented to DMVs as proof of identity and proof of lawful status in the United States. VLS allows the DMV to verify that the document matches the electronic record of the document held by DHS in the Systematic Alien Verification for Entitlements (SAVE) program.
2. Real ID–compliant driver licenses and ID cards can only be issued after a DMV has verified the lawful status of the applicant. VLS provides a means for DMVs to comply with this verification requirement.

VLS is designed to be integrated into DMV driver licensing and ID card issuing systems. Legacy AMIE messages or a Web service interface can be used for integration. Both options allow the VLS requests and responses to operate in real time.

Learn more at http://www.aamva.org/VLS/.

Chapter Six Vulnerabilities and Controls

The more controls that are in place to detect and deter fraud, the more benefits that can be reaped. If internal control processes and systems are implemented only to prevent fraud and comply with laws and regulations, then an important opportunity is missed. The same internal controls can also be used to systematically improve businesses, particularly in regard to effectiveness and efficiency.

The benefits of having at least one control measure in place for each risk area include the following:

- Appropriate checks and balances for all business processes ensuring effective, consistent, and efficient operations and processes
- Increased reliability of financial and statistical reporting
- Ensured compliance with applicable laws and regulations
- Effective and uniform application of procedures
- Increased fraud deterrence and prevention
- Clear expectations for staff and management
- Safeguarding of assets
- Credibility of credentials
- Positive morale
- Improved perception of staff as professionals
- Increased respect of administration
- Decreased possibility of identity theft, financial theft, asset theft, and criminal activities

The checklists on the following pages provide recommendations for processes and technology solutions that can be implemented to identify and combat both internal and external fraud. It is impossible for any jurisdiction to implement all of the recommendations herein. Administrators and managers should review the list and carefully consider each suggestion. Some provide for immediate implementation, but others will take longer to achieve an operational level. Funding may be a consideration for some of the solutions. Management must revisit controls on a regular basis and make enhancements and improvements to ensure the organization is staying ahead of potential risks. As the agency improves its processes, it should expect those who wish to circumvent them to develop new ways to do so.

Best practices are outlined via two sets of recommendations; one addresses process and procedural practices, and the other addresses technology controls, both of which are needed to combat internal fraud.

Fraud Deterrence and Detection Vulnerabilities and Controls Checklist			
Area of Vulnerability	**Specific Risk and General Recommendations**	**Process Recommendation or Solution**	**IT Recommendation or Solution**
General Review • Controls	• All agencies have fraud challenges; it is simply a matter of how big the problem is and how proactive management is in identifying and deterring fraud. • New technologies and constantly evolving schemes—for both staff and criminals—make it imperative that you no longer accept the status quo and that you are constantly proactive in looking for, combating, and deterring internal fraud. • Understand what drives the need that motivates employees to commit fraud, including hard economic times; financial difficulties; and event-driven occasions such as back to school, holidays, and addictions in order to identify employees at risk of committing fraud. • Agencies must emphasize adherence to policies and procedures and let employees know the repercussions for failure to comply. • Follow up and publicize your actions so employees know the agency is serious about fighting fraud. • Look for gaps that would allow employees to defraud the system and take steps to correct them. Be diligent after making changes by continuing to police processes and procedures. Making adjustments once will not fix identified problems indefinitely. • Audit processes must be developed, implemented, and constantly evaluated to ensure you are keeping up with changes and advancements to fraud schemes.	❑ Review processes and tools available to identify and combat internal fraud; make adjustments as necessary/ ❑ Complete regular review of processes and make updates and enhancements as technology changes, as loopholes are identified, and as fraud "schemes" progress and advance. ❑ Identify processes that need to be changed and make the necessary changes. ❑ Develop and implement an audit plan for processes associated with transactions, system access, issuance, inventory, overrides, financials, and so on. ❑ Include random reviews of processes and procedures to ensure proper steps were taken, appropriate documents were reviewed and scanned, required fees were collected, and so on. ❑ Audit a variety of each type of transaction on a regular basis. ❑ Establish a regular schedule to review and update the audit plan. ❑ Train staff on how to spot fraudulent documents and verify the authenticity of genuine documents. ❑ Establish an audit review committee to review processes, including those subject to override by managers. ❑ Separate duties for those responsible for finances and money. ❑ Implement job rotation for sensitive positions. ❑ Take investigative action any time suspicious activity is identified.	❑ Review IT system reporting and audit capabilities; make enhancements as needed to help identify, combat, and correct internal fraud. ❑ When possible, capture manager approval electronically to facilitate tracking and auditing of exceptions processing (e.g., overrides). ❑ Use digital system sign-in via a fingerprint scan to prevent employees from unknowingly obtaining a supervisor or manager password and approving transactions without proper authority to prevent employees from processing transactions using someone else's credentials. ❑ Be diligent about identifying potential technology gaps that may allow internal fraud. ❑ Take steps to close gaps. ❑ If a technology solution cannot be immediately implemented, develop a manual solution until the technology solution can be implemented. ❑ As systems are enhanced as a result of technology refreshments or policy or statutory changes, keep internal fraud in mind and ensure system enhancements help combat it. ❑ Require IT security awareness training for all employees who have access to DMV systems.

(*continued*)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
General Review • Controls *(continued)*	• The need for audits processes must also take into consideration what reviews are made by managers and supervisors to ensure that the internal controls are being followed. • Make sure there are processes in place to ensure that the managers, supervisors, and auditors also adhere to the agency's processes. In other words, check the checkers. • Conduct background checks as a condition of employment. • Display posters on ethics and fraud. • Develop working relationships and partnerships with local, jurisdictional, and federal agencies. • Form a fraud working group. • Create or enhance a right-sized fraud unit, with appropriate resources and training tools. • Use an internal fraud unit to review RFPs and proposals and other fraud reduction efforts.	❑ When wrongdoing is identified; take swift and certain personnel or legal action (e.g., discussion, documentation, retraining, disciplinary steps). ❑ Implement a hotline for reporting fraud and abuse by both employees and the public and let other employees know you mean business by publicizing any arrest or conviction. ❑ When applicable, put a notation in the individual's personnel file that she or he cannot or should not be hired by the agency or by any other government agency. ❑ Share best practices and lessons learned with your peers.	
General Review • Exception Processes and Overrides	• Overrides, although undesirable, are sometimes a necessity in our business. Multiple levels of approval can help reduce wrongdoing. • Exceptions processes should be tightly controlled and monitored.	❑ Require management review of documents for all transactions in which an override or exception process is initiated. ❑ Require exception or override transaction review and authorization by a supervisor or manager. ❑ Regularly review transactions that can be overridden and their related processes, looking for weaknesses on (at least an annual basis). ❑ Make adjustments as warranted. ❑ Regularly review exceptions processing, looking for weaknesses or holes (at least annually).	❑ Require management override to be electronically initiated before transaction can complete. ❑ Automatically stop transactions when appropriate. ❑ Develop and implement an electronic audit log that includes the capture of all overrides, who authorized the override, and who processed the transaction. ❑ Use this information to develop reports that are reviewed by a supervisor or someone outside of the area in which the override occurred; look for patterns.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
General Review • Exception Processes and Overrides *(continued)*		❑ Make adjustments as warranted. ❑ Do not allow a supervisor or manager to. override his or her own transactions. ❑ Require one-person offices to request central office authority for overrides.	❑ Record override activity in such a way that they can be easily discovered or reviewed later. ❑ Require electronic secondary review before an override can be completed.
General Review • Mail room	• Ideally, customers will not submit cash to pay fees. You can request customers not pay by cash, but the reality is, the agency will receive some cash. Ensure procedures are in place to avoid theft by employees (e.g., cameras). • Lock box processing can help ensure the safety of funds received. • Ensure safeguards are in place for returned indicia (e.g., authorizing document such as registration stickers or decals, license plates, driver licenses, ID cards) to prevent theft.	❑ Monitor or control inbound and outbound mail. ❑ Use a locked box for remittance processing. ❑ Set up processes to ensure cash and checks are securely processed. ❑ Immediately endorse all checks received. ❑ Ensure deposits are made securely and in a timely manner. ❑ Returned indicia procedures must account for any controlled document(s) (e.g., update customer's account, return indicia to inventory, destroy indicia).	❑ Install cameras in the mail room and other areas where payments are processed. ❑ Review tapes on at least a random basis. ❑ If you cannot afford working cameras, façade cameras can also help to deter theft.
General Review • Facility access	• Unauthorized access to sensitive areas or unsupervised after-hours access creates risks of misappropriation or misuse of sensitive inventory. • After-hours access to buildings should be tightly controlled and logged and should require the authorized employee to present a pass code, swipe card, or biometric before being granted access to sensitive areas or access to the building after hours. Such a system can ensure access is restricted to authorized personnel only. • Cameras, both overt and covert, can serve as both a deterrent and an investigative tool for theft and foul play. Motion-activated cameras can provide 24/7 security without the need for personnel. By recording only when motion is sensed, a review of recorded activities is more efficient. Remote viewing of cameras by supervisors or investigators is beneficial.	❑ Develop and adopt a comprehensive physical security plan for central and field offices and for other DMV facilities. ❑ Establish a regular schedule to review plans and make updates as needed (at least annually). ❑ Ensure third-party providers have comprehensive physical security plans in place. ❑ Complete background checks for staff with access to sensitive areas, including janitorial and maintenance staff. ❑ Investigate unauthorized access to buildings and sensitive areas. ❑ Tighten processes when applicable. ❑ Take employee action (e.g., warning, counseling, dismissal) when unauthorized access is made.	❑ Control access to buildings, as applicable, through implementation of a keycard, pass code, or biometric identifier to prevent unauthorized access to buildings or secure areas of buildings. ❑ Provide electronic authorization to buildings and sensitive areas based on job responsibilities. ❑ Electronically track entry and departure to buildings and sensitive areas. ❑ Electronically track employee access to hours reported as worked. ❑ Generate alert when authorized access is attempted. ❑ Regularly review access logs and take action when appropriate to tighten access controls.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
General Review • Facility access *(continued)*	• Alerts can be sent or reports generated and reviewed the following day for after-hours access. • A sign that advises individuals may be under video or audio surveillance will serve as a deterrent to both employees and the public. • After-hour access logs and video footage should be reviewed to verify that there was a business purpose for entry. • Consider the need for prior approval for after-hours access to areas where after-hours access is not normally needed.	❑ Establish building or secure room access limitations for each employee based on his or her specific duties and not on his or her general job classification. ❑ Establish procedures to watch camera footage on a regular basis to look for foul play. ❑ Set a retention schedule for camera footage sufficiently long for use in later investigations.	❑ Generate exception reports that show when employees are accessing the facility outside of normal operating hours. ❑ Ensure that employee access to buildings and systems is automatically and immediately revoked when an employee leaves employment, terminated or on administrative leave. ❑ Install and monitor cameras throughout facility, particularly in sensitive areas (both overt and covert). ❑ Fake cameras can also help to deter wrongdoing. ❑ Watch the camera footage on a random basis, looking for irregularities. ❑ Retain sufficiently long for use in later investigations. ❑ Zone building so alarms stay on in sensitive areas to prevent unauthorized individuals from entering.
General Review • Equipment control	• Use security devices for any piece of equipment that issues credentialing documents such as DLs or titles. Remove the devices when the office is closed and keep them in a secure location to prevent inappropriate indicia or document issuance. • Take immediate action to inventory and tag equipment when received. Completing a regular inventory will help deter theft or will allow quicker identification of theft when or if it occurs. • Copy machines can retain images of copies made on their hard drive. Nearly every digital copier built since 2002 contains a hard drive and stores an image of every document copied, scanned, or emailed by the machine. Be sure to sufficiently destroy retained images when getting rid of copy machines.	❑ Install security devices, such as DL/ID card printer dongles or other cryptographic devices, at the start of each work day; such devices must be present for the printer to work. ❑ Remove security devices at the close of business each day to prevent unauthorized use; lock secure devices in a safe when not in use. ❑ Establish inventory controls for production equipment. ❑ Store excess equipment in a secure area and require authorization for access to deter theft.	❑ Require security devices such as a key, USB device, or dongle on DL/ID card printers to be present for the printer to work for over-the-counter issuance of DLs/IDs. ❑ Secure local servers and allow only authorized individuals to access the server room. ❑ Disable USB drives on computers to prevent unauthorized individuals to use drives or to prevent viruses. ❑ Unless there is a business need, computers should not have a disc drive. ❑ Scrub all data from the hard drive of computers and copy machines before they leave the possession of the agency.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
General Review • Inventory control	• Any and all indicia (titles, plates, disabled parking placards, DL/ID materials, inspection stickers, license plate validation stickers) should be kept in a secure area that is accessible by only authorized staff. • The amount of inventory issued to third parties should be monitored and the quantities issued adjusted to ensure an appropriate amount is kept on hand. • Excess inventory should not be maintained in field offices or at third-party provider locations. • Report left or loss of indicia or equipment to AAMVA's fraud alert site.	❑ Keep inventory and indicia in a secure and locked location to prevent theft or misuse; provide access to only authorized personnel and track entry. ❑ Include in inventory processes a review of where forfeited and surrendered documents are kept (DLs, titles). ❑ Tighten processes as appropriate to prevent unauthorized access to the area. ❑ Reconcile controlled inventory on a frequent and regular basis. ❑ Boxes containing numbered indicia should be resealed after initial inventory is completed and reopened only as needed for use. ❑ Periodically conduct inventory reconciliation of inventory issued to third parties. ❑ Control and secure indicia received by return mail. ❑ Record return of credentials in driver or vehicle records. ❑ Control and physically destroy returned plates with decals to prevent the decals and plates from being removed and reused.	❑ Electronically track issuance of all controlled stock. ❑ Generate reports when controlled stock is used out of sequence; investigate and take appropriate action. ❑ Record returned indicia on the driver or vehicle record.

DMV Customers and Public
• General recommendations
	• Failure to implement and follow proper processes could result in financial, theft, or other illegal gain by those wishing to do harm.
	• DMV customers may commit or attempt to commit fraud for a multitude of reasons. Processes should be in place to detect and deter fraud in all parts of the agency.
	• Legitimate documents issued under fraudulent circumstances can be used to perpetuate a multitude of crimes.
	• Failure to collect correct fees could result in an unintended decrease in revenue for the agency.
		❑ Establish reciprocity standards for DL exchange.
		  ❑ Look for out-of-state applicants who failed the DL test numerous times and then returns with an out-of-state DL.
		  ❑ Ensure out-of-state applicants meet or exceed your standards.
		  ❑ Accept out-of-state DL/ID for identity only; require applicant to meet your licensing standards.
		❑ Train license issuance staff using FDR and other training tools and include training on interview techniques and how to stall a customer so authorities can be alerted of suspected fraud.
			❑ Use document scanning workstations and electronically attach scanned images to records.
			❑ Use an electronic document authentication system.
			❑ Electronically verify medical providers.
			❑ Use biometrics.
			  ❑ Follow established standards for print capture.
			❑ Implement knowledge base authentication.
			❑ Electronically access and verify information and documents with available databases.

(*continued*)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
DMV Customers and Public • General recommendations *(continued)*	• Submission and acceptance of fraudulent document(s) could lead to a variety of crimes. • DMV staff may be coerced by those wishing to compromise the system.	❑ Photocopy suspicious documents; confiscate them if possible. ❑ Give staff tools they need to authenticate or validate documents (e.g., mag loupes, lights, and access to databases). ❑ Build them into workstations. ❑ Develop a plan or process to get law enforcement assistance in the field when necessary. ❑ Implement a two-step process (two employees to review ID documents for new applicants). • Customer queuing software can help. ❑ Establish physical office security standards. • Minimize contact and interaction between FTE and customers to limit bribe attempts. ❑ Look to next-generation prevention in the design of credentials and processes. ❑ Create processes to deal with victims of identity theft and domestic violence. ❑ Establish processes to deal with insufficient funds payments. ❑ Require reporting to other affected agencies or jurisdictions of indicia loss or theft. ❑ Identify and share fraud information and trends with applicable entities and partners.	❑ Use address validation software. ❑ Use automated knowledge testing or randomly generated tests. ❑ Implement IT system checks to look for multiple use of addresses. ❑ Use cameras, real and fake, for monitoring. ❑ Capture field of passport and country, enabling identification of trends. ❑ Take the photo first and access the photo at each stop. ❑ Establish partnerships with the Bureau of Vital Statistics to validate birth certificates. ❑ Flag records as soon as possible when fraudulent documents are submitted at the time of application. ❑ Use image capture or create application-only records; must be able to notate record with details.
County and Municipal Entities Handling Transactions on Behalf of the DMV	• Issuance of credentials or release of information based on counterfeit or fraudulent documents can pose a threat to homeland security, highway safety, individuals, and the public in general. • Third parties may provide illegal access to public services or assistance unless proper controls are in place. • Failure to have proper financial, inventory, and processes in place may result in theft of funds or indicia.	❑ Set standards for who can be a third-party agent. • Legislative action is likely necessary because third parties can be politically sensitive. • This is often a highly political situation, so it is necessary to figure out how to make a case for the DMV to ultimately be in charge or take away some of the discretion of the county or municipality.	❑ Move to online or electronic transactions when possible. ❑ Require imaging and uploading to the DMV system of documents received and issued by third parties. ❑ Require electronic reporting of issuance, transaction, and volume information. ❑ Use electronic surveillance of transactions and reports to identify potentially high-risk operations.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
County and Municipal Entities Handling Transactions on Behalf of the DMV *(continued)*		❑ Establish MOUs/SLAs and renew them regularly. • The DMV **MUST** have complete oversight, including the ability to take swift and appropriate action for violations and violators. ❑ Require same employee eligibility requirements for third parties as required for DMV staff (e.g., background checks). ❑ Require entities to post a bond. ❑ Establish standard operating policies and procedures and require entities' compliance. • Give third parties as little discretion as possible to deviate from processes. • Automate as much as possible to reduce opportunities for fraud. ❑ Provide or require initial and ongoing training of third parties. ❑ Consider revenue sharing for online transactions. ❑ Set standard for security and destruction of indicia (ANSI standard). ❑ Audit regularly in the field and centrally, including covert observations, either in person or by camera. ❑ Require federal recommendations for FTE be followed for EDL issuance.	❑ Require electronic reports and electronic funds transfer of monies due in a timely manner.
Partnerships • Licensed businesses *(e.g., dealers, driving schools, salvage yards)* • Third Party Agents *(county officials, AAA, title services, tag agents, emissions and inspection stations, junk and salvage dealers)*	• Case management guidelines and processes for the handling of investigations, complaints, infractions, and so on should be established and documented. • Off-the-shelf case management systems can help track third-party partners' activities, issue tracking, contracts, and so on. Also, case management systems provide an effective method to manage investigations.	❑ Review, and if necessary, rewrite contracts with third parties that process transactions on behalf of the DMV to give the DMV more authority and control over the third-party regarding operation, personnel, oversight, and so on. ❑ Require independent contractors and third parties who have access to DMV systems to submit to the same background and security checks as internal employees. ❑ Require third parties accessing DMV records to follow the same guidelines for protecting customer data as internal staff.	❑ Require submission of information electronically whenever possible (e.g., certification for driver education or motorcycle safety training, insurance verification, convictions from courts). ❑ Use case tracking system for quality control and assurance. ❑ Monitor systems and record access by third parties and contractors providing services to the DMV to ensure compliance with system and record access rules.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Partnerships • Licensed businesses *(e.g., dealers, driving schools, salvage yards)* • Third Party Agents *(county officials, AAA, title services, tag agents, emissions and inspection stations, junk and salvage dealers)* *(continued)*	• Rotating auditors so they are not consistently responsible for the audit of the same entities prevents collusion by limiting the relationship between the auditor and the audited entity. • Oversight of third parties should mimic, as closely as possible, processes in place for DMV internal staff.	❑ Require third parties to sign agreements similar to those signed by DMV employees, including codes of conduct and ethics. ❑ Ensure authority is in place to shut down the third party or take other disciplinary action for failure to follow established rules. ❑ Randomly audit transactions processed by third-party entities on a regular and ongoing basis. ❑ Rotate auditors so they are not responsible for the audit of the same entities on an ongoing basis. ❑ Establish a two-step approval process for third-party data access and purchase. ❑ Periodically review contract compliance with the DPPA or the Canadian equivalent. ❑ Encourage customers of third-party processors to report problems or suspected fraud to the DMV, perhaps through a hotline. ❑ Routinely audit agency inventory controlled by third parties (e.g., dealers who are authorized to provide temporary tags or license plates). ❑ Publicize a hotline for reporting fraud or suspicious activity internally and in field offices. ❑ Require partners to publicize the hotline in their offices.	❑ Investigate and take appropriate action. ❑ Tighten processes when possible. ❑ Prohibit removal of customer data from the DMV by contractors and third parties. ❑ Implement a fraud hotline that customers can use to report suspicious activity. ❑ Implement case management guidelines and processes to handle investigations, complaints, infractions , and so on.
Human Resource Management • Hiring • Retention • Promotions • Terminations	• A zero tolerance policy for fraud should be created through the agency's code of ethics. All employees should be required to annually review the policy and sign a statement that they understand it and agree to follow it. • The agency's code of conduct should include fraud deterrence language. • Posters about fraud throughout the office can remind employees about the issue and serve as a deterrent.	❑ Ensure employees read, understand, and sign internal policies and codes regarding fraud and the repercussions for failure to follow ethics and established rules for system access, accounting processes, penalties for violations, and so on. • Include language to deter fraud directly into your code of ethics and conduct.	❑ Require electronic "clock-in" and "clock-out" by employees. ❑ Assign unique IDs and passwords for system access; better yet, provide system access via a keycard or biometric. ❑ Grant the ability to process specific transactions based on user ID and password as needed for job requirements; even better, require biometric or keycard authorization before granting system access.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Human Resource Management • Hiring • Retention • Promotions • Terminations (*continued*)	• Background and financial checks, particularly for those in sensitive areas, can be a tremendous aid in ensuring quality of staff. • Cameras, both overt and covert, can serve as a deterrent and as an investigative tool for staff theft and foul play. • In addition to fraudulent issuance of documents, alteration of records, or theft of funds, employees can also commit fraud by embezzling time by forging timesheets and leave slips. Technology and supervisory reviews can help prevent such practices. • Proper processes and checks can prevent employees from submitting fraudulent or inflated expense reimbursement requests. • Institute employee or public hotlines to allow reporting of fraud and theft. • Garnishments or bankruptcy filings should be an indicator that an employee is having financial problems that may make him or her more susceptible to committing fraud or theft	❑ Complete background and financial checks before promotion and on a regular or random basis, especially for personnel with system access, individuals privy to confidential information, and those who handle any type of payment. ❑ Be diligent in observing employees who handle payments; complete regular spot monitoring, particularly if foul play is suspected. ❑ Check driver and motor vehicle record before hiring and run records on a regular basis. ❑ Identify actions that put an individual or agency in difficult situation or that bring discredit to the agency. ❑ Be observant of employees' lifestyles; be diligent in reviewing the work of employees living above their means or those dealing with financial crises; it may be indicative that they are taking payment for "illegal" transactions or that they are committing some type of theft. ❑ Develop procedures to permit or require employees to explain or notify the DMV when there are adverse events in their background on an ongoing basis or as violations occur (e.g., bankruptcy, criminal activities, arrests). ❑ Take disciplinary action for failure to report. ❑ Establish legal authority, including statutory, administrative, and criminal authority for disciplinary or dismissal actions when fraud occurs, including preventing employee from working for another agency. ❑ Take swift and appropriate action when fraud is identified. ❑ Control the level at which retention or termination decision is made. ❑ Thoroughly document progressive discipline steps taken.	❑ Establish a hotline for fraud reporting by employees and the public. ❑ Generate annual reports and reminders for background, financial, and driver checks for employees working in sensitive areas.

(*continued*)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Human Resource Management • Hiring • Retention • Promotions • Terminations *(continued)*		❑ File criminal charges when applicable. ❑ Publicize action taken to discourage other employees from taking similar actions. ❑ Complete exit interviews with every employee before they leave; ask about irregularities and vulnerabilities in their work area. • Departing employees may be aware or be suspicious of fraudulent activity and are anxious to report it as they prepare to walk out the door. ❑ As soon as employees are terminated or placed on administrative leave, invalidate system and building access, collect keys or pass cards, and so on.	
Human Resource Management • Employee training	• In addition to training staff on their job duties, it is imperative that you provide information on repercussions for failure to follow policies. Part of the battle is education; tell staff what is acceptable and what will happen for failure to follow established processes. • Ensure that new employee training emphasizes the agency's fraud deterrence and prevention policy, ethics policy, code of conduct, and so on. Administrators should deliver fraud messages. During new employee orientation and other employee training, give real-world examples of fraud in the agency and the consequences suffered by employees who committed fraud. Delivery by the administrator sends a powerful message. • Provide annual refresher training on the agency's fraud policies.	❑ Establish a zero tolerance policy for ethical, fraud, and theft and establish disciplinary actions for all other violations of policies and procedures, rules, regulations, and laws. ❑ Establish a code of ethics or conduct for employee behavior and require annual signatures by employees. ❑ Train staff on ethics, proper procedures and policies, and any repercussions for failure to comply with established processes. ❑ Provide initial and ongoing ethics training. ❑ Train employees on how to spot fraud and what to do when they suspect it, including where to report it and what types of information they should provide. ❑ Create written materials to be distributed to each new and existing employee to provide information about the agency's fraud deterrence and prevention policies and how to report suspicions of fraud (internal and external).	❑ Develop self-administered electronic training for ethics and code of conduct policies. ❑ Electronically record and track employee training and refresher training. ❑ Generate reminders when training is due. ❑ Set up and publicize a hotline employees can use to report fraudulent activity.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Human Resource Management • Employee training *(continued)*	• A fraud hotline can allow employees to provide information on fraud activities and suspicions in a safe and nonthreatening manner. Let employees know about the hotline and encourage them to use it if they suspect fraud.		
Human Resource Management • Employee monitoring and oversight	• After employees are trained, they should be monitored on a regular basis to ensure established procedures are followed. • Do not assume you have only honest and ethical staff. Although most will be, you will also likely have employees who will steal or commit fraud. They may be those you least suspect. • Do not forget to monitor the monitors or check the checkers—auditors, supervisors, and managers. No one is above temptation or reproach. • Front counter staff should not be allowed to have personal items, such as purses, backpacks, or cell phones, at the front counter. Cell phones can allow staff to make calls or send texts to advise a fraudster to come to the office or counter immediately or to provide confidential information or take a screen shot of a document or record. • Talk to staff regularly and make sure they are comfortable reporting their suspicions. They probably will not report if they believe they will be negatively impacted or threatened in any way. • In small rural field offices (one- or two-person operations) where some internal controls are not possible to fully implement, determine if other procedures can be implemented to deter fraud.	❑ Develop, measure, and refine (update) audit, oversight, and supervisory controls. ❑ Implement ongoing monitoring programs to check employees' work performance on a regular basis (daily, weekly, or monthly, as appropriate for the job). ❑ Conduct spot monitoring on a regular basis to check specific transaction types or samples of work. ❑ Document monitoring results and complete training and retraining as indicated. ❑ Complete end-of-day reviews and reconciliations for key and critical processing areas. ❑ Establish processes to verify that supervisors are properly reviewing, monitoring, and approving transactions. ❑ Determine effective management oversight and supervision on the need to audit sensitive transactions. ❑ Rotate work duties (cross-training) to deter collusion and theft. ❑ Encourage or require those who conduct audits and handle money to take time off or to complete a job rotation on a regular basis. • If fraud is taking place, their absence may bring to light illegal or improper activities. ❑ Develop and implement a confidential whistleblower policy to protect employees who report other employees or managers who are committing fraud.	❑ Generate random system stops that require supervisory review or authorization for specific transactions to complete. ❑ Allow real-time review of any transaction by a supervisor or manager when desired. ❑ Give supervisors pr managers the ability to "ghost" transactions and covertly watch employees as they process transactions in real time. ❑ Electronically record management approval for exception processing such as overrides. ❑ Use data mining software to analyze transactions to assist with the identification of employee or customer fraud. ❑ Establish a toll-free hotline for fraud reporting for both employees and the general public. ❑ Install covert cameras to observe employees suspected of fraud to capture their activities, including screen shots if possible. ❑ System generate reports on employee transaction totals by transaction type; include transaction times. ❑ Limit transactions each employee can process based on his or her job responsibilities via his or her system authorization or log-on.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Human Resource Management • Employee monitoring and oversight *(continued)*		❑ File criminal charges for violations and publicize actions; fear of being caught instills caution. ❑ Do not allow counter staff to have purses, backpacks, cell phones, and so on at the front counter. ❑ If front counter staff members have access to a telephone while they wait on customers, make every effort to limit phone calls to only those needed to complete the customer's transaction. ❑ Rotate management and change responsibilities to ensure relationships are not forged that could cause managers to "look the other way" for employees with whom they have developed friendships. ❑ Rotate audit staff responsibilities so they cannot get comfortable with the individual or company being audited or look the other way or collude in a criminal activity. ❑ Look at the types of transactions and number of each processed per employee and compare them with other employees and averages; if any given number is higher or lower than normal, further investigation is warranted.	❑ Generate reports for management action when unauthorized transactions are attempted or completed. ❑ Record telephone calls and spot monitor them regularly.
DL/ID Card Transactions • General issuance practices	• Central issuance enhances overall control of DL/ID card products. It reduces the ability of front-line staff to issue documents by bypassing important checks and balances before an identification document is issued. • Photo-first processing and scanning of documents can help combat fraud. Because of the sensitive nature of scanned documents, control measures must be put into place to ensure security of the information.	❑ Issue DL/IDs cards through a central issuance vs. an over-the-counter process. ❑ Develop and implement an audit plan for DL/ID card issuance processes. ❑ Establish a regular schedule to review and update the plan (at least annually). ❑ Establish processes to eliminate or reduce theft of documents and securely destroy surrendered licenses as soon as possible.	❑ Take the photo first to verify the applicant throughout the application process. ❑ Scan or digital image documents presented at the time of application. ❑ Provide a link to scanned images from the electronic record. ❑ Develop or implement an electronic audit log to facilitate audit processes, including the capture of all record changes, who made the changes, and who authorized the changes.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
DL/ID Card Transactions • General issuance practices *(continued)*	• Lax security processes for handling surrendered licenses potentially provides an easy opportunity for theft or loss of genuine documents. • Overrides are an evil necessity in our business. Multiple levels of approval and post-transaction auditing can help reduce wrongdoing.	❑ Review processes that allow override transactions and tighten processes as much as possible. ❑ Require two approvals to complete an override transaction. ❑ Document details of override for record keeping purposes. ❑ Use AAMVA's courtesy verification program before issuance of newly designed cards to ensure cards meet specified standards. ❑ Send DL/IDs annually for CVP analysis to ensure standards continue to be met. ❑ Request changes to security features of credential when vulnerabilities are identified. ❑ Follow AAMVA's card design standards. ❑ Do not allow hats, facial covering, sunglasses, or other clothing or covering that impedes identification of the individual through facial recognition or other type of comparison review.	❑ This may require updating the databases so that information is easily used. ❑ Analyze the potential impact for data storage on system performance. ❑ Electronically record management approval for exception processing such as overrides. ❑ Secondary approvals in small offices may require involvement by a manager in another location.
DL/ID Card Transactions • Validation of identity and eligibility	• We typically think of external (customer) fraud when thinking about DL/ID transactions, but keep in mind that in some cases, there may be collusion with the agency's field office staff. • DL/ID card issuance should be a core competency of the DMV. If at all possible, third parties should not be authorized to issue new DL/IDs. If third parties are authorized, stringent processes should be implemented, and strong oversight should be present. Central office issuance should be required for third-party DL/ID credential issuance. Employees of third parties issuing DL/IDs must be held to the same standards, including background checks, as DMV employees.	❑ Establish and implement a list of acceptable and verifiable documents that a customer must present to establish his or her identity (a multi-level list is preferable). ❑ Establish and implement a two-step approval process for initial DL/ID applications and review of breeder documents. ❑ Require a second-level review and authorization for changes to gender, date of birth, name, and other key data. ❑ Take investigative action as appropriate in suspicious circumstances. ❑ Take personnel, disciplinary, administrative, or criminal actions as appropriate.	❑ Whenever possible, electronically verify data elements required for credential issuance (e.g., SSOLV, VLS, digital image exchange) and require an electronic response before approving issuance. ❑ Use a facial recognition system. ❑ Use document verification and authentication tools. ❑ Use OCR (optical character recognition) scanner or other applicable technology when applicable to read bar-coded documents or those with chips or mag stripes. ❑ Require key data elements from ID documents to be data entered or scanned to the DL/ID record.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
DL/ID Card Transactions • Validation of identity and eligibility *(continued)*			❑ Image or scan documents presented by applicants. ❑ Provide a link to the scanned images from the DL/ID record. ❑ Use address validation software as a tool to validate information provided by the applicant. ❑ Automatically generate reports when a specific address is used multiple times for issuance in the preceding year(s). ❑ Require secondary electronic approval for changes to gender, date of birth, or other key data fields before updates to the record are finalized.
Driver License Transactions • Knowledge testing processes	• Knowledge and skills testing are potential areas in which employees may "assist" customers in achieving passing scores without the applicant having actually passed, or in some cases taken, the exam(s). • In the administration of a knowledge testing program, the potential for fraud exists with the test administrator, as well as the applicant. Mechanisms to detect and deter fraud must be in place for both. • Automated knowledge testing systems provide a proven mechanism to combat fraud. They provide random tests and random test questions to each applicant and prevent cheating by the applicant and manipulation of the test or test results by the examiner. • Test takers may sell written test answers when the same test (no randomization) is given over and over.	❑ Take the photo first and use it throughout the process. ❑ Use a two-step identification process. ❑ Keep track of knowledge test results for each examiner; look for pass/fail rates that are excessively low or high (not applicable if knowledge testing is automated). ❑ Compare pass rates among offices and third parties, looking for anomalies. ❑ Hire field office clerks with foreign language skills (especially in areas where that population resides). ❑ Establish a contract with translation service providers (e.g., companies that provide such services over the phone) vs. allowing applicants to bring translators with them. ❑ If interpreters are allowed, require that they be certified or approved by a trusted entity or require that they complete a specific approval process, including a background check. ❑ Require authorized interpreters to submit proof of identification when providing services.	❑ Take the photo first to verify the applicant throughout the testing and application process. ❑ Randomize test questions each time or use automated knowledge testing that automatically randomizes questions to minimize cheating and results manipulation. ❑ Electronically post knowledge test results to the driving record upon test completion to prevent alteration of test results.. ❑ Place security cameras in the knowledge testing areas of the office and regularly monitor the testing area.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Driver License Transactions • Knowledge testing processes *(continued)*	• Ideally, interpreters or translators should not be allowed because there is no way to determine if they are providing more than interpretation services. If you allow interpreters, make sure they are vetted; do not allow just anyone to provide such services.	❑ Provide knowledge tests in foreign languages to avoid the need for interpreters. ❑ Review processes and identify ways to reduce the need for interpreters. ❑ Establish policies to prohibit conflict of interest between interpreters and DMV staff. ❑ Monitor pass/fail rates and average test duration for approved interpreters. • Tests taken while cheating, particularly when interpreters are involved, can take much less time than a normal test. ❑ Look for trends in specific speaking populations visiting offices. ❑ Do not allow overrides for written knowledge tests. ❑ Prohibit cell phones, headsets, pagers, and other electronic devices, as well as hats by test takers. ❑ At a minimum, road signs testing should be in English. ❑ Use AAMVA's guidelines for knowledge and skills test development. ❑ Review testing processes and look for areas in which internal fraud may occur; make changes as necessary. ❑ Rotate testing responsibilities among employees. ❑ Do not allow employees to process their own DL/ID card transactions.	
Driver License Transactions • Skills testing	• In the administration of a skills testing program, the potential for fraud exists with the test administrator, as well as the applicant. Mechanisms to detect and deter fraud must be in place for both. • Unqualified or unsafe drivers pose a public safety threat. • Applicants allowed to carry a gun while testing could pose a threat to the tester.	❑ Monitor, track, and evaluate pass/fail rates of skills test examiners and investigate pass and fail rates that fall out of the norm ❑ Monitor examiner test times for noncommercial and CDL skills tests; investigate examiners whose test times are shorter than the norm. ❑ Use AAMVA's guidelines for knowledge and skills test development.	❑ Electronically record skills test results on driver record upon completion of the test. ❑ Use electronic skills testing tools such as tablets, in-car video, or GPS to track test routes and times. ❑ Automatically generate system reports for examiners whose pass/fail rates fall outside of the norm.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Driver License Transactions • Skills testing *(continued)*	• Using tables with GPS capabilities provides for the safety of examiners and allows for better oversight of skills tests.	❑ Spot check to ensure that examiners are passing predetermined points on drive test route if GPS is not used.	❑ Flag short testing times and follow up with examiners. ❑ Investigate and take appropriate action. ❑ Use technology such as in-car videos or GPS units to assist with examiner evaluation. ❑ An added benefit is the protection such devices provide for examiner safety, as well as proof of events when accusations are made by the applicant.
CDL Truck Driver Training Schools and Other CDL Third-Party Testers	• Lax processes or oversight in a CDL program may result in unknowledgeable or unsafe driver(s) operating on the nation's highways in an 80,000-lb vehicle, one placarded for hazardous materials, or a bus carrying passengers. Crashes, injury, death, or property damage may result. Illegal transport of drugs, guns, contraband, and stolen materials may occur. • Transportation of hazardous materials for illicit purposes could threaten homeland security (e.g., 9/11 pilots). • Allowing schools to both train and test drivers could result in a potentially biased test. • Requiring an examiner to conduct a specified number of tests per year will ensure their skills and knowledge remains current.	❑ Complete background checks of owners and instructors. ❑ Audit schools and records on a regular basis via records and in the field. ❑ Audit individual examiner records regularly, looking at pass/fail rates. ❑ Conduct covert audits; watch skills tests as they are conducted. ❑ Randomly retest individuals who have completed testing with third-party examiner. ❑ Require third parties to post a bond and sign an MOU that they agree to meet established guidelines. ❑ Require schools to meet established regulations, both initially and ongoing convert/overt audits. ❑ Require training class on rules and regulations for owners and instructors. ❑ Prosecute and publicize fraud cases. ❑ Require a minimum number of CDL tests to be conducted annually by the examiner as a condition of keeping examiner certification.	❑ Require third-party testers to use electronic testing devices with GPS to allow road test routes to be analyzed. ❑ Require automated reporting of skills test results. ❑ Electronically audit examiner records for pass/fail rates.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Driving Schools	• Unknowledgeable or unsafe drivers operating on our nation's highways potentially result in crashes, injuries, death, or property damage. • Schools may teach students to pass the test vs. how to drive safely. • Schools may sell training certificates without requiring sufficient training. • In states where the driving school can conduct the DMV behind-the-wheel driving test, the instructors could conduct an insufficient number of drive tests, causing them to lose their skills and knowledge, resulting in inconsistencies in conducting and scoring drive tests. • Online courses have greater potential of fraud (e.g., another individual takes the course). • Individuals can have points removed from their records or a court order satisfied by not properly completing course requirements.	❑ Establish minimum requirements for schools wishing to become agents of the DMV to offer testing. ❑ Review and audit paperwork regularly. ❑ Require annual certification. ❑ Partner with the Department of Education if it has authority over schools to establish standards and audit criteria. ❑ Complete federal and state background checks of owners and instructor initially and on a regular basis. ❑ Work with driving school associations to share fraud trends, enforcement efforts, and so on. ❑ Require third parties to post a bond and sign an MOU that they agree to meet established guidelines. ❑ Require a minimum number of driving tests to be conducted by the examiner as a condition of keeping drive test certification. ❑ Conduct covert observations on the driving tests to ensure they are conducting them properly and following approved drive test routes. ❑ Take swift action to invalidate school or instructors testing authority for noncompliance or for fraud.	❑ Require third-party testers to use electronic testing devices with GPS to allow road test routes to be analyzed. ❑ Require automated reporting of skills test results. ❑ Electronically audit examiner records for pass/fail rates.
Driver License Transactions • Medical Screening	• Medical conditions of drivers and assessment of their driving abilities are sometimes best left to medical professionals. A medical advisory board can provide much needed guidance, as can a nurse or medically trained person(s) on your staff. • A case tracking system can help ensure that appropriate steps are followed throughout the process. • Failure to properly screen drivers can result in unsafe drivers on public roadways.	❑ Have nurses or other medically trained personnel on staff or under contract to complete case reviews. ❑ Establish and use a medical advisory board when in-house staff are unable to determine appropriate action. ❑ Train employees who have access to medical information regarding Health Insurance Portability and Accountability Act (HIPPA) requirements and require that they sign a statement of understanding.	❑ Scan DOT medical cards and medical forms presented at the time of CDL application and link to driver record. ❑ Use a case tracking system for quality control and assurance. ❑ Limit access to medical records to only those authorized to review and view the record(s). ❑ Require electronic reporting from licensing entity to ensure physicians are properly credentialed.

(*continued*)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Driver License Transactions • Medical Screening *(continued)*			❑ Require electronic reporting from physicians for all medical reporting (CDL and non-CDL). ❑ Validate reporting entity and license number with appropriate jurisdictional medical agency to ensure they are who they claim to be.
DL/ID Card Transactions • Duplicates, Replacements and Corrections	• The definition of duplicate, replacement, and corrected licenses varies from jurisdiction to jurisdiction. The Working Group recommends that duplicate be defined as an exact replacement of the previously issued document. If any information is changed (e.g., address, photo or image), the document should not be considered a duplicate. • Application requirements for issuance of duplicates, replacements, and corrections should be clearly defined. • Any process that deviates from established procedures (e.g., no-fee transactions) should require secondary level approval. • The DL record can provide a history of activity in regard to license issuance by tracking details on exceptions processing, including the date of the transaction, the individual who initiated or approved the transaction, and other critical information.	❑ When identity documents are not scanned, an audit after the fact will not be able to verify that controls were followed. • A supervisor or auditor needs to observe such processes to verify that established procedures were followed. ❑ Require proof of identification for duplicate DL/ID applications. ❑ Do not change information (e.g., photo, expiration date) on duplicate DLs/IDs; a duplicate should be defined as an exact replacement of the previously issued document. ❑ Limit the number of duplicates allowed and the timeframe in which they are issued. ❑ Implement processes to flag instances of multiple duplicate DL/IDs and review transactions before issuance. ❑ Establish business rules and differentiate requirements between the issuance of a duplicate, replacement, and corrected document. ❑ For over-the-counter issuance, centrally issue duplicates, corrected licenses, and replacements, facilitating additional review of the application and record. ❑ Review processes for no-fee transactions; make adjustments as necessary to ensure security. ❑ Require supervisor or manager review of overrides, no-fee transactions, and any other transaction outside the norm.	❑ Develop and implement an electronic audit log that includes details on changes made to the driver record, who made the changes, and who authorized the changes. ❑ Capture a digital image of the applicant and verify the photo on file through facial recognition or, when appropriate, digital image exchange. ❑ For duplicate documents, systematically prohibit information, including the photo, to be changed. • A duplicate should be defined as an "exact" replica of the previously issued document. ❑ Capture a new photo and customer signature for the record with the issuance of duplicate replacement and corrected product. ❑ Generate reports that identify customers with more than a predetermined number of duplicate, replacement, or correction issuances; require review and approval before document issuance. ❑ Generate reports of no-fee transactions by user. ❑ Keep records on number of no-fee transactions and investigate or take action on anyone above the norm. ❑ Electronically track no-fee and reduced fee transactions by user ID; flag excessive number of approvals for further investigation.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Driver License / ID Card Transactions • Undercover Driver Licenses	• Undercover or confidential DL/ID cards and records must be very tightly controlled and protected to ensure the safety of the officer or agent. • Background checks can provide needed insight for employees who process undercover licenses.	❑ Limit staff who process transactions for undercover or confidential DLs/IDs to staff who have undergone comprehensive background checks and scrutiny. ❑ Require central office or limited location(s) issuance for processing of confidential or undercover DLs/IDs.	❑ Allow "true identity information" access for confidential or undercover record systems or information by authorized personnel only. ❑ Driver record for confidential or undercover DL/ID holders should appear as any other individual's record. ❑ Track access to driver records for confidential or undercover holders and generate a flag or notice when the record is accessed.
DL/ID Card Transactions • Valid Without Photo	• The issuance of valid without photo DL/ID cards is not recommended. It is impossible to verify the identity of the card holder without the photo.	❑ Limit the circumstances under which VWPs can be issued.	
Card Transactions • Fee waivers	• Transactions for which a fee is waived or reduced present a serious vulnerability for the agency. Staff can potentially mark the records as fee waived while actually pocketing any fees collected. • Secondary approval—ideally, electronically—should always be required for no-fee or reduced fee transactions. A narrative of the reason for the fee waiver, as well as an approving supervisor or manager signature, should always be captured.	❑ Develop written procedures outlining the circumstances in which a fee can be waived or reduced. • Require management approval for fee waivers and overrides. ❑ Require a written narrative to be included with the transaction outlining the reason for the no-fee or reduced fee transaction. ❑ Require primary, and in some cases, if warranted, a secondary supervisor or manager approval for all no-fee or reduced fee transactions. ❑ Regularly audit no-fee and reduced fee transactions; tighten procedures as warranted.	❑ Create an audit log that includes the capture of additions and changes to driver records, who made the changes, who approved the changes, and details of the changes made. ❑ Image or scan the exception or approval or capture the narrative electronically whenever a fee is waived or reduced. ❑ Require primary and, if applicable, secondary approval to be entered into the system electronically before the transaction finalizes. ❑ Electronically track no-fee and reduced fee transactions by user ID; flag excessive number of approvals for further investigation.

(*continued*)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Driver Control • Driver record entries *(suspensions, revocations, stops, disqualifications, cancellations, convictions, reinstatements, and clearances)*	• Because of the importance of the DL, individuals may try to influence staff to inappropriately remove entries from their driving record or to add satisfaction of reinstatement requirements. Establish procedures and use technology to control and monitor the work of staff members who have the authority to make changes to the record. • Receipt of electronic information should be directly posted to the record (e.g., electronic reporting from courts should result in a conviction being automatically added to the record, and if warranted, a suspension notice should automatically generate).	❑ Authorize only certain individuals to have the ability to remove entries from, or add reinstatement requirements to, a driver record ❑ Require supervisor or management approval for certain types of transactions.	❑ Require electronic reporting when possible (e.g., conviction reporting from courts, insurance verification from insurance companies, imposition of suspensions or reinstatements). ❑ Create an audit log that includes the capture of additions or changes to the driver record, who made the changes, and details of the changes, made ❑ Track changes and updates to the record by user ID to look for an unusually high number of transactions or high frequency of record changes. ❑ Image or scan requirements provided for reinstatement; facilitate access to scanned images from driver records. ❑ Electronically allow reinstatement notices to generate only when all required documentation or proof has been entered into the record.
Defensive Driving Schools	• Driver training schools are potentially biased if they are allowed to both train and test drivers.	❑ Certify defensive driving schools initially and recertify them annually. ❑ Audit defensive driving schools annually. ❑ Spot monitor or review testers regularly. ❑ Complete federal and state background check for owners and instructors. ❑ Require final tests to be completed in person (vs. online). ❑ Work with driving school associations to share fraud trends, enforcement efforts, and so on.	❑ Require online programs to continually request personal information that only the driver would know. ❑ Implement a secure certificate issuance or tracking process. ❑ Require electronic reporting of course completion and required financial information.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Ignition Interlock Providers	• Failure by drivers to comply with IID requirements poses highway safety issues. • The potential to falsify data or installation is a challenge if oversight is lacking. ***NOTE:*** *AAMVA's Ignition Interlock Best Practices will be published by August 2015. AAMVA recommends that defined best practices be followed.*	❑ DMVs should have legislative or regulatory authority to provide oversight of IID providers. ❑ Establish an onsite audit program. ❑ Take swift action for violations. ❑ Establish program to test devices to ensure they are properly functioning; staff expertise is required. ❑ Solicit feedback from IID users on device issues and vendor performance.	❑ Require electronic submission of data from IID providers on a regular basis. ❑ Camera-equipped IIDs are recommended to prevent nondrivers from blowing into the device.
Titling and Registration Transactions • Title issuanced	• Eliminating paper titles through implementation of an electronic lien and title program is a best practice. It is also a cost-saving measure. • Title issuance from a central location provides for security of title issuance, as well as controlled inventory of title stock. • Follow established guidelines to use NMVTIS for real-time, fully integrated inquiries and updates.	❑ Issue titles from a central location (vs. in the field). ❑ Use title stock and registration stickers that contain security features to prevent fraud and counterfeiting. ❑ Assign unique inventory control numbers to title stock and registration documents and stickers and maintain the issuance information in an electronic database. ❑ Implement and follow strict inventory control procedures. ❑ Require vehicle transaction applicants to provide proof of identification. ❑ Do not allow employees to process their own title transactions or those of family members.	❑ Implement an electronic lien and title program. ❑ Scan or image documents presented at the time of application and link to the vehicle record. ❑ Develop an electronic inventory tracking system that is linked to the titling and registration record. ❑ Use Vehicle Identification Number (VIN) verification software to validate VINs. ❑ Require VIN verification or NMVTIS checks before a title is issued. ❑ Generate a report or flag for supervisor or manager investigation when a minimum tax is charged on a high-value vehicle. ❑ Scan or image identity documents provided at the time of application and link to the vehicle or title record.
Titling and Registration Transactions • Lien perfections • Lien releases	• Implementation of an electronic lien and title (ELT) program will reduce the possibility of fraud by requiring financial institutions to report information electronically. However, even with an ELT program, paper lien releases will sometimes be received. In those cases, a secondary review should be required before the lien is released.	❑ Develop specific processes or policies for manual lien releases with a goal of making the process as secure as possible. ❑ Require applicants providing manual lien release information to prove their identity. ❑ Paper titles should be issued to the lienholder. ❑ Require return of the title if a second lien is placed on the vehicle; then return the title to the original lienholder.	❑ Implement an ELT program. ❑ If not implementing a full ELT program, require electronic lien release directly from the lienholder to release the title. ❑ If an electronic release is not received, require supervisor or manager review for lien release authorization; electronic authorization should be required before transaction can continue.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Titling and Registration Transactions • Lien perfections • Lien releases		❑ Follow AAMVA's ELT Best Practices. ❑ Do not allow employees to process their own lien-related transactions or those of family members.	❑ If using a manual lien or title program, image or scan the lien or title documents provided and capture key information electronically (e.g., the bank and loan number); require such key fields to be entered before the transaction is completed. ❑ Require the system to document verification of the applicant's identification. ❑ Check NMVTIS before releasing the lien. ❑ Scan or image identity documents provided at the time of application and link to the vehicle or title record.
Titling and Registration Transactions • Branded titles	• Carrying brand information from out-of-state titles will help prevent title washing. If a brand from another jurisdiction that does not exist in your jurisdiction is titled in your state, the other state's brand should be carried forward. • Retaining scanned copies of the previous title and running electronic verification checks will help ensure employees followed the correct steps in issuing titles. • Centrally reviewing brand-related transactions before issuance and mailing alleviates title washing by allowing a review and confirmation or approval of the transaction. • Using the NMVTIS can prevent the issuance of a clear title for one that should have been issued branded.	❑ Capture and retain brand information for out-of-state titles. ❑ Issue branded titles and brand removal titles centrally. ❑ Centrally review brand-related transactions before issuance or mailing to confirm or approve the transaction.	❑ Modify the title record to retain brand information from out-of-state titles. ❑ Scan or image out-of-state titles received and provide electronic retrieval capabilities to the "old" title. ❑ Complete an electronic check of branded vehicles or requests for brand removals against stolen vehicle and other electronic databases, such as NMVTIS. ❑ The end-of-day audit process should include electronic checks for key information. ❑ Critical information that cannot be verified electronically should be checked manually. ❑ Scan or image identity documents provided at the time of application and link to the vehicle or title record.

(*continued*)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Titling and Registration Transactions • Duplicates • Corrections • Replacements	• To prevent fraud, the same processes should not be followed for duplicate, corrected, and replacement titles, so proper processes should be determined for each (e.g., if issuing over the counter, consider whether duplicates should be issued centrally, with additional reviews or approvals required). • As with duplicate DL/ID cards, the definition of a duplicate title should be a replica of a previously issued document. The only information that should change is the title number, issue date, and control number. Changes to other information mean that the title is no longer a duplicate. • When replacement, duplicate, or corrected titles are issued, the previously issued title should be nullified. • Any titles containing a lien should be issued to the lienholder. • Require involvement from the primary lienholder any time additional liens are added to the title.	❑ Establish business rules and differentiate requirements for the issuance of duplicate, corrected, and replacement titles. ❑ Require applicants to prove their identity for duplicate, corrected, or replacement titles, especially if the title is being issued over the counter. ❑ Limit the number of duplicate or replacement titles allowed within a specified timeframe. ❑ If titles are sent to the owner, vs. the lienholder, put processes in place to include or notify the lienholder of any duplicate title requests. ❑ Define a duplicate title as an exact replica of the original document, with changes allowed to title specific information only (title number, control number, issue date). ❑ If information needs to be changed, a new title should be issued, and issuance of the new title should void the previously issued title.	❑ Develop and implement an electronic audit log that includes the capture of all transactions and changes, who made the changes, and who authorized the changes. ❑ For over-the counter transactions, require the system to document the fact that the applicant's ID was verified. ❑ Electronically prevent information from being changed on a duplicate title. ❑ Scan or image identity documents provided at the time of application and link to the vehicle or title record.
Titling and Initial Registration Transactions • Transfer of ownership transactions	• Central issuance of title transactions containing ownership transfers allows independent verification of the transaction before a title is issued.	❑ For over-the-counter title issuance jurisdictions, centrally issue titles with ownership transfers. ❑ Complete audit of transfer of ownership paperwork before issuance. ❑ If full auditing not possible, complete a random audit of such transactions. ❑ Require applicants to provide proof of ID for all ownership transactions. ❑ Do not allow employees to process their own vehicle transactions or those of family members.	❑ Create an electronic audit log to capture all transactions and changes to the record, including who made the changes and any resulting credential issued. ❑ Require the system to document verification of the applicant's identity for all transactions. ❑ Consider tying vehicle owner information to the individual's DL/ID record. ❑ Scan or image identity documents provided at the time of application and link to the vehicle or title record.

(*continued*)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Titling and Initial Registration Transactions • Registration renewals	• Using tamperproof stock that contains control numbers, in conjunction with an inventory tracking system, will greatly reduce the possibility of theft. • For registration renewals processed via the mail, phone, or Internet, make sure controls safeguard both the fees and the indicia.	❑ Use registration decals that contain security features to prevent fraud and counterfeiting. ❑ Print a unique number, such as the plate number, on the registration decal. ❑ Do not allow employees to process a registration renewal for their own vehicles, or those of family members.	❑ The system should prevent use of duplicate control numbers.
Titling and Initial Registration Transactions • "Flag" removals • Reinstate-ments	• A secondary level review greatly reduces the possibility of foul play. • Processing of flag removals or reinstatements from a central location provides for greater oversight. • The fewer people who have the ability to complete flag removals or reinstatements, the better. • Implement a secondary approval process for flag removals or reinstatements when appropriate.	❑ Require flag removals reinstatements to be processed centrally. ❑ Limit and identify the type of flag removals and reinstatements that can be processed in the field if not all reinstatements are required to be processed centrally. ❑ Require second-level supervisory or management review and authorization of flag removal and reinstatement transactions.	❑ Electronically transfer data from local jurisdictions to update registration record in real time. ❑ Allow only specified user IDs to complete flag removals or reinstatement transactions. ❑ Create an audit log that includes the capture of additions and changes to the vehicle record, who made the changes, and details (including the date and time of the transaction) of the changes made. ❑ Image or scan requirements provided for flag removal or reinstatement; facilitate access to the scanned image from the vehicle record. ❑ Electronically require reinstatements to generate only when all required documentation or proof has been entered onto the record. ❑ Require secondary approval to be to be entered electronically.
Miscellaneous Vehicle Transactions • Handicap	• Most processes regarding handicap placards make them subject to theft and abuse. Handicap placard fraud can be reduced by tightening issuance processes and spot monitoring the validity of medical reports. • Issuing only one placard per individual will reduce misuse.	❑ Print unique tracking number on placards and implement inventory control processes. ❑ Require applicants to provide proof of identity at the time of application. ❑ Require medical documentation before issuance of handicap placards.	❑ Develop and implement an audit log that includes the capture of all transactions, changes made, who made the changes, and who authorized the changes. ❑ Image or scan application documents presented; link the image to the record.

(*continued*)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Miscellaneous Vehicle Transactions • Handicap *(continued)*	• Placards should be returned and cancelled when no longer needed or when the individual dies. • Be sure established HIPPA guidelines are followed whenever dealing with medical information.	❑ Spot monitor the validity of medical reports via phone calls to physician's offices. ❑ A better option is to require electronic reporting from the physician. ❑ Reconcile and destroy returned placards. ❑ Issue placards for a specified period vs. an indefinite period of time.	❑ Require the system to document verification of the applicant's identity. ❑ Run a comparison match with a vital statistics agency and identify deceased placard holders; issue a letter requesting return of the placard.
Miscellaneous Vehicle Transactions • Temporary tags • Permits	• Using stock that is tamperproof or contains security features, as well as inventory control numbers will greatly reduce the possibility of theft. • Establishing short-term expiration dates and limiting the number of credentials issued will reap multiple benefits. • Using a print-on-demand system will reduce fraud and theft issues.	❑ Record expiration date on the face of the document. ❑ Assign unique tracking number for all indicia and develop and implement an inventory control system. ❑ Use temporary tags that are tamper resistant and contain security features to prevent alteration of critical information. ❑ Limit the validity period of temporary tags (e.g., 15 or 30 days). ❑ Limit the number of temporary tag issuances and the timeframe in which they are issued. ❑ Include the vehicle description on the temporary tag or permit.	❑ Develop and implement an audit log that includes the capture of all transactions, changes made, who made the changes, and who authorized the changes. ❑ Image or scan application documents presented and link them to the record. ❑ Implement an ELT program to facilitate electronic reporting from dealers and other third parties. ❑ Record issuance of temporary tags on the vehicle record. ❑ Generate reports of employees who issue more than the average number of temporary tags and investigate. ❑ The system should prevent issuance of more than the permitted number of permits to a given vehicle. • The system should issue one permit for any single vehicle, which is valid for a limited period of time. ❑ Maintain real-time registration information and provide access to law enforcement immediately upon issuance.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Dealers, Banks, Financial Institutions, Notaries, and Armored Car Companies	• An unwarranted increase in vehicle value can occur through title washing or odometer fraud. • Vehicle cloning and theft are potential threats. • Title and registration records tied to incorrect individual could be used in criminal endeavors. • Financial gain can be achieved by those who do not follow proper processes. • Indicia theft can occur when proper inventory control procedures are not put into place. • Legitimate documents issued under fraudulent circumstances can be used to perpetuate a multitude of crimes. • Loss of revenue can occur through theft of deposits for field and central office operations. • Requiring third parties to scan and electronically transfer paperwork on a daily basis will allow the DMV to have access to imaged documents sooner and will alleviate the DMV from having to scan the paperwork upon receipt.	❑ Establish MOUs/SLAs and renew them regularly. ❑ Require annual recertification of dealer licenses. ❑ Require license dealers to meet established guidelines. ❑ Require dealers to post bond. ❑ Establish fees that dealers can charge for providing DMV services. ❑ Require dealers to provide history reports of used cars to customers. ❑ Require dealers to provide paperwork to the DMV within a specified timeframe. • In the interim, require the transaction to be reported electronically (electronic temporary tag or pending transaction). ❑ Require criminal and financial background checks of dealers and salespersons. ❑ Require power of attorney to be secured; documents should be numbered and issued by the state. ❑ Audit process with floor planners to verify vehicle inventory. ❑ Use or mandate ELT. ❑ Revoke participation in the program for violations. ❑ Require electronic tracking and issuance of temporary tags. ❑ Require dealers to notify the DMV of lost or stolen indicia within a specified period of time. ❑ Require secure storage and tracking of indicia. ❑ The DMV must have ability to cancel, revoke, or suspend a dealer's license when warranted. ❑ Require background and financial check of owners and salespeople.	❑ Implement an electronic lien and title program. ❑ Require electronic issuance and reporting of plate and indicia inventory; provide direct connection to the DMV system for fees, etc. ❑ Require electronic tracking of temporary tag issuance. ❑ Require dealers to scan paperwork and forward copies to the DMV on a daily basis. ❑ Track receipt of follow-up paperwork and generate a report when a dealer fails to send paperwork.

(*continued*)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Dealers, Banks, Financial Institutions, Notaries, and Armored Car Companies *(continued)*		❑ License salespeople initially and annually. ❑ Train dealers, banks, and lenders on how to verify ID; recommend they use AAMVA's FDR program. ❑ Audit regularly via paperwork and in-person field audits. ❑ Require NMVTIS checks for used cars. ❑ Require owner(s) to complete training on rules and regulations and require refresher training as warranted. ❑ Require title clerks and financial managers to complete title and registration requirements training. ❑ Enlist local law enforcement help for curbstoning and other issues. ❑ Communicate with locals (e.g., law enforcement and zoning organizations). ❑ Build relationships with dealer associations; they can be strong political allies. ❑ Require banks, floor planners, and dealers to share info on liens. ❑ Require any potential data breaches to be immediately reported.	
Junk and Salvage Yards, Dismantlers, Rebuilders, and Itinerate Vehicle Collectors	• An unwarranted increase in vehicle value could occur through title washing or odometer fraud. • Vehicle cloning and theft are potential challenges. • Title and registration records may be tied to an incorrect individual. • Those who buy unsafe or improperly titled or inspected vehicles may incur a financial loss. • Unsafe vehicles may be placed on the roadways if proper processes are not followed. ***NOTE:*** *Jurisdictions are urged to refer to and implement AAMVA's Best Practice for Title and Registration of Rebuilt and Specially Constructed Vehicles.*	❑ State licensure requirements should include mandate to participate in NMVTIS. ❑ Establish and implement DPPA agreements. ❑ Audit regularly, including audits to ensure vehicles are properly sent to NMVTIS. ❑ Report audit discrepancies and concerns to the DOJ. ❑ Establish regulations for dismantlers, recyclers, and truck towers for the appropriate agency to regulate. ❑ Require proof of ownership to dispose of vehicles. ❑ Require notice of disposal to the DMV and NMVTIS. ❑ Require entity to obtain certificate of ownership at the time of purchase.	❑ Require facilities to participate in NMVTIS.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Junk and Salvage Yards, Dismantlers, Rebuilders, and Itinerate Vehicle Collectors *(continued)*		❑ Require junk and salvage, dismantlers, rebuilders, crushers, and other applicable entities to be licensed with NMVTIS. ❑ Require background checks on owners and employees of junk, salvage, dismantlers, crushers, and other applicable entities , initially and on a regular basis. ❑ Require any potential data breaches to be immediately reported to the DMV.	
Auto Auctions and Insurance Auctions	• Improper practices may lead to an unwarranted increase in vehicle value through title washing, odometer fraud, or vehicle cloning or theft. • Those who buy unsafe or improperly titled or inspected vehicles may incur a financial loss. • Unsafe vehicles may be placed on the roadways if proper processes are not followed.	❑ Require auctions to obtain vehicle ownership paperwork from the seller. ❑ Establish and implement DPPA agreements. ❑ Carry branding information from the previous jurisdiction(s). ❑ Implement policies and procedures for exporting of vehicles. ❑ Conduct regular audits. ❑ Report audit discrepancies and concerns to the DOJ.	❑ Licensure requirements should include mandate to participate in NMVTIS, if applicable. ❑ Require auctions to scan and maintain digital copies of ownership documents.
Emissions/ Safety Inspection Stations	• Failure to follow proper processes may result in unsafe vehicles on the roads • Financial gain may be achieved by those who seek to avoid requirements. • Improper testing could have a negative impact on the environment. • Federal penalties exist for exceeding emissions measurements.	❑ Complete covert inspections /and implement a secret shopper program. ❑ Monitor OVD computers to identify clean scans. ❑ Require electronic reporting of results. ❑ Electronically verify inspection results at the time of registration. ❑ Audit regularly and as needed on a volume basis. ❑ Ensure secure control of indicia. ❑ Shut down station when violations occur (e.g., discontinue providing new stickers). ❑ Require certification and licensing by the appropriate agency (at least biannually). ❑ Define requirements for initial certification and licensing, both initially and upon renewal.	❑ Electronically compare the VIN on the vehicle's computer with the VIN on the registration to identify stolen vehicles. ❑ Electronically report inspection results. ❑ Require reporting and tracking of vehicle miles.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Emissions/ Safety Inspection Stations *(continued)*		❑ Prosecute and publicize fraud findings. ❑ Require any potential data breaches to be immediately reported to the DMV.	
Insurance Agencies	• Uninsured drivers on the roads. • DPPA violations could occur through improper release of records or data. • Backdating of insurance coverage may occur.	❑ Validate current licensing with insurance regulators in the state in real time, at the time of registration, if electronic reporting of insurance is not required. ❑ Require in a signed agreement that the agent will follow DPPA.	❑ Require electronic reporting of insurance information. ❑ Audit electronic inquiries.
Record Buyers and Providers and Entities That Have Access to DMV Records	• Unauthorized access to personal data • Financial gain • Unauthorized release of personal information • Confidentiality of data • Ownership of data • DPPA violations • Data breach	❑ Establish secure record access procedures and policies. ❑ Establish and implement reciprocal working agreements with other state and federal agencies. ❑ Work with law enforcement for warrant enforcement. ❑ Require posting of bond. ❑ Require background checks on individuals accessing DMV records. ❑ Include performance and security metrics as part of contracts; invoke penalties for noncompliance. ❑ Complete a compliance check by inserting fictitious records into record requests to check for misuse of DPPA protected data (sometimes referred to as "salting" records). ❑ Require inquirers to take IT security training annually. ❑ Require secure disposal of sensitive documents. ❑ Establish and implement DPPA agreements and require annual recertification. ❑ Establish record access procedures and policies via MOU or SLA. ❑ Require purchasers to immediately notify the agency of any data breaches related to DMV records.	❑ Mask data as appropriate based on authorizations or access needed. ❑ Require password protection processes identical to agency employee processes. ❑ Complete IT system audits (e.g., number of inquiries, time of data inquiries). ❑ Mask data as appropriate based on authorizations and access needed.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Record Retention and Disposal	• Record control is a critical aspect of document security. Employees must understand the sensitive nature of records and how to handle them appropriately.	❑ Develop and implement a document and record retention schedule. ❑ Establish mandatory penalties and sanctions for unlawful disposal of documents or records. ❑ Enforce penalties for all violations; publicize violators and repercussions. ❑ Require employees to sign, both initially and annually, a confidentiality agreement that includes a statement of understanding on proper uses of the system and records.	❑ Work with a vital records agency to facilitate a purge of deceased record holders on a regular basis. ❑ Generate a report if action is taken on a record marked deceased. ❑ Investigate and take appropriate action.
Indicia Providers	• Failure to control inventory and information could release confidential information. • Theft or loss of indicia could take place if proper inventory control processes are not in place.	❑ Establish and implement DPPA agreements. ❑ Establish record access procedures and policies. ❑ Complete regular auditing. ❑ Require background checks on employees. ❑ Include performance and security metrics as part of contract and include penalties for noncompliance. ❑ Require secure disposal of sensitive documents. ❑ Establish controls for transportation of secure indicia. ❑ Institute security protocols for mailing of documents to customer. ❑ Require providers and entities to advise the DMV immediately of data breaches. ❑ Establish and include in the MOU penalties for lost inventory, including payment of penalties. ❑ Require notification of theft or loss of indicia immediately.	❑ Complete an electronic comparison of documents requested vs. documents produced. ❑ Implement inventory controls for card stock and other indicia. ❑ Require purge of data after specified period of time (data retention policy).

(*continued*)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Information Technology • Internal control practices • IT management • Security protocols	• Implementing secure and authorized access to systems will ensure not only that unauthorized personnel do not access the system but will also provide tracking for any changes initiated. • Authorizing users to make changes to records based on their job responsibilities will ensure non-authorized individuals do not alter records incorrectly or fraudulently. • For jurisdictions with centralized IT, employee compliance requirements should be the same.	❑ Initiate biometric identifiers for system access. ❑ In lieu of a biometric identifier, initiate password protections, swipecard, or other electronic log-in requirement. ❑ Define authority access levels (i.e., do not give everyone access to the entire system). ❑ Define criteria for password content. ❑ Develop a written policy to prohibit staff from sharing password(s). ❑ Take action for policy violators. ❑ Eliminate biometric and password access for employees immediately upon termination, resignation, or in cases of administrative leave. ❑ Follow up to ensure authorities have actually been deleted, removed, and invalidated after departure. ❑ Review and make changes to accesses and authorizations when employees change jobs. ❑ Train employees on acceptable record and system access. ❑ Require employees to sign an agreement of understanding regarding allowable access, prohibited uses, and confidentiality requirements. ❑ Establish mandatory penalties and sanctions for employees who unlawfully access records. ❑ Aggressively enforce policies and take timely disciplinary action. ❑ Publicize arrests and convictions. ❑ Establish procedures and chain of custody processes for removing secure information to an offsite location to only authorized personnel (e.g., investigators, auditors, and legal staff).	❑ Use a biometric identifier for system access at every workstation. ❑ Assign system access levels or authorizations based on job responsibilities. ❑ Record and log the important events in the business cycle that are performed by systems. ❑ Track identification of employees who process transactions. ❑ Log browsing of records activity by system users. ❑ Review logs on a random basis to ensure compliance with policies. ❑ Encrypt information as appropriate. ❑ Record overrides or unusual activity in a way that it can be easily tracked or discovered later (e.g., via an audit log). ❑ Require the system to prompt changing of passwords on a regular basis (at least every 45 days). ❑ Implement computer forensic technologies. ❑ Use automated reporting capabilities. ❑ Track any and all transactions. ❑ Use automated queuing. ❑ Record query vs. transaction process. ❑ Develop and implement comprehensive ad hoc reporting capabilities.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Information Technology • Internal control practices • IT management • Security protocols *(continued)*		❑ Take disciplinary action for violations. ❑ Do not allow nonapproved staff to take secure or prohibited information offsite. ❑ Limit system access to "view only" for those not authorized to make changes to the record as part of their job duties. ❑ Update system access requirements as duties for positions change. ❑ Eliminate system access for third parties and independent contractors immediately upon termination of agreements or contracts. ❑ Follow up to verify that system access for third parties and independent contractors has actually been revoked.	❑ Generate alert when "flagged" records (e.g., confidential or undercover records, witness protection records, VIPs) are accessed. ❑ Investigate access to "flagged" records (e.g., confidential or undercover records, witness protection records, VIPs) to determine if access was in fact for business purposes. ❑ Reduce the number of machines that have drives that can be used to write data to removable by disabling drives. ❑ Limit the ability to install new hardware such as zip drives and portable drives to system administrators. ❑ Require a business purpose and manager approval before a given piece of software or hardware is installed at a given workstation. ❑ Track changes to records that are completed outside of the normal transaction processes. ❑ Reports should be generated and investigated whenever nonstandard changes are made. ❑ Use data mining software to sift through customer records and transactions to flag suspicious activity. ❑ Investigate unusual activity. ❑ Make process changes as warranted. ❑ Take appropriate disciplinary action. ❑ Sanitize media when no longer needed or before disposal, as appropriate. ❑ Ensure sensitive data being transferred or shared use a secure method.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Information Technology • Internal control practices • IT management • Security protocols *(continued)*			❑ Access management procedures should provide for periodic review of user access rights. ❑ Back up data and logs, as appropriate. ❑ Mask personal data that an employee does not need to see to do his or her job (e.g., SSNs, credit card information, "a number" for SAVE verification,). ❑ Implement system controls to continuously monitor hacking.
Financial Oversight and Control • Bank deposits	• Ensure bank deposits from the central office, field, offices, and third parties are securely and timely transferred to a financial institution. • Drop safes placed in areas that collect money can provide additional security. Checks are immediately scanned, and funds are withdrawn from the individual's account. Cash is immediately counted, validated, and deposited into the agency's account. • Do not keep deposits in a safe overnight.	❑ Use drop safes in areas or offices that collect money. ❑ Use an armored car service or other secure service to transport funds from the office to the bank. ❑ Set up a process to review bank deposits vs. field office records daily. ❑ Take investigative action for any shortages and overages. ❑ Request financial institutions to notify the central office when anticipated field office deposits are not made; ideally, notification is sent electronically. ❑ Take immediate investigatory or corrective action.	❑ Set up electronic access for authorized central office accounting and audit personnel to the bank(s) where deposits are made. ❑ Set up a system to receive alerts for any overages and shortages. ❑ Investigate and take appropriate action.
Financial Oversight and Control • Refunds • Reconciliation and reporting	• Tight control and oversight of financial transactions is crucial. As the economy weakens and employees deal with personal financial crises, internal theft of checks and cash will increase. No-fee transactions may also increase unless secondary approval is required. • Accepting only electronic payments will reduce overages and shortages and time spent reconciling reports. Budget impacts need to be considered when only accepting electronic payments (increase in merchant fees and the funding of these fees).	❑ Do not provide cash refunds if at all possible. ❑ Establish escalated disciplinary response to cashier shortages and overages. ❑ Require end-of-day supervisor review of no-fee and reduced fee transactions. ❑ Complete a daily review of financial reconciliation reports by clerks. ❑ Make secure daily deposits to a financial institution.	❑ Program all fees into the system to disallow fee changes except in override situations. ❑ Establish an electronic paper trail that justifies all refunds. ❑ Install cameras in field offices, particularly in all areas in which money and checks are collected and counted. ❑ Watch the screens and footage on a regular or random basis.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Financial Oversight and Control • Refunds • Reconciliation and reporting	• Ensure the refund process contains sufficient checks and balances. Avoid issuing cash refunds and discourage the public from paying for transactions via cash. Cash refunds at point of sale should be avoided; otherwise, cash refunds should be handled the same as any other refund. • If cash refunds are given, limit them to refunds under a specified dollar amount. • Monitoring cashier shortages and overages on an ongoing basis will provide insight as to potential weaknesses. • Ad hoc reporting programs can provide an effective tool in monitoring financials. • Weigh the pros and cons of providing refunds in the field. Issue only those that have a business need from the field. All others should be processed from the central office. • Implement secondary approval and review for refund issuance. • Cash refunds provide temptation and are an easy target for those intent on committing theft. • Processes for refund issuance and no-fee transactions should be well documented and strictly enforced. • Establish cash handling procedures that define all methods of payment receipt, how refunds are handled, and provide overage and shortage guidelines. • Require all cashiers to have their own cash drawers. Sharing of cash drawers reduces accountability. • Establish timelines for refund issuance (e.g., waiting 30 days to verify check clearance and receipt of credit card funds). • Establish an internal audit function that verifies that all established procedures are followed.	❑ Provide automatically generated receipts to the customer to allow the customer to verify that the amount collected matches the receipt. ❑ Advise customers via signage to speak to a manager or to call the hotline if they do not receive a receipt. ❑ Require supervisor or manager approval for all refunds issued in the field. ❑ Implement processes that prevent the person who handled the initial transaction to also process the refund. ❑ Perform random cash counts of cashiers during the day. ❑ Require managers to verify cash drawer balance and deposits on an ongoing basis. ❑ Add cash handling to performance plans for cashiers, establishing what is acceptable. ❑ Set specific criteria for overages and shortages, including timeframes and consequences. ❑ Require dual counting of the safe funds and deposits on a daily basis; include a documentation requirement. ❑ Require that receipt of cashier deposits are documented (e.g., sign-in sheet verifying receipt by manager and cashier).	❑ Require supervisory or manager electronic override for transactions requiring alteration of fees. ❑ Automatically generate a report showing refund amounts by employee, especially when the amounts exceed the norm for that position. ❑ Automatically generate a report when more than one refund has been issued to a given customer in a specified timeframe. ❑ Fees paid should be linked to a given transaction and vehicle, and system checks should be in place to ensure that a customer is not refunded more than was actually paid. ❑ Implement an electronic check fund verification program to allow immediate validation of check. ❑ Automatically generate a report that provides information on total dealer refunds. ❑ Excess refunds may indicate too much inventory or training issues regarding the proper calculation of fees. ❑ Integrate point-of-service transaction processing in system (detailed reporting by clerks). ❑ Automatically generate end-of-day financial reports. ❑ Require daily review by an auditor or supervisor. ❑ Send system alerts to an auditor or internal affairs for excessive overages or shortages or adjusting entries.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Financial Oversight and Control • Refunds • Reconciliation and reporting *(continued)*			❑ Develop system reports that track the number of no-fee and reduced fee transactions by employee or approving manager and location. ❑ Track information to look for patterns on overages and shortages; updates should automatically post to appropriate systems or records. ❑ If manual entry required, accuracy of entries should be regularly reviewed. ❑ The system should generate a detailed customer receipt for all transactions. ❑ Prevent the refund unit from making changes to records; they should only process refunds. ❑ Implement comprehensive ad hoc reporting capabilities.
Audits • Audit unit • Audit processes	• Most agencies have internal audit units and audit processes already in place. In addition to simply reviewing paperwork and transactions, such individuals or entities can contribute to the identification of processes that lend themselves to fraud. Auditor training should include proper steps to take when fraud or theft is suspected or identified. • Thorough documentation will help in the disciplining, dismissing, or prosecution of staff. • Auditors' responsibilities should be rotated on a regular basis to ensure they do not become lax or subject to coercion or fraud through relationship building.	❑ Establish an internal audit unit to look for internal fraud. ❑ If already established, determine whether the size of the unit is sufficient to handle the volume of work required. ❑ Seek funding to increase the size of the unit if an increase is warranted. ❑ Develop specific plan for conducting regular audits. ❑ Include resource allocation. ❑ Focus on areas of greatest risk. ❑ Implement and create a regular review schedule for audit procedures (at least annually). ❑ Processes must change as fraudsters improve their methods and schemes.	❑ Develop, implement, and use comprehensive ad hoc reporting capabilities.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Audits • Audit unit • Audit processes *(continued)*	• Do not forget to audit the auditors. Do not assume that simply because they are auditors that it is not necessary to review their work performance.	❑ Conduct vulnerability assessment. ❑ Take corrective action. ❑ Conduct assessment annually. ❑ Rotate auditors and responsibilities on a regular basis. ❑ Audit the auditors, supervisors, and managers. ❑ Review work processes and recommend updates as necessary in order to reduce evolving fraud risks as they are identified.	
DMV-Related or Imitator Websites *(e.g., DMV.org)*	• Consumers paying unnecessary fees for information they could receive for free from the DMV or the DMV website. • Complaints come to the DMV.	❑ Make customers aware of these sites and fees they charge. ❑ Purchase domain names for sites similar to the DMV domain.	❑ Prevent hijacking of web searches to an imitator site.
Telecommuting Employees	• Employees working from home have access to a tremendous amount of data and may have the ability to manipulate data and provide access to unauthorized individuals. • Remote employees may steal time by not working a full day. • Employees telecommuting over unsecured wireless network may be putting personal and sensitive data at risk.	❑ Provide equipment for telecommuters. ❑ Require employee to sign acknowledgement of acceptable work environment, productivity requirements, and so on. ❑ Audit work of remote employees. ❑ Establish security standards for working over a wireless network.	❑ Electronically monitor employee work hours and productivity. ❑ Send an alert when an unacceptable time period of not working occurs.
Call Centers	• Customer service representatives (CSRs) could provide information or alter records inappropriately in violation of established policies. • Employing CSRs with foreign language skills is a best practice. • If possible, avoid any situation in which CSRs must take credit card information over the phone.	❑ Establish a process to ensure callers are the individuals they claim to be. ❑ Use an Interactive Voice Response (IVR) system to provide 24/7 information to customers. ❑ An IVR can accept credit card information and eliminate the need for CSRs to accept the information. • If this cannot be accomplished, limit the number of CSRs who have the ability to take credit card information over the phone.	❑ Record calls for future access. ❑ If CSRs also handle email inquiries, encrypt emails to protect information. ❑ Establish a IVR function for collecting credit card information from callers to eliminate CSR interaction with payment data. ❑ Online chats should be encrypted. ❑ Use an audit log to record changes to the record.

(continued)

Area of Vulnerability	Specific Risk and General Recommendations	Process Recommendation or Solution	IT Recommendation or Solution
Call Centers *(continued)*		❑ For call centers in prisons, restrict access to personal information. ❑ Randomly monitor phone calls.	❑ Use customer authentication data services to verify the identities of customers over the phone.
Kiosk and Web Transactions	• Improper access by an individual other than licensee or vehicle owner or registrant can occur when proper precautions are not implemented. • Theft or vandalism can take place with kiosks in an unsecure location. • Individuals may place skimming devices or cameras on or near kiosks to capture credit card and other confidential information.	❑ Place kiosks in secure locations to avoid theft, unauthorized access, and vandalism. ❑ Alert customers of phishing scams to obtain personal information.	❑ Require multiple point verification of the applicant's identity before the transaction is processed. ❑ Equip kiosks with video cameras to record users during transactions. ❑ Use facial recognition for DL transactions. ❑ Take steps to prevent spoofing (non-authorized entities redirecting web traffic to their site). ❑ Notify customers of these sites and advise how to ensure they visit the official DMV website.
Credit Card Processing	• Deter credit card fraud by limiting employee access (with the goal to eliminate employee access) to customers' credit card numbers.	❑ Use credit card swipes for all over-the-counter payment transactions. ❑ Unless the financial transaction is one that individuals will repeat on a frequent basis (monthly), do not store credit card information for future use. Only store the credit card data for authorization and settlement purposes. This reduces risk and exposure.	❑ Ensure your jurisdiction and providers adhere to the Payment Card Industry Data Security Standard (PCI DSS) applicable to the methods of accepting credit card transactions and data protection to encrypt all static and transmitted credit card data. ❑ For all credit card entry applications, ensure all credit card fields are masked: the first 12 digits of the credit card number should appear as X's. • Enable billing address verification for all credit card transactions via merchant service provider(s). • Enable card security value (CSV) collection and verification via service provider(s).

Appendix A Examples of Statutory Authority for Law Enforcement Authorities

Kansas Statutory Language for Investigator Subpoena Authority

75-5157. Issuance of subpoenas by secretary of revenue; law enforcement agents; authority.

(a) The secretary of revenue or the secretary's designee may issue subpoenas to require the attendance of any witnesses and the production of any records, books, papers and documents that is considered necessary for the investigation of driver's license fraud and to: (1) Ascertain the eligibility of an applicant for a Kansas driver's license or identification for such license or identification card; (2) ascertain the eligibility of a holder of a Kansas driver's license or identification card for such license or identification card; (3) determine whether a person's identity has been stolen by a person in Kansas; (4) facilitate the investigation of suspected fraudulent activity with regard to obtaining a Kansas driver's license or identification card; (5) facilitate the investigation of violations of the licensure of vehicle sales and manufacturing statutes in article 24 of chapter 8 of the Kansas Statutes Annotated; or (6) facilitate the investigation of vehicle title and registration fraud. Subpoenas so issued may be served by any law enforcement officer, in the same manner as similar process in the district court. Any person who testifies falsely, fails to appear when subpoenaed or fails or refuses to produce material pursuant to the subpoena shall be subject to the same orders and penalties to which a person before a court is subject. Any district court of this state, upon application of the secretary of revenue, may in its discretion compel the attendance of witnesses, the production of material and the giving of testimony before the secretary of revenue, by an attachment for contempt or otherwise in the same manner as production of evidence may be compelled before the district court. Agents designated by the secretary of revenue are hereby vested with the power and authority of peace and police officers, in the execution of the duties imposed upon the secretary of revenue in chapters 8 and 79 of the Kansas Statutes Annotated.

(b) Each agent designated by the secretary under subsection (a), shall have the authority to make arrests, conduct searches and seizures and carry firearms while investigating violations of laws administered by the secretary of revenue, director of vehicles and director of taxation and generally to enforce all the criminal laws of the state as violations of those laws are encountered by such agents during the routine performance of their duties. No agent of the secretary shall be certified to carry firearms under the provisions of this section without having first successfully completed the training course or courses prescribed for law enforcement officers under subsection (a) of K.S.A. 74-5604a, and amendments thereto. The secretary may adopt rules and regulations prescribing other training required for such agents or employees.

(c) Each agent designated by the secretary shall: (1) Be vested with law enforcement authority; (2) be in the classified service under the Kansas

civil service act; (3) not have been convicted of a felony under the laws of any state or of the United States prior to or during employment as law enforcement officer under the authority of the secretary of revenue; (4) be a certified law enforcement officer or have one year of investigative experience or, in lieu thereof, a bachelor's degree from an accredited university or college.

Statutory Language for Law Enforcement Authorities

CALIFORNIA

830. Any person who comes within the provisions of this chapter and who otherwise meets all standards imposed by law on a peace officer is a peace officer, and notwithstanding any other provision of law, no person other than those designated in this chapter is a peace officer. The restriction of peace officer functions of any public officer or employee shall not affect his or her status for purposes of retirement.

830.3. The following persons are peace officers whose authority extends to any place in the state for the purpose of performing their primary duty or when making an arrest pursuant to Section 836 as to any public offense with respect to which there is immediate danger to person or property, or of the escape of the perpetrator of that offense, or pursuant to Section 8597 or 8598 of the Government Code.

These peace officers may carry firearms only if authorized and under those terms and conditions as specified by their employing agencies:

(c) Employees of the Department of Motor Vehicles designated in Section 1655 of the Vehicle Code, provided that the primary duty of these peace officers shall be the enforcement of the law as that duty is set forth in Section 1655 of that code.

1655.

(a) The director and deputy director of the department, the Deputy Director, Investigations Division, the Chief, Field Investigations Branch, and the investigators of the department, including rank-and-file, supervisory, and management personnel, shall have the powers of peace officers for the purpose of enforcing those provisions of law committed to the administration of the department or enforcing the law on premises occupied by the department.

(b) Any person designated in subdivision (a) may inspect any vehicle of a type required to be registered under this code, or any component part thereof, in any garage, repair shop, parking lot, used car lot, automobile dismantler's lot, steel mill, scrap metal processing facility, or other establishment engaged in the business of selling, repairing, or dismantling vehicles, or reducing vehicles or the integral parts thereof to their component materials for the purpose of investigating the title and registration of the vehicle, inspecting wrecked or dismantled vehicles, or locating stolen vehicles.

NEW YORK

Section 392-B New York State Vehicle and Traffic Law

Investigators of the Department of Motor Vehicles shall have all the powers of Peace Officers as set forth in section 2.20 of the NYS Criminal Procedure Law.

Criminal Procedure

§ 2.20 Powers of peace officers.

1. The persons designated in section 2.10 of this article shall have the following powers:

   (a) The power to make warrantless arrests pursuant to section 140.25 of this chapter.

(b) The power to use physical force and deadly physical force in making an arrest or preventing an escape pursuant to section 35.30 of the penal law.

(c) The power to carry out warrantless searches whenever such searches are constitutionally permissible and acting pursuant to their special duties.

(d) The power to issue appearance tickets pursuant to subdivision three of section 150.20 of this chapter, when acting pursuant to their special duties. New York city special patrolmen shall have the power to issue an appearance ticket only when it is pursuant to rules and regulations of the police commissioner of the city of New York.

(e) The power to issue uniform appearance tickets pursuant to article twenty-seven of the parks, recreation and historic preservation law and to issue simplified traffic information pursuant to section 100.25 of this chapter and section two hundred seven of the vehicle and traffic law whenever acting pursuant to their special duties.

(f) The power to issue a uniform navigation summons and/or complaint pursuant to section nineteen of the navigation law whenever acting pursuant to their special duties.

(g) The power to issue uniform appearance tickets pursuant to article seventy-one of the environmental conservation law, whenever acting pursuant to their special duties.

(h) The power to possess and take custody of firearms not owned by the peace officer, for the purpose of disposing, guarding, or any other lawful purpose, consistent with his duties as a peace officer.

(i) Any other power which a particular peace officer is otherwise authorized to exercise by any general, special or local law or charter whenever acting pursuant to his special duties, provided such power is not inconsistent with the provisions of the penal law or this chapter.

(j) Uniformed court officers shall have the power to issue traffic summonses and complaints for parking, standing, or stopping violations pursuant to the vehicle and traffic law whenever acting pursuant to their special duties.

2. For the purposes of this section a peace officer acts pursuant to his special duties when he performs the duties of his office, pursuant to the specialized nature of his particular employment, whereby he is required or authorized to enforce any general, special or local law or charter, rule, regulation, judgment or order.

3. A peace officer, whether or not acting pursuant to his special duties, who lawfully exercises any of the powers conferred upon him pursuant to this section, shall be deemed to be acting within the scope of his public employment for purposes of defense and indemnification rights and benefits that he may be otherwise entitled to under the provisions of section fifty-k of the general municipal law, section seventeen or eighteen of the public officers law, or any other applicable section of law.

Appendix B Codes of Ethics Examples

ARIZONA

THE ADOT CODE OF CONDUCT

Although the Code may not cover every situation, it does set forth a basic philosophy of conducting business. Employees are encouraged to seek the advice of their immediate supervisors if they are in doubt about any situation, potential decision or action. More specific guidelines may be available to employees of individual business sections to help them apply the Code in particular work areas.

Interaction with Customers and Stakeholders

ADOT employees and representatives are expected to be honest, fair and objective when communicating with customers and stakeholders. We are committed to satisfying our customers and partners by delivering quality products and services.
This means that ADOT employees and representatives must never:

- make false or misleading statements
- engage in deceptive or unfair practices
- engage in activities that may be perceived to be dishonest, deceptive or unfair

Contract Related Activities

Employees who deal with outside contractors must maintain independence and impartiality in their business relationships, both in fact, as well as in appearance. ADOT will not tolerate illegal or unethical business practices. All decisions shall be based on an impartial assessment of the costs and benefits to ADOT.

This means that ADOT employees and representatives must:

- not give or receive gifts, gratuities, or entertainment in exchange for business favors or to influence a business decision.
- avoid personal relationships that can be construed as conflicts of interest or raise the appearance of impropriety.
- adhere to the ADOT Gift Policy and other procurement related policies and restrictions.

Conflicts of Interest and Personal Gain or Benefit

All employees have a responsibility to act in the best interest of ADOT. Employees are prohibited from using their positions for personal benefit or gain. All employees need to avoid not only conflicts of interest, but the appearance of a conflict of interest.

Any ADOT employee having a personal (including a family or other close personal relationship), or financial stake in the outcome of a decision is required to reveal to their supervisor that relationship before being involved in the decision making.

Use of ADOT Resources

ADOT resources, (tangible assets such as equipment and tools; and intangible assets such as time and knowledge) are for ADOT business. It is the responsibility of each employee to ensure the proper use and protection of all ADOT resources. Employees are expected to be familiar with and adhere to all ADOT policies including electronic equipment usage.

Outside Business Interests

Employees may choose to become involved in business interests outside ADOT. Situations that may have potential conflicts of interest should be discussed with your supervisor and be in accordance with ADOA Rule R2-5-501 Standards of Conduct, and ADOT PER-6.02 Conflict of Interest of Officers and Employees and Secondary Employment.

Political Activity

All employees are expected to adhere to the provisions of ARS 41-770 Causes for Dismissal or Discipline, regarding political activity, as well as the ADOT Policy on Political Activity PER-6.01.

Equal Employment Opportunities

ADOT is committed to a policy of nondiscrimination. ADOT employees at all levels do not discriminate against any individual on the basis of race, color, sex, religion, national origin, age, pregnancy and/or disability.

Personnel decisions should be made based on merit. These decisions include hiring, promotions, discipline, transfer, recruitment, advertising, reduction in force, all compensation, selection for training, job assignments, accessibility, working conditions, special duty details, and employee evaluations.

Compliance with ADOT's Code of Conduct

Employees who violate ADOT's Code of Conduct put themselves and the agency at the risk of facing serious legal consequences, including criminal penalties. Code of Conduct violations will result in disciplinary action, up to and including termination.

Periodically, all ADOT employees will be required to take a training course and will be asked to sign a document stating that you understand and are in compliance with the Code of Conduct, and have disclosed all situations that may present a conflict of interest.

MARYLAND

MVA ETHICS STATEMENT

Background

The MVA is in a unique position of significant trust, responsibility, and accountability for the safety and security of the people of Maryland, the traveling public and everyone within the transportation services community.

Therefore, ethical conduct - and the avoidance of the appearance of impropriety - is of critical importance in our relationships with individuals, businesses, government agencies and with each other.

The MVA has instituted a "Zero Tolerance" policy for any and all illegal activity and will vigorously prosecute fraud, identity theft and other crimes. However, ethics consists of much more than the absence and avoidance of illegal activity. Ethics is the basis for the principles of conduct that govern each and every action of MVA employees.

The Ethics Statement

The following declaration clearly communicates the values, ethical standards and principles that are held by the MVA.

The MVA is in the privileged/trusted position of providing Marylanders with identity documents, driver and vehicle products and services that promote the mobility, security and safety of everyone living in Maryland, traveling through Maryland, and the public at large. The responsibility for maintaining that privilege/trust rests with each and every MVA employee and extends beyond the normal workday to every hour of every day.

To that end, MVA employees must always:

1. Be mindful of the public trust/confidence that has been accorded them.
2. Remain committed to protecting and building the public trust to the highest level.

3. Be diligent in safeguarding the personal and confidential information and products that are entrusted to them and must be vigilant in identifying and reporting any misuse of this information and/or these products.

4. Be professional, respectful, responsive, objective, fair and impartial in their dealings with customers and other employees.

5. Be honest and accountable for the productive use of their work time, as well as their use of MVA supplies, materials, equipment and other resources.

6. Remember to never take any action, or conduct themselves in any way, that could give the appearance of impropriety, or that could tarnish, diminish or erode the public's trust and confidence in the MVA.

Appendix C Working Group Rosters

Internal Fraud Working Group Roster

CHAIR

John T. Kuo
Administrator (former)
Maryland Motor Vehicle Administration

Marshall Rickert
Assistant to the Chair
Maryland Motor Vehicle Administration

JURISDICTION REPRESENTATIVES

Shawn B. Sheekey
Deputy Chief Administrator (former)
New Jersey Motor Vehicle Commission

Doris Bonet
Field Audit Supervisor (retired)
Arkansas Department of Revenue

Carmen Alldritt
Director (former)
Kansas Division of Motor Vehicles

Tom Edwards
Supervising Investigator
California Department of Motor Vehicles
2120 Broadway, Sacramento, CA 95818
Telephone: (916) 229-0167
tedwards@dmv.ca.gov

FEDERAL GOVERNMENT REPRESENTATIVES

Selden Fritschner
Chief, Commercial Driver License Division
Federal Motor Carrier Safety Administration
1200 New Jersey Avenue, SE
MC-ESL, 6th Floor, West Wing
Washington, DC 20590
Telephone: (202) 366-0677
selden.fritschner@dot.gov

L. Keith Fowler
National Program Manager, Office of Investigations
Identity and Benefit Fraud Unit
Immigration and Customs Enforcement
500 12th Street, SW
Washington, DC 20536
Telephone: (202) 276-0450
lawrence-II.fowler@dhs.gov

AAMVA STAFF

Fred Porter
Director of Member Support, Regions I and II (retired)
AAMVA

Staff Liaison

Sheila Prior
Director of Member Support, Regions III and IV
AAMVA
10800 N. 101st Street
Scottsdale, AZ 85260
Telephone: (480) 275-4584
sprior@aamva.org

External Fraud Working Group Roster

CHAIR

Owen McShane
Director of Investigations
New York Department of Motor Vehicles
6 Empire State Plaza, Room 431
Albany, NY 12228
Telephone: (518) 474-8805
Owen.McShane@dmv.ny.gov

REGION I

Chrissy Nizer
Deputy Administrator
Maryland Motor Vehicle Administration
6601 Ritchie Highway, N.E., Room 102
Glen Burnie, MD 21062
Telephone: (410) 787-7830
cnizer@mva.maryland.gov

Tiffany Roadcap
Pennsylvania Department of Transportation
1101 S. Front Street
Harrisburg, PA 17104
Telephone: (717) 425-7393
tiroadcap@pa.gov

REGION II

Brenda Mays
Director, Identity Verification Unit
Oklahoma Highway Patrol
3600 North Martin Luther King Avenue
Oklahoma City, OK 73136
Telephone: (405) 425-2402
bmays@dps.state.ok.us

Karen Grim
Assistant Commissioner
Virginia Department of Motor Vehicles
2300 W. Broad Street
Richmond, VA 23220
Telephone: (804) 367-6659
Karen.Grim@dmv.virginia.gov

REGION III

Major Paul Steier
Director, Bureau of Identity Theft and Investigation
Iowa Motor Vehicle Division
6310 SE Convenience Boulevard
Ankeny, IA 50021
Telephone: (515) 237-3260
paul.steier@dot.iowa.gov

Dean Reynoldson
Chief Investigator, Office of Special Investigations
Kansas Department of Revenue
915 S.W. Harrison, Room 1030
Topeka, KS 66612-1588
Telephone: (785) 213-5220
dean.reynoldson@kdor.ks.gov

REGION IV

Frank Alvarez
Chief, Investigations
California Department of Motor Vehicles
Investigation Division
2120 Broadway M/S N215
Sacramento, CA 95818
Telephone: (951) 653-5324
Falvarez@dmv.ca.gov

David Martin
Program Coordinator, Fraud Prevention Section
Oregon Driver & Vehicle Services
1905 Lana Avenue, NE
Salem, OR 97314
Telephone: (503) 945-5263
david.k.martin@odot.state.or.us

FEDERAL PARTICIPANTS

Keith Fowler
National Program Manager, Homeland Security Investigations, Identity and Benefit Fraud Unit
Immigration and Customs Enforcement
500 12th Street SW
Washington, DC 20536
Telephone: (202) 276-0450
Lawrence-II.K.Fowler@ice.dhs.gov

Mike Loose
CDL Specialist
Federal Motor Carrier Safety Administration
1200 New Jersey Avenue, SE
MC-ESL, 6th Floor, West Wing
Washington, DC20590
Telephone: (202) 366-9579
michael.loose@dot.gov

AAMVA STAFF

Staff Support

Geoff Slagle
Director, Identity Management
AAMVA
10322 Fairchild Road
Spring Hill, FL 34608
Telephone: (703) 342-7459
gslagle@aamva.org

Brian Ursino
Director, Law Enforcement
AAMVA
2112C Alki Avenue SW
Seattle, WA 98116
Telephone: (703) 350-5103
bursino@aamva.org

Staff Liason

Sheila Prior
Director, Member Support, Regions III & IV
AAMVA
10800 North 101st Street
Scottsdale, AZ 84260
Telephone: (480) 275-4584
sprior@aamva.org

American Association of Motor Vehicle Administrators
4401 Wilson Boulevard, Suite 700
Arlington, Virginia 22203
703.522.4200 | **aamva.org**