



American Association of  
Motor Vehicle Administrators

**Security** *Integration*  
**Law** **MISSION**  
**Enforcement**  
**Investigations**  
**OPERATIONS**  
*Guidance*



# DMV Investigative Unit Resource Guide



March 2017

INVESTIGATOR INTEGRATION WORKING GROUP  
LAW ENFORCEMENT STANDING COMMITTEE

2017 © Copyright All Rights Reserved  
American Association of Motor Vehicle Administrators

Cover photo credits: Thinkstockphotos.com – “Crime Scene” by Jayson Photography, “Evidence” by Praathan; “Arrest” courtesy AAMVA.

# Contents

- Executive Summary ..... 2
- Introduction and Background ..... 3
  
- Chapter 1     **The Investigative Unit** ..... 4
  - Non-investigatory Benefits of an Investigative Unit* ..... 4
- Chapter 2     **Hiring DMV Investigators** ..... 10
  - Job Descriptions* ..... 10
  - Recruitment* ..... 11
- Chapter 3     **Training and Retention** ..... 12
  - Retaining the Team* ..... 12
- Chapter 4     **Supporting Investigations through Partnerships** ..... 13
  - Internal Partnerships* ..... 13
  - External Partnerships* ..... 16
- Chapter 5     **Tools** ..... 21
  - U.S. Tools* ..... 22
  - Canadian Tools* ..... 25
- Chapter 6     **Review and Assessment** ..... 28
- Chapter 7     **Awards and Recognition** ..... 29
  - Create an Employee Recognition Committee* ..... 29
  
- Appendix A   **Survey** ..... 31
  - Survey Overview* ..... 32
- Appendix B   **Federal Resources** ..... 54
- Appendix C   **Working Group Roster** ..... 58

# Executive Summary

This Department of Motor Vehicles (DMV) Investigative Unit Resource Guide (hereinafter referred to as the *Resource Guide*) is a product of the DMV Investigator Integration Working Group (hereinafter referred to as the *Working Group*) and represents one of two *Working Group* deliverables. The other deliverable is an Integration Strategies document that includes five strategies and 10 specific recommendations identified by the *Working Group* that would better integrate DMV investigators into the American Association of Motor Vehicle Administrators (AAMVA) community and the law enforcement discipline specifically.

This DMV Investigator *Resource Guide* was identified by the DMV investigator community as a need that AAMVA could fill. This *Resource Guide* includes general organizational and operational principles and guidance for DMV investigative units based on the research, experiences, and practices of Working Group members and the agencies they represent.

The AAMVA already has resources of use to the DMV investigator community; however, this *Resource Guide* pulls into a single document the portions of those multiple resources most applicable to DMV investigators and their respective missions. The Working Group also conducted a gap analysis between existing resources and identified additional resources and guidance that would be helpful and have woven that information into the *Resource Guide* as well.

There are several Best Practices on the AAMVA website applicable to DMV investigators. The *Facial Recognition Program Best Practices* falls under the DL/ID Standards and Guidelines subheader on the AAMVA best practices landing page, and several more resources fall under the Fraud subheader. To view them in their entirety, go to <http://www.aamva.org/best-practices-and-model-legislation/>

# Introduction and Background

The mission statement of the AAMVA Law Enforcement Standing Committee (LESC) is “To inspire collaboration between law enforcement and motor vehicle administrators to improve highway and public safety.” The LESC believes that in order to reach the next level of collaboration, DMV investigators need to be better integrated into the AAMVA community and into the activities of the law enforcement discipline specifically. Toward that end, the AAMVA DMV Investigator Integration Working Group was established in FY 2015.

The staffing, mission scope, and authority of DMV investigative units vary throughout North America. Therefore, Working Group membership selection focused on individuals representing DMV investigative units of various mission disciplines (driver and vehicle), and authority levels. There was also a focus on ensuring balance among the four

AAMVA regions and representation from state law enforcement agencies that sometimes assist DMV investigators with investigations or arrest operations. The Working Group consisted of 11 DMV investigators (including one Canadian), four law enforcement representatives, one board advisor, and three AAMVA staff.

The aforementioned variables also means that portions of this Resource Guide are likely not applicable to every DMV investigative unit depending on their specific mission, composition, and authority. However, the majority of this document should be helpful to every unit.

This *Resource Guide* is considered a living document and as such will be evaluated annually and updated as needed to ensure it remains a useful tool to the DMV investigator community.

# Chapter 1 The Investigative Unit

The primary role of a DMV investigative unit is to protect the integrity of DMV records, documents, credentials, processes, and revenues. Investigators are charged with investigating crimes associated with internal and external fraud, identity theft, titles, registration, and more. Investigations can involve lone offenders or complex criminal organizations.

DMVs are on the front lines of national security and identity protection, and the need is greater than ever to address fraud by enhancing or creating functional, stand-alone investigative units. With a sufficiently staffed and properly equipped investigative unit, the DMV keeps an eye on critical identification processes. The investigative 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.

The investigative unit will likely be tasked with conducting investigations related to employee misconduct, fraud, and theft allegations that stem from information provided by outside law enforcement agencies, informants, and data and work reviews performed by internal sources. These types of investigations can utilize much of the same training and skill sets of the field investigations, but they typically require a much more in-depth knowledge of the inner workings and policies of the agency.

## Non-investigatory Benefits of an Investigative Unit

In addition to handling investigations and addressing fraud challenges, investigators can provide valuable assistance in many other areas including:

- Provide analysis for proposed legislation.
- Provide input to improve policies, processes, and training.
- Provide education and training to front-line staff.
- Identify areas of vulnerability.
- Assist with internal audits.
- Provide undercover testing (both internally and with third parties).
- Assist with development and analysis of requests for proposals.
- Provide input and feedback on equipment purchases.
- Provide insight into the overall design and security features of driver's licenses and identification cards (DLs/IDs).
- Share findings to improve DMV functionality.
- Work with human resources in developing employee hiring standards.
- Work with the information technology (IT) division to modernize existing databases and identify elements that should be recorded and tracked.

- Work with auditors to show potential vulnerabilities both inside and outside the organization.
- Conduct background checks.
- Help develop ethics training.
- Train staff on DMV fraud.
- Teach fraud detection to other law enforcement agencies.
- Train prosecuting attorneys on DMV fraud and the societal impact(s).
- Provide expert testimony on DMV-related cases.
- Serve as a resource for outside law enforcement agencies and prosecutors to obtain records, identify fraudulent records, and stop titles and licenses from being issued to ineligible applicants.

The experience of DMV investigators can be a significant benefit when deciding what is necessary for the security of DMV credentials. 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 investigative 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.

For all of the reasons stated here and for many more reasons, an investigative unit can greatly benefit the agency, the jurisdiction, and the public. 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.

### *Establishing an Investigative Unit*

DMVs should strive to implement and maintain—at a minimum—a “good” investigative program. The table below describes basic tenants that constitute “good, better, and best” programs.

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

## *Setting Up an Investigative Unit for the First Time and Managing Change*

When establishing an investigative 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. After the unit has been established, both the mission and staffing levels of the investigative unit should be regularly reviewed to determine if changes are needed.

Agencies should 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 investigative 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 investigative 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.

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

### *Responsibilities of the Investigative Unit*

Management must determine what the unit will investigate. Facial recognition “hits,” title and odometer fraud, dealer regulations, written and road driver testing fraud, DL fraud, identity theft, and DMV tax fraud are just a few of the areas of potential responsibility of the unit. Determine whether the unit will conduct general investigations, inspect vehicle 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 investigative unit should have the training and authority to conduct covert operations (e.g., observing third-party commercial driver license [CDL] testing or translated tests or seeking out corrupt examiners), 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. An investigative 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 investigative 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 investigative 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 investigative unit, they can help promote the unit to the public and to the legislature and can provide valuable information to the unit.

In jurisdictions with reciprocal license agreements, there is a need to examine each of the licenses submitted to ensure authenticity. The investigative unit can provide necessary tools and resources for the verification of questionable documents.

### *Staffing and Equipping an Investigative Unit*

A core competency of the DMV is the issuance of credentials. An equally important core competency



should be fighting fraud. A crucial requirement in the fight against fraud is an appropriately sized and adequately equipped investigative 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 investigative unit provides the ability to proactively oversee the operation from a focused perspective because its primary mission is the detection and deterrence of fraud. An investigative 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.

The investigative unit should have oversight and authority to address both internal and

external fraud. The appropriate size of the unit depends on the size of the DMV, 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

**An optimum investigative team includes:**

- Sworn investigators (or a hybrid of sworn and nonsworn)
- Forensic auditors
- Forensic IT analysts
- Research analysts
- Document examiners

legislation or policies, consideration should always be given to the potential need for additional staff for the investigative 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 because 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.

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.

### *Support Staff Qualifications 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, and forensic accountants play key roles in the deterrence and detection of fraud. These positions do not necessarily need to be part of the investigative unit, but they should certainly exist within the organization and should work collaboratively with the investigative 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.

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 investigate 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 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.

Computer forensic analysts can provide services related to the data from devices seized during such investigations. Analysts can be responsible for the identification, collection, examination, and presentation of electronically stored information as evidence.

Staff should have 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 IT unit must cooperate with the investigative 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.

### *Funding the Investigative Unit*

A variety of federal agencies offer grant opportunities and sharing programs that can provide support for investigative units. A few examples are listed below:

The United States Secret Service 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. <https://www.secretservice.gov/investigation>

The U.S. DHS Document Benefit Task Forces are set up around the country. They work closely with DMV investigative units across the country and provide staff and equipment when needed. They also offer periodic grant opportunities for projects and system enhancements. [www.ice.gov/identity-benefit-fraud](http://www.ice.gov/identity-benefit-fraud)

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 Regional Information Sharing Systems (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. [www.riss.net](http://www.riss.net)

The Federal Motor Carrier Safety Administration offers annual grant opportunities for agencies looking to make enhancements to its CDL license issuance process. [www.fmcsa.dot.gov](http://www.fmcsa.dot.gov)

### *Existing Investigative Unit Review*

If an investigative 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 investigative unit when planning for new legislation or programs to ensure fraud deterrents are in place.

### *Alternatives if Establishing an Investigative Unit Is Not Possible*

If it is not possible to obtain funding or authorization to establish an “in-house” investigative unit, it 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.

## Chapter 2 Hiring DMV Investigators

The success of the DMV investigative unit will largely depend on selecting and hiring individuals who have the required education, investigative experience, and knowledge of DMV processes. Ideally, investigators should have law enforcement experience. Retired or former law enforcement officers with specific experience in investigation bring well-honed and pertinent skills to a DMV investigative unit.

### Job Descriptions

Job descriptions for each job classification within the investigative unit should be developed. Duties and responsibilities of an investigator may include, but not be limited to:

- Conduct investigations pertaining to identity theft, licensing and regulation of businesses (e.g., dealers, vehicle safety and emissions inspections, third party testers).
- Conduct investigations related to stolen vehicles, organized theft rings, Vehicle Identification Number (VIN) removals, and other auto-related crimes.
- Conduct investigations related to internal fraud.
- Make criminal arrests and initiate other enforcement action(s).
- Provide court or administrative hearing testimony.
- Prepare comprehensive investigative case reports.
- Assist other law enforcement agencies as needed.
- Inspect rebuilt salvage vehicles and specially constructed vehicles.
- Handle complaints from the public.
- Participate in impaired driving, underage drinking, and other traffic safety–related programs.
- Perform other duties as required or assigned.

### *Investigator Qualifications and Requirements*

It is important to establish minimum requirements and criteria for knowledge, skills, and abilities, some of which may include:

- Minimum of 21 years of age
- Possession of a valid driver's license
- working knowledge of relevant motor vehicle laws, rules, regulations, and policies
- Working knowledge of the criminal justice system
- Working knowledge of VINs, certificates of titles, and vehicle registrations
- Ability to exercise law enforcement skills and responsibilities
- Ability to establish and maintain positive interactions and working relationships with personnel from other law enforcement agencies and the general public

- Ability to maintain a physical fitness standard as prescribed by the department
- Excellent written and oral communication skills
- Appropriate law enforcement certification(s)

## Recruitment

Qualified investigators can be recruited through college and other job fairs, newspaper advertisements, agency websites and social media, internal recruitment, the military, professional networking, current and former law enforcement officials, and internship programs, to name a few.

### Selection Process

After job descriptions have been established and qualification and requirements defined, the selection process can take place. The following are steps in a robust selection process.

- *Written exam* – Should be standards based and defensible, test the applicant’s knowledge, and evaluate writing skills and problem-solving abilities.
- *Physical fitness testing* – Should be validated against the job requirements and adapted to the applicant’s age and gender norms.
- *Oral board* – Questions and scoring should be standardized, job specific, and approved by the human resources (HR) department.
- *Reference checks* – A minimum of three checks provided by the applicant should be completed. Additional references not specifically suggested by the applicant should also be checked to validate the information provided.
- *Conditional letter of employment* – After the preferred candidate is identified, a conditional letter of employment can be issued. The offer will depend on the applicant’s passing a

background check, polygraph test, and other requirements as defined by the agency.

- *Background investigation* – After a conditional offer of employment is made, a comprehensive background investigation should be completed for all investigative unit staff. Background investigations should include, at a minimum, a fingerprint-based criminal history check, driving record history, credit history, and social media review. References checks should include previous employers, landlords, and local police agencies. Background investigations should be standardized. A checklist should be developed to ensure uniformity in background investigations.
- *Polygraph test* – If allowed by the jurisdiction, a polygraph test should be administered. Any evidence of deception should result in automatic disqualification of the candidate.
- *Medical exam(s)* – Medical exams may be conducted to determine fitness for duty. Drug screening should be included.

## Chapter 3 Training and Retention

To be successful, an investigative unit must develop a comprehensive training program. In addition to training required by jurisdictional law, curriculum should be based on a current training needs assessment.

A variety of training delivery options can be offered, including:

- New employee orientation or on-boarding
- Basic law enforcement training (e.g., academy or Police Officer Standardized Training [POST])
- In-service training
- On-the-job training (e.g., , Field Training Officer [FTO])
- Webinars
- Specific task related training such as facial recognition comparison training
- AAMVA fraud tools, such as Fraud Detection and Remediation training, Facial Recognition Best Practices, Best Practices for the Deterrence and Detection of Fraud, or National Motor Vehicle Title Information System (NMVTIS)
- Attendance at AAMVA and other conferences or trainings that allows for networking with peers
- Other professional development opportunities

### Retaining the Team

For continuity and efficiency of operations, agencies should make every effort to retain experienced staff. The cost of training is high, and the loss of institutional knowledge by those departing can have an adverse impact on the unit's effectiveness. When retention efforts fail, prompt replacement of departing personnel should be a high priority to avoid long-term case overload by remaining personnel. Retention strategies may include offering:

- A competitive salary
- A positive work culture or environment
- Continuing education and training
- Professional development and advancement opportunities
- Employee recognition and reward
- Telecommuting opportunities
- Flexible work schedules
- An avenue for employee feedback and suggestions and by taking action when appropriate

When employees leave, use exit interviews to learn about the strengths and weaknesses of the agency and unit. Based on the information learned, take actions to improve areas of weakness and prevent further loss of staff.

## Chapter 4 Supporting Investigations through Partnerships

### Internal Partnerships

The investigative unit must forge effective working partnerships with other divisions within the agency, as well as outside entities to accomplish their goals. These partnerships provide a regular source of information and may also provide early fraud detection.

### *Motor Vehicle Operations*

The vehicle operations department is charged with maintenance of motor vehicle registration and title records that may be vital during the course of an investigation. Vehicle records can help establish patterns of life for people by showing their past residences; addresses used; vehicle ownership or joint vehicle ownership; liens or security interests, which can lead to banking and financial history; and license plate information, which might be tied to crimes in the present or even used to solve cold case crimes ranging from misdemeanors to felonies. Vehicle operations may have records that may show patterns of crimes related to dealer fraud, which could include any number of crimes. The records they keep may contain applications for title and registration, bills of sale, odometer statements, damage disclosure statements, and prior title ownership assignment history.

Dealer crimes detected by reviewing vehicle records can range from disposal of inventory out of trust with a lending institution, internal embezzlement by selling vehicles acquired and not on the official inventory of the dealership, and disposal of vehicles as a commodity related to the illegal drug trade. Many times, this review can be done with records

maintained by vehicle operations without the knowledge of the dealership that their actions are being investigated and before any physical audit or investigation at the actual dealership.

A vehicle records review can detect the selling of vehicles to hide the disclosure of vehicle brands such as rebuilt, flood, fire, hail, or other damage not disclosed to the buyer to increase the value of the vehicle when sold by either a licensed dealer or a private individual.

Another commonly committed crime is the potential for taxation evasion. Many times, vehicle operations maintain the records, which are presented when the title or ownership record is changed. There may be instances when a trade-in vehicle is shown to be credited to the applicant to reduce the taxable amount required to be paid in jurisdictions that have this provision when the trade-in vehicle was not part of the actual transaction. This ghost trade can be determined by following the ownership and title assignments of the vehicle. For example, if dealership A sells a vehicle to customer B and gives the customer credit of a vehicle traded to the dealership on a purchase agreement, an investigator will want to ensure that when ownership changes on the title record that the dealership is named on the assignment. Often, the dealership will allow the credit for the trade-in vehicle when it was sold at retail by the customer to another party and not sold at the actual dealership. This violates provisions to reduce the tax due on motor vehicles in some jurisdictions.

Another crime is the transfer of vehicles that have odometers altered and the mileage reduced to

increase their value to achieve higher profits from the sales. The historical records to vehicles based on title, registration, and ownership records are maintained by vehicle operations and will become an evidentiary item to prove historical fact for the investigator.

The investigative unit needs to determine the following before any record requests are made:

- Can the records be used as evidence in court, or is a court or administrative subpoena required?
- Can the records be released and shared with other agencies that may be assisting the investigative unit in the matter?
- Can the records be obtained at no fee, or if not, is there a prorated fee available for the agency?
- Can the records be retrieved electronically by the unit or do the records have to be manually accessed and retrieved by the vehicle operations department?
- Can the records be retrieved at all hours of the day (via a secure internet connection) or are investigators limited to access only during the business hours of vehicle operations?

### *Dealer and Business Licensing Operations*

Dealer and business licensing operations is usually responsible for licensing of motor vehicle dealers, motor vehicle recyclers, motor vehicle demolishers, auto parts dealers, and junk and salvage yards.

A large volume of information is collected during the application for licensing by entities both before issuance and during the time any license is held. Such information can help the investigator determine connections to a business, possible leads when investigating crimes, those who associate with the business, insurance holders and lenders, and infractions or recorded violations that may not have been issued by the investigative unit.

An application for a dealer's or business license can contain personal information, including phone numbers, email addresses, residence addresses, driver license number, date of birth, social security number, previous criminal history, and the hierarchy of a business.

The investigative unit must develop an effective working relationship with dealer and business licensing operations and establish the protocols to access and receive information from the licensing records. This information may become evidentiary in nature, and the determination of what can be used or made available as evidence, public and nonpublic, should be determined ahead of time. Direct access by the investigator can be helpful because direct access limits the number of people who may become aware of an investigation.

### *Driver License and ID Card Operations*

DL/ID card operations is responsible for maintaining documents used in support of the issuance of driver license and nondriver ID cards. Contained within these documents is information that may be helpful in investigations, including, but not limited to the following.

- Copies of original handwriting samples
- Image capture or facial recognition
- Personal data such as date of birth, physical descriptions, addresses, and social security number
- Birth certificate information
- Passport information
- Prior name, address, or state of record
- Conviction and suspension data
- Lawful presence information
- Medical records, including handicap placard information



- Knowledge and skills testing records
- Identity of the individual who processed the transaction

### *Motor Carrier Operations*

Motor carrier operations is responsible for oversight of motor carriers and commercial motor vehicle operations and/or enforcement. Information they can provide for investigative purposes includes inter and intrastate records on the following.

- Commercial driver license (CDL) information
- Oversize or overweight permitting
- Trip permits
- Heavy Vehicle Use Tax (HVUT)
- Fuel tax records
- International Registration Plan (IRP)
- International Fuel Tax Agreement (IFTA)
- Taxicabs, transportation network companies, and other livery entities
- Fees and payment information

### *Field Operations and Third-Party Partners*

Field operations is responsible for application and issuance of DMV credentials, driver education, and testing, whether by DMV employees working in the field or by third-party agents (e.g., AAA offices, county officials, tag agents) working on behalf of the DMV.

Many field offices are equipped with cameras, electronic access controls, and other tracking systems that may be of help to the investigations unit. In cases of internal fraud, such records can be accessed to review the transactions of a particular clerk, to determine office entry and exit dates and times, to research electronic transactions, and to follow

monies received. Such information can also be used to research customer transactions in the case of suspected fraud.

Those responsible for third-party oversight are charged with ensuring that entities performing services and transactions on behalf of the DMV are following established procedures. Their records can be used to audit third parties to ensure protocols are being followed and to investigate suspected fraud by either the third-party agent or by a customer.

### *Vehicle Safety Inspection and Emissions Operations*

In jurisdictions with a vehicle safety inspection or an emissions program, it is helpful for the investigative unit to develop a relationship with the responsible entity in order to access their records. The data is particularly helpful in determining vehicle information, ownership, odometer information, physical location, and presumed condition or warranty of inspect-ability at the time of inspection. Records can be used for both audit and investigation purposes.

### *Information Technology*

Information technology may be managed within the DMV or at a jurisdiction level where IT for all state agencies is handled centrally. Regardless of where IT operations are housed, the records they manage are an essential tool for DMV investigators. At a minimum, IT departments can provide information related to the following.

- Employee or customer transaction tracking
- Offline search (persons, vehicles, businesses)
- Partial plate number searches
- Vehicle searches associated by geographic locations, vehicle make and model, and so on
- Vehicle crash records

- Vehicles or persons associated with specific addresses or businesses
- Building access control reports (General Headquarters [GHQ] and satellite locations)
- Employee reports related to customer inquiries
- Tracking of specifically identified individuals
- Photo and video requests
- Data analysis for trends, patterns, or other specific requests
- Performance metrics

Information technology is an evolving and valuable tool available to DMV investigators. Relationships should be established and maintained to ensure full value of the tool is accomplished.

### *Human Resources and Legal Department*

It is important to establish a positive working relationship with the agency's HR department to appropriately staff the investigative unit and effectively supervise and train personnel. HR can play a vital role in investigating and disciplining employees.

A strong partnership with the agency's legal department may be helpful in drafting policies, rules, regulations, and legislation. This resource is also critical in assisting with the interpretation and implementation of statutes, regulations, and court rulings. The legal department can also provide guidance in conducting investigations, managing privacy issues, and responding to records requests.

## **External Partnerships**

Forming partnerships with federal, state, provincial, and other stakeholders can provide value to the unit. Partners can bring resources, expertise, and database access that the unit likely does not possess. Partners can also provide information on related cases or

trends that may otherwise be missed. In some cases, it may be necessary to first educate potential partners on the impact of this type of criminal activity on the public. After the partnership has been established, discussions between the unit and its partners should take place on a regular basis.

Expanding partnerships with other agencies enhances investigative success and expands the ability to identify individuals who in the past may have been unknown. Partnerships are about working together and sharing resources. This can only be accomplished through established policies, mutual understanding of roles, and continuous communication. Sharing fraud results between stakeholders provides valuable information to all involved, often resulting in identification of fraud that may otherwise go undetected. Partnerships should be developed with stakeholders within the jurisdiction, as well as cross-jurisdictionally.

### *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 privileged to. 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.

### *Prosecutor, State's Attorney, and Secretary of State Partnerships*

Prosecuting entities should be included in the agency's efforts to fight fraud. Prosecutors are responsible for taking cases before the court; getting them involved early in the process will strengthen the likelihood of a successful outcome. When possible, it is recommended that jurisdictions have specialized prosecutors trained in and designated to the prosecution of fraud. Opportunities to educate the judiciary should be pursued. Investigators in the secretary of state's office are valuable partners in fraud detection and effort should be made to include and partner with them in the enforcement effort.

### *Partnerships with Fusion Centers*

Fusion centers were created after the events of 9/11 to share information among local, state, and federal law enforcement and intelligence community 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.

### *Other Governmental Agencies*

There is significant value in establishing relationships with other state, provincial, and federal agencies as it relates to the detection and reduction of fraud. Investigators from many disciplines of government may benefit from services provided from the DMV and are often unaware. Establishing these mutually beneficial relationships can greatly enhance the detection and prosecution of fraud. Examples of potential partnerships are indicated below.

- Health and human services agencies
- Family and social services agencies
- Social Security Administration
- Department of work force development or unemployment services
- State, provincial, and federal departments of revenue

- State, provincial, and federal departments of homeland security
- Supreme Court or Supreme Court Technology Services
- Department of Justice

### *Criminal Justice Meetings, Working Groups, and Task Forces*

DMV investigators should participate in all relevant law enforcement and fraud reduction meeting opportunities. Participation creates opportunities to offer services and gather investigative knowledge and fraud trends from various geographic locations.

### *Memorandums of Understanding*

Memorandums of understanding should be established and maintained between agencies exchanging information and providing access to service and data.

### *Outreach and Education*

Outreach to and education of partners and other stakeholders will enhance the investigative unit's effectiveness, garner support, and increase the chance of successful prosecutions. As a public service entity, the goal of the investigative unit is to serve the public. This can only be accomplished by working to inform and educate the DMV's "customers." It is critical that the investigative unit create, promote, and foster an active program to educate and inform consumers about the available services and capabilities of the unit.

This process should also serve to educate policymakers and partners about the value, capabilities, and successes of the unit.

### *General Outreach*

Educating the public on the role of the investigative unit, significant successful case outcomes, and new programs or laws can increase the public's confidence

in the DMV as a whole. Openly sharing information provides transparency and builds trust. Delivering an effective outreach and education program will educate, engage, and enable stakeholders to understand how DMV programs contribute to the integrity of the DMV. 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 an investigative unit are well spent.

Outreach may take the form of a high-profile or low-profile campaign and is usually dependent on the message to be delivered. A high-profile campaign is the proactive sharing of information. A low-profile campaign is more passive and is mostly reactionary through responses to media and public inquiries. Even when a low-profile campaign is used, communications with stakeholders remain important.

Outreach methods and processes should be tailored and updated to effectively reach the intended audience. The most effective medium to reach a 25-year-old consumer may be very different from that used to reach a 65-year-old senior citizen. An effective program should consider the entire spectrum of the audience and take a multifaceted approach involving several different mediums and methods.

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.

### *Establish Hotlines or Unit Email*

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. Whistleblowers expose a large percentage of fraud, and 24-hour tip lines encourage the reporting of potential offenses. Publicize the confidentiality and anonymity of fraud prevention reporting. Witnesses to fraud often 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.

Another option for public reporting is through the establishment of an email address or other program such as Crime Stoppers. The agency's email in box should be regularly monitored by the investigative unit, and appropriate action should be taken. Consider allowing the ability for the email address of the sender to be masked or anonymous. Determine if the reporting entity is willing to be a witness to a crime or if it prefers to remain anonymous. Consider circling back to the person who reported fraud to let them know the outcome of their report. If the fraud report comes from an internal source, consider formal recognition of the individual for reporting the fraud.

### *Agency Website*

An agency website also provides an effective way to inform the consumer and direct them to appropriate services. A website allows the DMV to provide access to large amounts of information and to quickly push updated, accurate information. An important element of a marketing strategy involving a website is to create and maintain links from other websites

and pages likely to be of interest to the target audience and to ensure that the site is easily located using popular search engines likely to be used by the consumer. The website may include information on how to report fraud or file complaints, products and services, victim resources, public warnings, consumer alerts, and fraud-related trends, as well as links to success stories of the unit and links to partner agencies offering related services.

### *Social Media*

Social media outlets such as Facebook and Twitter can be used for the agency to inform the public about the efforts of the investigative unit. Information on the type of information that can be reported to the agency or unit, responsibilities of the unit, fraud trends, and so on can be shared. Awareness should help with reporting of fraud and decrease reporting of issues that belong to another agency. Consider adding links for other types of reporting commonly received to the appropriate agency to point the person in the right direction. Use of social media provides instant sharing of information. Social media outlets may be most effective in "pulling" or directing interested consumers to the unit's website or email address for specific information or follow-up communication. Agencies should ensure they have sufficient resources to manage social media communications. Policies on social media should be considered before deployment.

### *Traditional Outreach Methods*

Use of newspaper, television, radio, and distributed "hard-copy" materials is an effective way to reach consumers. These may include informational brochures on products and services, victim resources, public warnings, consumer alerts, fraud-related trends.

### *"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. The Department

of Homeland Security 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.

### *Victim Education and Assistance*

Include information on the agency's website on requirements for credential issuance, copies of pamphlets or brochures on identity theft, human trafficking, and so on as well as links to other agencies that can provide crime victim assistance. Provide a means by which a victim can meet with a DMV representative to request personal assistance.

Credit consumers can receive a free credit report yearly by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com).

Resources for identity theft victims can be obtained from the Federal Trade Commission at [https://www.bulkorder.ftc.gov/publications?f%5b0%5d=field\\_campaigns%3A1587](https://www.bulkorder.ftc.gov/publications?f%5b0%5d=field_campaigns%3A1587)

Additionally, identity theft victims should be directed to the three credit reporting bureaus:

Equifax  
800 525-6285  
[www.equifax.com](http://www.equifax.com)

Experian  
888 397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
800 680-7289  
[www.transunion.com](http://www.transunion.com)

### *Celebrate and Publicize Unit Successes*

An effective outreach strategy involves not only the “push” of information regarding available products and services but also an active effort to celebrate and publicize success, both externally and internally.

Externally, it is important to continuously keep the goals, services, and efforts of the investigative unit in front of the target audience, the consumer. One way to accomplish this is to publicize efforts and successes of the unit. By publicizing arrests and prosecutions, the visibility and reputation of the investigative unit are validated and enhanced.

The benefits to this are multifaceted. Public consumers will gain confidence in the ability of the unit to follow through with the provision of services and be encouraged to report illegal activity. External criminal justice partners and policymakers will begin to see the unit as an effective force for good, an agency that goes after and gets the bad guy.

Take the opportunity to promote your successes in deterring, investigating, stopping, and prosecuting illegal activity without providing investigative tactics or sensitive case details. This is accomplished through issuing press releases and posting on the unit website and social media outlets discussed earlier.

Internally, it is vital to celebrate individual and unit accomplishments and successes. Intrinsic rewards and recognition programs should be designed to promote new initiatives and successes. This is an important yet often overlooked aspect of leading an investigative unit that can reap benefits and encourage similar achievements in the future.

## Chapter 5 Tools

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. 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. 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. Unmarked vehicles should be equipped with radios and other essential equipment. Such vehicles allow investigators to conduct surveillance and other vital functions throughout the course of the investigation.

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.

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.

*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.*

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 or 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.

It is imperative for a DMV to establish information sharing, both internally and externally. Numerous databases are available, but it is important to identify sites containing reliable information. Listed below are several reliable databases made available to investigators to both gather and exchange information.

## U.S. Tools

Various entities throughout North America provide tools that may be of value to DMV investigators. Descriptions of each follow.

### *AAMVA Community Directory*

The AAMVA webpage contains a community directory that provides search capabilities for AAMVA members. Searches can be completed by contact type (e.g., driver contact, DMV fraud contact, law enforcement fraud contact, document authenticity contact). The AAMVA is also establishing a contact for each agency's investigative unit.

## 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

In Canada, a country-wide ability (10 provinces and three territories) to search a name and date of birth for an active, expired, or suspended driver licenses exists through the Interprovincial Record Exchange (IRE).

## CRIMINAL OFFENDER/JAIL BOOKING AND REPORTING SYSTEMS

Many states and regions of the country have a criminal offender or jail booking database system. These systems are valuable to investigators to verify the status of an offender and get notification of an arrest and booking of a suspect or person of interest. Investigative units should check with state or local police and sheriffs to determine what systems are in place for the states or regions where they have investigative responsibilities.

### *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.

### *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.

### *Law Enforcement Information Exchange (LinX)*

The Naval Criminal Investigative Service (NCIS), along with its federal, tribal, state, county and local law enforcement partners, launched the Law Enforcement Information Exchange (LinX) initiative in 2003. LinX is designed to enhance information sharing between participating law enforcement agencies in areas of strategic importance to the Department of the Navy. LinX provides member agencies with secure access to regional crime and incident data and the tools needed to process it, enabling investigators to search across jurisdictional boundaries to help prevent, stop, and solve crimes and share that information. Ownership and control of the data always remains with the host agency.

### *National Insurance Crime Bureau*

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 Claim search, 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.

### *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 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.

### *National Motor Vehicle Title Information System*

The NMVTIS) is a system that allows the titling agency to instantly and reliably verify the information on a 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. The NMVTIS is also a tool that assists states and law enforcement in deterring and preventing title fraud and other crimes. Consumers can use the NMVTIS to access important vehicle history information.

### *National Odometer and Title Fraud Enforcement Association*

The National Odometer and Title Fraud Enforcement Association (NOTFEA) was formed in 1980. The 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

*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.*

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.

### *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.

### *Social Media*

Social media websites are an increasingly valuable tool for investigators to gather information, obtain evidence, and locate suspects and persons of interest. As of this writing, popular social media websites include Facebook, YouTube, Twitter, LinkedIn, Pinterest, Google Plus, Tumblr, and Instagram.

### *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.

Regular communication and coordination should be established among the business units responsible for the entities regulated. If possible, keep and be able to provide statistics regarding cases referred, from where, reason, and outcomes. 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, 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.

### *TransUnion/TLOxp*

Originally created for law enforcement, the search and locate technology in TLOxp® and advanced linking algorithms deliver actionable data through a user-friendly interface in a matter of seconds. Begin investigations with broad parameters. Then dig deeper into leads you've identified. This TransUnion solution delivers instant access to reliable and pertinent data about people, businesses, assets, and locations.

## **Canadian Tools**

Some of the many tools available to Canadian investigators are described below.

### *Canadian Police Information Centre*

Much like the U.S.'s National Crime Information Center (NCIC), the Canadian Police Information Centre (CPIC) is a central police database where Canada's law enforcement agencies can access information on a number of matters. It is Canada's only national law enforcement networking computer system, ensuring officers all across the country can access the same information. Offenders' criminal record history, outstanding warrants, charges before the Courts, stolen property, and missing person information can all be found in CPIC.

### *Justice Online Information Management System*

The Justice Online Information Management System (JOIN) is an Alberta-wide application used to support the administration of the criminal justice process and data activities for federal, provincial, and municipal enforcement agencies, prosecutions, and courts. Primary business functions of JOIN include criminal case tracking, witness management, police scheduling, traffic ticket processing, and financial management.

### *Criminal Intelligence Service Alberta*

Criminal Intelligence Service Alberta (CISA) acts as a central hub for strategic analysis and intelligence sharing on organized and serious crime in Alberta. CISA links organizations responsible for intelligence gathering, criminal investigations, and provincial and federal law enforcement. Through membership in CISA, organizations are able to receive information held in numerous law enforcement databases. Any information shared by CISA with member agencies is governed by the third-party rule.

### *British Columbia Court Services Online*

Court Services Online is British Columbia's electronic court registry. Free online access allows a user to search criminal, civil or traffic courts by name, file number or agency. <https://justice.gov.bc.ca/cso/>

### *Canadian Council of Motor Transport Administrators Interprovincial Records Exchange*

In Canada, a country-wide ability (10 provinces and three territories) to search a name and date of birth for an active, expired, or suspended driver's license exists through the Interprovincial Record Exchange (IRE). The IRE is a tool that provincial and territorial governments use to do the business of driver licensing and vehicle registration. It was developed in 1989 to support the National Safety Code (NSC) and was endorsed by all members of the Council of Deputy Ministers Responsible for Transportation and Highway Safety.

In the mid-1990s, access to the IRE system was increased in support of a road safety requirement—vehicle safety and environment recall campaigns. In the late-1990s, the board reconfirmed IRE's road safety purpose and expanded its purpose to allow for access by other third parties to address safety requirements. Over time, access to third parties has been granted to organizations for multiple purposes such as advancing road safety, for consumer protection purposes, as mandated by government, or under legislative requirements.

As the custodian of IRE, the Canadian Council of Motor Transport Administrators (CCMTA) ensures that it meets the following member needs:

- Operates in a private network, not the Internet, and is active in real time
- Delivers secure transmission of driver and vehicle data from jurisdiction to jurisdiction

- Maintains an audit capability to determine if there is any change that may constitute a breach of security
- Provides member jurisdictions, vehicle manufacturers, and other road safety-focused clients access within agreed-upon parameters by CCMTA members

### *Motor Vehicles System*

The Motor Vehicles System (MOVES) is the Alberta provincial database housing all information relating to motor vehicles registration and driver licensing. Access to MOVES is restricted to select Government of Alberta (GoA) employees and Alberta registry agent personnel as well as agencies that have been granted access through an *Access to Motor Vehicle Information Regulation* (AMVIR) Agreement with the GoA.

Under AMVIR, those that require access to driving and motor vehicle information maintained in the Office of the Registrar of Motor Vehicles Services (Registrar) must apply and may be approved to enter into an AMVIR Agreement with the Registrar. Access to personal information through an agreement may be obtained by any qualified organization in Canada. Access to nonpersonal information through an agreement may be obtained by any qualified organization anywhere in the world.

### *Insurance Bureau of Canada Vehicle Identification Number Verify Service*

The VIN Verify Service allows a user to check a VIN online to determine whether that vehicle has been reported as non-repairable as a result of flood damage. The database has been compiled by IBC and its member insurance companies. There is no cost to conduct a VIN search.

### *CPIC Online Vehicle Identification Number Search for Public*

Motor vehicle VINs—including those for snowmobiles, farm vehicles, trailers, and all-terrain vehicles—can all be searched on this free public database to see if the item has been reported stolen. As well, serially numbered property such as bicycles can be checked through this website to determine if they have been entered onto CPIC by a Canadian police jurisdiction. There are daily updates for vehicle data and weekly updates on property information.

[www.cpic.ca](http://www.cpic.ca)

### *Saskatchewan Government Insurance Vehicle Identification Number Search*

This is a free service that provides the status of a vehicle; its most recent Saskatchewan registration expiry date; its damage claims history in Saskatchewan since Nov. 1, 2002; and whether the

Saskatchewan provincial sales tax is payable. The results only include claims paid under Saskatchewan Government Insurance's Auto Fund license plate insurance and does not provide information about any inspection requirements or check to see if a vehicle has been reported stolen in other Canadian jurisdictions.

[https://www.sgi.sk.ca/online\\_services/vin/](https://www.sgi.sk.ca/online_services/vin/)

### *Insurance Corporation of British Columbia Vehicle Claims History Report*

This is a no-cost online service for looking up the status assigned to a vehicle on British Columbia's vehicle registry. A person searching is able to determine whether a vehicle is registered as normal, rebuilt, salvage, altered, or nonrepairable. A VIN and model year are required.

<https://onlinebusiness.icbc.com/vdwqs/VDWQSServlet/WelcomeAction>

## Chapter 6 Review and Assessment

The investigative unit should conduct an annual assessment to determine success with respect to its mission and goals. Findings should be documented in a written annual report and shared with management, stakeholders, and policymakers. Reviews should address all areas of the investigative unit and should measure whether cases are worked properly, timely, and thoroughly. Additionally, management should conduct periodic assessments to ensure that the direction of the unit is in alignment with the mission and goals of the agency.

The unit review should include:

- Legislative, policy, and regulatory review to ensure information is up to date, accurate, and relevant

- Workload assessment, including a caseload vs. staffing review
- Review of current training and development of staff, resources, and equipment
- Feedback from both internal and external stakeholders

The annual report should include recommendations on any changes to processes, laws, policies, or other changes being recommended by the investigative unit. Inclusion of statistics and performance measures should also be included.

## Chapter 7 Awards and Recognition

An employee recognition program can help improve agency efficiency and effectiveness by using awards to motivate individuals to use their knowledge, talents, and abilities to excel in their jobs. The program should be designed to fairly and equitably recognize and reward individuals for excellence in fulfilling the agency's mission of combating fraud. Recognition can be either formal or informal. Formal initiatives can be put in place on a periodic basis, with informal recognition taking place when it is merited.

Employees or teams who make contributions toward the goals of the unit, whether it is sustained distinguished service to the unit or a specific instance of exemplary work, should be recognized. Recognition should be provided 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 lookout for instances of fraud or for weaknesses in the process and increase the likelihood of identifying fraud. Group recognition contributes to team building and informs the group that together, they are valuable to the organization.

The steps below may be beneficial to revising or creating an employee recognition program.

### Create an Employee Recognition Committee

The purpose of the committee is to develop and implement a recognition program and should consist of both managers and employees. Having support from both groups will help ensure the success of the

program. The committee will determine what types of awards and recognition employees will receive based on the goals, priorities, and values of the unit. The committee will be responsible for determining how employee nomination and selections are made. Committee members may serve for fixed periods of time, such as one or two years, but provisions should be in place to avoid electing all new members at the same time to maintain continuity and institutional knowledge. Recognition may be in the form of defined awards, including leadership, creativity and innovation, teamwork, and excellence in an investigation.

Awards should be meaningful and relevant to the award recipient(s). Recognition can be given formally or informally and may include the following.

- Challenge coin
- Flexible work hours
- Compensatory time off
- Reserved parking
- Relaxed dress code
- Commendation letter
- Equipment or clothing perks
- Bonus or cash incentive
- Reception or luncheon
- Investigative team member (investigator, support staff, and so on) of the month or year
- Press release or story in agency newsletter
- AAMVA award

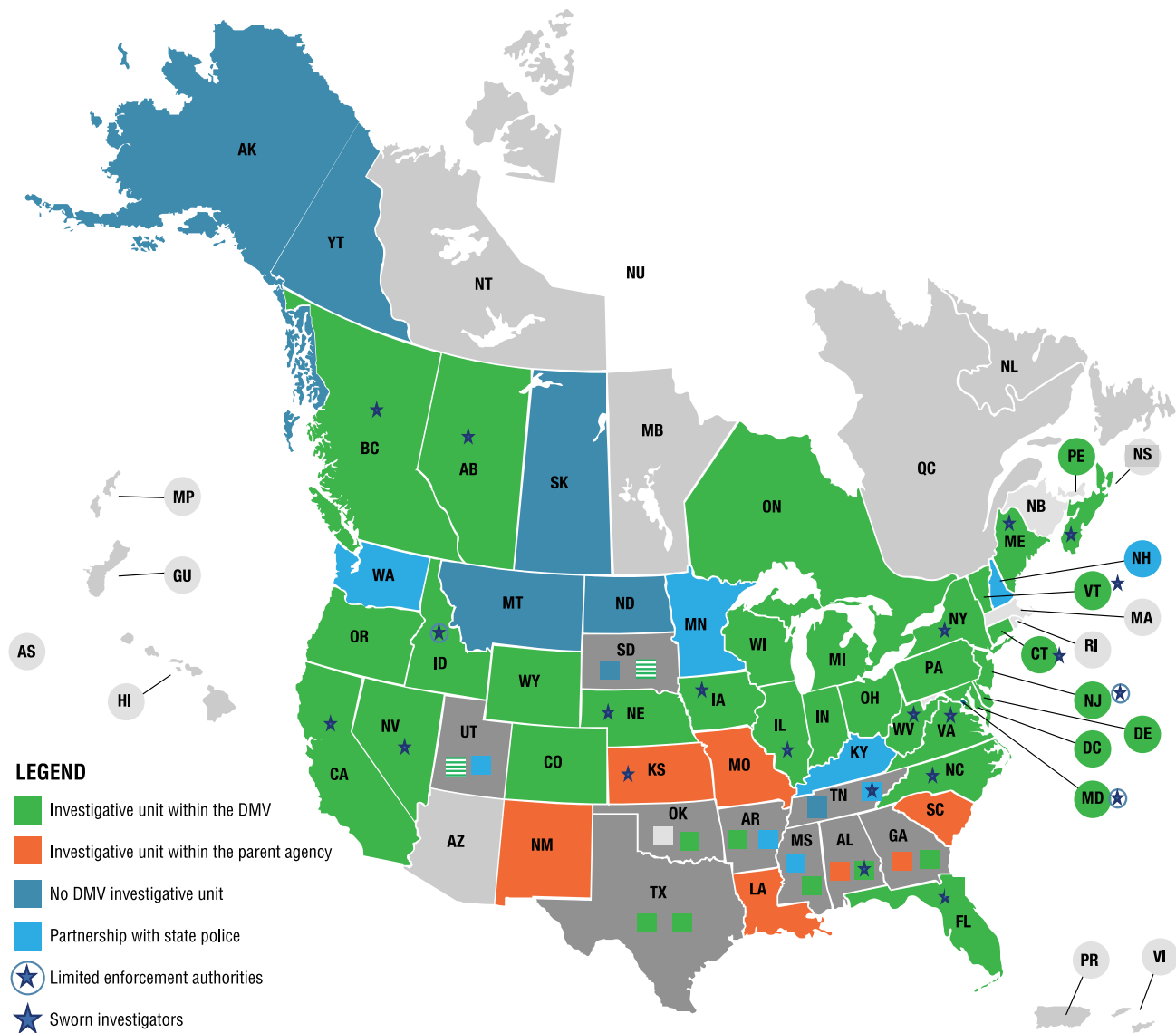
The recognition committee will be responsible for advertising the recognition program to ensure all employees are aware of it, the process of nomination, award categories, deadlines for nomination, and

when award selections will be made. This can be done via employee email, supervisor meetings, department website, or bulletin boards.



# Appendix A Survey

The Working Group completed a survey in April of 2016 via AAMVA's web survey tool to gather information on the make-up of jurisdictional investigative units. Below are a map and overview table summarizing survey results followed by complete survey results.



## Survey Overview

Jurisdiction	# of Licensed Drivers	Agency Where Fraud Unit Resides	# of Investigators	Sworn/Nonsworn Investigators	# of Responsibilities	# of Tools Used
Alberta		DMV	30	16/14	9	10
Alabama (DL)	1,887,023	No	6	0	4	5
Alabama (vehicles)	1,887,023	Yes	1	5	5	10
Alaska	250,745	LE	LE	0/6	10	13
British Columbia		DMV	14	6/8	5	9
California	12,562,214	DMV	370	198/172	9	17
Colorado	1,986,768	DMV	9	0/9	8	16
Connecticut	1,254,209	DMV	12	8/4	7	13
Delaware	356,242	DMV	6	0/6	9	13
D.C.	205,433	DMV	Unknown	0/Unknown	9	9
Florida	6,801,601	DMV	83	36/47	9	13
Georgia	3,154,117	DLD	24	0/24	6	12
Idaho	566,663	DMV	11	8*/3	3	11
Illinois	4,117,722	DMV	76+	53/23	10	22
Indiana	2,183,871	DMV	13	0/13	5	12
Iowa	1,103,271	DMV	20	17/3	11	23
Kansas	99,818	DOR/Agency	12	4/8	8	18
Kentucky	1,481,935	State Police	SP	Unknown	4	12
Louisiana	1,595,750	DPS/Agency	SP	Unknown	5	12
Maine	503,693	DMV	4	10	8	17
Maryland	2,038,539	DMV	44	35*/9	8	14
Michigan	3,448,100	DMV	16	0/16	9	13
Minnesota	1,686,830	DPS/Agency	SP	0	0	1
Mississippi (DL)	938,995	DLD	2	2	4	5
Mississippi (veh)	938,995	LE	0	0	0	7
Missouri	2,103,429	DOR/Agency	5	0/5	8	15
Montana	390,536	None	0	0/2	6	6
Nebraska	693,692	DMV	7	¾	9	17
Nevada	918,198	DMV	68	30/38	9	16
New Hampshire	537,483	DOS/Agency	101	Unknown	8	19
New Jersey	3,020,014	DMV	154	0/101	9	22
New Mexico	720,178	DOR/Agency	8	0/4	7	11
New York	5,806,337	DMV	154	100/54	9	22
North Carolina	3,404,244	DMV	297	158/139	11	22
North Dakota	273,542	No	0	0/0	0	0
Ohio	3,835,277	DMV	38	0/38	5	15
Oklahoma (DL)	1,135,024	DLD	3	0/3	9	10
Ontario		DMV	14	0/14	9	3
Oregon	1,376,809	DMV	6	0/6	5	11
Pennsylvania	4,425,045	DMV	20	0/20	10	14
Prince Edward Island		DMV	1	7	10	12
Saskatchewan		No	0	0	0	0
South Carolina	1,737,987	DMV	2	0/2	7	7
South Dakota (DL)	307,326	DPS/Agency	SP	0/0	1	8
South Dakota (veh)	307,326	No	0	0/0	2	7
Tennessee	2,216,142	DOS & HS/Agency	47	12/18	7	9

continued

Survey Overview (continued)

Jurisdiction	# of Licensed Drivers	Agency Where Fraud Unit Resides	# of Investigators	Sworn/Nonsworn Investigators	# of Responsibilities	# of Tools Used
Texas (DL)	7,714,337	DPS/Agency	SP	Unknown	7	3
Texas (vehicle)	7,714,337	DMV	25	0/26	0	11
Utah (vehicle)	716,585	DOR/Agency	7	30	7	12
Vermont	217,795	DMV	16	4/12	10	21
Virginia	2,809,780	DMV	114	57/57	7	22
Washington	2,790,748	DMV	21	0/21	3	10
West Virginia	582,047	DMV	8	21	20	17
Wisconsin	2,096,328	DMV	9	0/9	7	14
Wyoming	217,481	DMV	Unknown	Unknown	6	15
Yukon			0	0	0	0

1. Do you have an investigative unit within the DMV? If no, how do you handle fraud and administrative / criminal investigations?					
Jurisdiction	Yes	Comments	No	Comments	
Alberta	Yes	Alberta has two Special Investigations Units—one for the northern and one for the southern parts of our province. Our investigators are sworn Peace Officers with Criminal Code of Canada powers of investigation, arrest and charge.			
Alabama (DL)			No	The department has a criminal investigations unit. The state bureau of investigations also conducts criminal investigations.	
Alabama (V)	Yes	We have a civilian Fraud Investigative Tech at our HQs and (4) four sworn plain clothes investigators who work throughout the state. The sworn investigative fraud, obtain warrants as needed, and make arrest. They prepare individual case files for each case. The Tech does photo validation, support the investigators, assist in preparing files, and basically assist as needed with reviewing files.			
Alaska			No	Investigations are handled through the Directors office or forwarded to the Alaska Department of Public Safety/ Alaska State Troopers or other relevant LE agency.	
Arkansas	Yes	Arkansas uses facial recognition (FR) to detect fraud in issuance of driver's licenses and identification cards. If fraud is suspected by the FR unit, then AR has an administrative process and the issuance is set up for an administrative hearing. If the hearing officer determines fraud, then the license is cancelled and the incident may be turned over to the Arkansas State Police for further investigation.			
British Columbia	Yes				
California	Yes				
Colorado	Yes				
Connecticut	Yes				
Delaware	Yes	Unit established in 2006			
District of Columbia	Yes				
Florida	Yes	The Department of Highway Safety and Motor Vehicles (DHSMV) has both sworn and non-sworn employees that make-up our investigative unit. There are non-sworn members that handle the administrative side of the fraud investigations dealing with driver license and motor vehicle fraud. Once their administrative investigation is complete, the case is then forwarded to the Florida Highway Patrol (FHP) Bureau of Criminal Investigations and Intelligence (BCII) to begin the criminal investigation. The FHP BCII has a large group of criminal analysts who begin the criminal investigation and gather as much intel on the case as possible. Once the criminal analysts conclude their portion of the investigation, it is then sent to field and assigned to a sworn law enforcement investigator.			
Georgia	Yes				

(continued)

(continued)

1. Do you have an investigative unit within the DMV? If no, how do you handle fraud and administrative / criminal investigations?				
Jurisdiction	Yes	Comments	No	Comments
Idaho	Yes	Idaho has “motor vehicle investigators” which are commissioned, limited law enforcement authority staff. They deal with Idaho’s licensed dealers, salesman, unlicensed dealers, and consumer complaints. They have citation authority for title laws and dealer licensing laws. For internal fraud or felony investigations, Idaho would work the appropriate law enforcement agency. The investigators also work with county prosecutors and local law enforcement.		
Illinois	Yes			
Indiana	Yes			
Iowa	Yes			
Kansas			No	KS Department of Revenue’s Office of Special Investigations resides outside of the DMV because the unit also conducts investigations for the division of Taxation and other business units within Revenue.
Kentucky			No	Suspected fraudulent documents are referred to either the Kentucky State Police or to the Office of Inspector General.
Louisiana	Yes	This unit falls under the entire Department of Public Safety		
Maine	Yes			
Maryland	Yes			
Michigan	Yes			
Minnesota			No	Minnesota Driver and Vehicle Services does not have an investigative unit and in cases involving fraud or criminal investigations would rely upon the Minnesota State Patrol Vehicle Crimes Unit for assistance. Internally cases of fraud are investigated by the Internal Affairs department of the Department of Public Safety.
Mississippi (DL)	Yes			
Mississippi (V)			No	We do not have “in-house” investigators. If we suspect fraud or other criminal activity, we contact the MS Bureau of Investigations and/or other local law enforcement agencies depending on specifics of the incident.
Missouri	Yes			
Montana			No	We do have an individual (me) that follows up on any suspected fraud. We just lack the resources to be proactive.
Nebraska	Yes			
Nevada	Yes			
New Hampshire			No	There is a unit within N.H. State Police, Troop G that handles criminal and administrative investigations for the DMV
New Jersey	Yes	New Jersey Motor Vehicle Commission (MVC) maintains a Security and Investigations Unit of approximately 52 civil investigators (no law enforcement authority) The MVC also maintains an Internal Audit Unit consisting of 5 auditors. MVC formally partners via MOU with the NJ Division of Criminal Justice MVC Crimes Unit and the New Jersey State Police Interstate Theft North and South Units to handle the bulk of criminal matters related to MVC fraud, etc.		

(continued)

(continued)

1. Do you have an investigative unit within the DMV? If no, how do you handle fraud and administrative / criminal investigations?				
Jurisdiction	Yes	Comments	No	Comments
New Mexico	Yes	NM MVD has a multi-prong approach to detecting and investigating fraud and pursuing appropriate administrative or criminal investigations: * Through the use of facial recognition, we are able to identify individuals who may be committing identity theft or who have misrepresented themselves. There is a work unit within MVD that conducts these facial recognition reviews and conducts interviews. Depending upon the level of the infraction, cases result in either administrative action or are referred to the Tax Fraud Investigation Division (TFID) of our parent agency, the Taxation & Revenue Department. * The MVD Dealer Licensing Bureau has an investigator who provides compliance monitoring and complaint investigation for all new and used auto dealers, as well as auto recyclers. The investigator works closely with TFID and local law enforcement to take appropriate administrative and criminal action. * The MVD CDL unit conducts audits of 3rd party testers. It also reviews for compliance all CDL issuance transactions. When necessary, the CDL unit works closely with TFID, local law enforcement and FMCSA to take appropriate administrative or criminal action. * When other types of potential fraud or impropriety are suspected, the MVD management teams conducts an initial review/investigation. When deemed necessary and appropriate, a referral is made to TFID for a full investigation. * TFID works closely with federal, state and local law enforcement when necessary to conduct investigations or to refer cases to the appropriate law enforcement agency, the results of which may result in administrative and/or criminal penalties		
New York	Yes			
North Carolina	Yes			
North Dakota			No	North Dakota does have not an investigative unit referenced in the survey. Investigations would be conducted using available systems and personnel. The review could be completed internally with operations personnel, or Audit Services personnel, or an outside fraud investigator or forensic accountant could be hired to assist with the review.
Ohio	Yes			
Oklahoma DPS	Yes			
Ontario	Yes	Ministry of Transportation, Service Delivery Partnerships Branch (SDPB), Fraud Prevention and Business Integrity Office (FPBIO)		
Oregon	Yes			
Pennsylvania	Yes			
Prince Edward Island	Yes	Investigation functions within audit and quality control measures.		
Saskatchewan	No	We have a Special Investigation Unit within our Claims Division that we use from time to time. We are in the process of implementing Facial Recognition and determining how the fraud cases will be handled (i.e. if we will be using our SIU or have the FR staff deal directly with law enforcement). We do not believe we have enough volumes to warrant a dedicated investigative unit at this time.		
South Carolina	Yes	Any allegations involving suspected illegal activity by employees or customers are forwarded to the South Carolina Law Enforcement Division (SLED) for criminal investigation and prosecution. Any administrative investigations of the same subject matter are held in abeyance until the conclusion/prosecution of the criminal investigation. Administrative investigations involving employee misconduct or violations of departmental policies and/or procedures are investigated by an two person Internal Affairs Unit and adjudicated in accordance with the department's disciplinary policy		
South Dakota DPS (Drivers)			No	We don't have a special unit. Fraud is investigated by supervisors and reported to the Director. After all possible checks have been run the info/documents are turned over to law enforcement. An administrative person or an examiner reviews the facial recognition cases and refers any legitimate cases to the South Dakota Fusion Center.

(continued)

(continued)

1. Do you have an investigative unit within the DMV? If no, how do you handle fraud and administrative / criminal investigations?				
Jurisdiction	Yes	Comments	No	Comments
South Dakota DOR (vehicles)			No	
Tennessee (DOSHS)			No	TDOSHS is comprised of three division: The Office of Homeland Security (OHS), Tennessee Highway Patrol (THP), and Driver Services. The Special Investigations Bureau (Identity Crimes Unit) within the Tennessee Highway Patrol handles all fraud and criminal investigations related to Driver Services.
Tennessee (THP)	Yes	Criminal Investigation Division and Identity Crimes Unit		
Texas DPS	Yes			
Texas DMV	Yes			
Utah (veh)	Yes	Motor Vehicle Enforcement Division handles all fraud, Administrative and Criminal Investigations for the State Of Utah. The DMV and MVED are both under the Utah State Tax Commission, but we are separate.		
Vermont	Yes	Our Investigation Unit also has an Education unit		
Virginia	Yes			
Washington	Yes	Administrative actions are initiated by the investigators who work directly with law enforcement, county prosecutors, to pursue criminal matters		
West Virginia	Yes			
Wisconsin	Yes			
Wyoming	Yes			
Yukon			No	Information is brought to Motor Vehicles supervisory/management staff (Manager, and Supervisor, Client Services), a preliminary investigation is undertaken, and a decision is made as to whether to pass to the RCMP for further investigation.

2. Please describe the organizational make-up of the unit. Check the box for the type of staff in the unit and provide the number of staff in each position in the comments box.								
Jurisdiction	Managers/ Supervisors	Sworn Investigators	Nonsworn Investigators	Analysts	Administrative Support Staff	Auditors	Forensic Accountants	Other
Alberta	In our north office we have 16 members. Our south office has a few less. Both offices also have Document and Facial Recognition Investigators who conduct all FR related reviews as well as the forensic examination of all out of country driving licences surrendered to the AB government for exemption to our Graduated Driver Licence GDL Program.	In our north office we have 16 members. Our south office has a few less. Both offices also have Document and Facial Recognition Investigators who conduct all FR related reviews as well as the forensic examination of all out of country driving licences surrendered to the AB government for exemption to our Graduated Driver Licence GDL Program.			In our north office we have 16 members. Our south office has a few less. Both offices also have Document and Facial Recognition Investigators who conduct all FR related reviews as well as the forensic examination of all out of country driving licences surrendered to the AB government for exemption to our Graduated Driver Licence GDL Program.			
Alabama (DL)	2	0						
Alabama (V)	Sgt. Or Lt.	4	1	0	0	0	0	

(continued)

(continued)

2. Please describe the organizational make-up of the unit. Check the box for the type of staff in the unit and provide the number of staff in each position in the comments box.								
Jurisdiction	Managers/ Supervisors	Sworn Investigators	Nonsworn Investigators	Analysts	Administrative Support Staff	Auditors	Forensic Accountants	Other
Alaska	Deputy Director		5		1			
Arkansas	Yes (see response to #1)			Yes (see response to #1)	Yes (see response to #1)			
British Columbia	3	6	4	When required	1	When required		1 research assistant
California	45 includes sworn	198	18	26	77	0	6 are sworn inv.	
Colorado	1 Chief of Investigations 1 Supervisory Criminal Investigator II 5 Criminal Investigator I's 1 Compliance Investigator I 1 Administrative Assistant II	The State does not recognize the peace officer status of investigators in the CO DMV however most of the investigators have extensive law enforcement background and worked as full time sworn officers prior to coming to the DMV investigations unit						
Connecticut	1 sworn LT 1 sworn sgt 2 sworn inspectors (fraud, employee backgrounds) 2 sworn inspectors – auto theft, junk/salvage investigators 2 sworn inspectors – dealer investigations			4 civilian analysts / MV agenda (dealer consumer complaints)				
Delaware	1 Chief of Unit		5 investigators					
Dist rict of Columbia			Yes					
Florida	20	36	6	15	6			
Georgia	17				7			
Idaho	3	8						
Illinois	13	53		10	Numerous			
Indiana	3		7		3			
Iowa	2	17		1 (also provides admin support)				1 investigative intern
Kansas	1	4	2	3	1	1		
Louisiana	Investigators under State Police. Internal audit system under Management and Finance. CDL auditors within OMV All of these entities work separately and together.							
Maine	1 manager (sworn) 3 supervisors (sworn)	7						

(continued)

(continued)

2. Please describe the organizational make-up of the unit. Check the box for the type of staff in the unit and provide the number of staff in each position in the comments box.								
Jurisdiction	Managers/Supervisors	Sworn Investigators	Nonsworn Investigators	Analysts	Administrative Support Staff	Auditors	Forensic Accountants	Other
Maryland	9	35 (arrest powers on MVA properties)			12			1 security liaison (CCTV and PROX readers)
Michigan	4		4	3	5			
Minnesota	0	0	0	0	0	0	0	
Mississippi (DL)		2						
Mississippi (V)	0	0	0	0	0	0	0	0
Missouri						5 (Internal Audit Unit)		
Montana	1	0	0	0	0	1	0	0
Nebraska	1 manager (chief investigator) 1 analyst supervisor	3		2				
Nevada	17	30	14	2	5			
New Hampshire	Yes							
New Jersey 101 total	1 director 3 managers 6 supervising investigators		53 5 part-time 12 temp/ part-time	11	5	4		1 unit coordinator
New Mexico	4				3	1		3 compliance officers
New York	24	100			30			
North Carolina	43 (sworn) 1 Director 1 Deputy Director 2 Asst. Director 9 Supervisors 30 Assistant Supervisors 5 non-sworn managers	158 inspectors	63 civilian inspectors	16	17			2 Training, 8 Notice & Storage, 6 Dealer, 9 Inspections
North Dakota	0	0	0	0	0	0	0	
Ohio	7		30		1			6 investigator assistants (dealer inspectors)
Oklahoma DPS	1		1		1			
Ontario	3			10	1			4 fraud screeners
Oregon	1	None	2	1	1	1	None	
Pennsylvania	2		6		9	3		
Prince Edward Island	1	5 (role is within additional duties)	2					

(continued)



(continued)

2. Please describe the organizational make-up of the unit. Check the box for the type of staff in the unit and provide the number of staff in each position in the comments box.								
Jurisdiction	Managers/ Supervisors	Sworn Investigators	Nonsworn Investigators	Analysts	Administrative Support Staff	Auditors	Forensic Accountants	Other
Saskatchewan	NA at this time							
South Carolina			2 (1 also supervises)					
South Dakota DPS (driver)								
SD DMV (vehicles)	6	0 in DMV directly		2	0 in DMV directly	0 in DMV directly	1	42
Tennessee (TDOSHS)	5	12	0	2	1			
Tennessee (THP)	1 Major, 1 Captain, 4 Lieutenants	16	N/A	N/A	5	N/A	N/A	N/A
Texas DPS								
Texas DMV	3	None	21	None	1	None	None	N/A
Utah (veh)	7	21	1	1	7	0	0	
Vermont	3	4	8	0	2	0	0	
Virginia	12 managers (11 sworn) 15 supervisors (14 sworn)	57		4	12	14		
Washington	3		15		3			
West Virginia	8 Combination of both Investigative & Dealer	0	6	1	4	10		
Wisconsin	2		7			7		
Wyoming	x		x		x			

3. What are responsibilities of the investigative unit? Please check all that apply.												
Jurisdiction	Background checks for internal staff/third parties	Legislative/internal process review or audit	Review or audit of external entities/processes	Internal fraud invest.	External fraud invest.	Identity theft invest.	Facial recognition matches	Auto theft invest.	Dealer/salesman licensing invest.	Vehicle safety and emissions inspections	Junk/salvage dealer(s) invest.	Other(s)
Alberta	X	x	x	x		x	x	x	x		x	
Alabama (DL)	x			x	X	x						External investigations are primarily tax investigations
Alabama (V)				X	X	X	X		X			
Alaska	X	X	X	X	X	X	X	X	X	X	Alaska	X
Arkansas		x		x		x	x					These questions are answered for the Office of Driver Services, not for the Office of Motor Vehicle. The Arkansas State Police conducts motor vehicle fraud investigations.
British Columbia				x	x	x	x	x				
California	X	X	X	X	X	X		X	X		X	Participate on various task forces, local, state and federal
Colorado		x	x	x	x	x	x			x	x	
Connecticut	x			x	x	x		x	x		x	
D.C.		x	x	x	x	x	x	x		x	x	
Delaware	X		X	X	X	X	X	X	X		X	

(continued)

(continued)

3. What are responsibilities of the investigative unit? Please check all that apply.												
Jurisdiction	Background checks for internal staff/third parties	Legislative/internal process review or audit	Review or audit of external entities/processes	Internal fraud invest.	External fraud invest.	Identity theft invest.	Facial recognition matches	Auto theft invest.	Dealer/salesman licensing invest.	Vehicle safety and emissions inspections	Junk/salvage dealer(s) invest.	Other(s)
Florida			x	x	x	x	x	x	x	x	x	Cargo theft, organized crime, terrorism, threats, burglaries, vandalism, odometer fraud, title fraud, VIN fraud, sex assaults, non-traffic related death investigations, missing and endangered persons investigations, domestic violence, credit card fraud
Georgia	x	X		x	x	x	x					Employee credentialing, emergency management, undercover license issuance, Federal, State, and Local law enforcement assists with DDS information, photos, SMEs, Lawful Status reviews, internal affairs investigations
Idaho			x						x		x	The investigators primarily ensure that licensed dealers are following Idaho code, and administrative rules. For newly licensed dealers, the investigators work with them to ensure they have received appropriate education on the requirements, to help them avoid problems and be successful. Investigators inspect dealer's place of business, records, dealer plate usage, temporary registration, salesman licenses, and audit records on a periodic basis or as needed for cause. Investigators help identify vehicles, and VIN#'s as requested by law enforcement, or for titling issues for customers. They research and help resolve consumer complaints against dealers. Using whatever means available, the investigators will work unlicensed dealer cases, and write citations. They work with prosecutors on criminal charges, and provide expert testimony at trials.
Illinois	x	x	x	x	x	x	x	x	x		x	Our investigative unit is engaged in traffic safety, truck registration violations, school bus safety, investigation of unlicensed driver schools, new and used car dealer inspections. We are also the investigative branch for all other crimes involving the inappropriate use of notaries, the Illinois Seal, as well as crimes committed in SOS facilities.
Indiana	x			x	x	x	x					
Iowa	x	x	x	x	x	x	x	x	x	x	x	NMVTIS Facility security and security training. Fraud and salvage vehicle inspection training Processing and investigating applicants for UC DL's
Kansas	x	x		x	x	x	x		x		x	
Kentucky				x	x	x	x	x				
Louisiana	x	x	x	x	x	x		x	x	x	x	
Maine	x		x	x	x	x		x	x		x	Branch office incident investigation and prosecution Critical Incident management/training dealer training
Maryland	x		x	x	x	x		x	x		x	Tag and Title services (3rd party vendor) inspections
Michigan	x		x	x	x	x	x	x	x		x	There is a Separate Division within the Office of Investigative Services that conduct the review/audit of external entities; dealer licensing/salvage vehicle oversight. This area is the Regulatory Monitoring Division. This Division works hand-in-hand with the Enforcement Division on fraud related incidents.
Minnesota												
Mississippi (DL)				x	x	x	x					
Mississippi (V)												
Missouri			x	x	x	x	x		x	x	x	Facial recognition matches: Yes/No—Missouri no longer has facial recognition program due to legislation Other: Excise tax (cigarette & dyed off-road fuel)

(continued)

(continued)

3. What are responsibilities of the investigative unit? Please check all that apply.												
Jurisdiction	Background checks for internal staff/third parties	Legislative/internal process review or audit	Review or audit of external entities/processes	Internal fraud invest.	External fraud invest.	Identity theft invest.	Facial recognition matches	Auto theft invest.	Dealer/salesman licensing invest.	Vehicle safety and emissions inspections	Junk/salvage dealer(s) invest.	Other(s)
Montana				X	X	X	X		X		X	Dealer and vehicle investigation unit is a separate unit
Nebraska	x		x	x	x	x	x	x	x		x	Training Odometer Fraud Use Tax Fraud VIN and Odometer Inspections Title Fraud Threat Assessments
Nevada	X	X		X	X	X	X	X	X		X	
New Hampshire				x	x	x		x				
New Jersey	x	x	x	x	x	x	x	x				All criminal matters are developed to a point where criminal probable cause is either reached or clearly expected and then a transfer of the matter is coordinated with our law enforcement partners. The MVC maintains a Business Licensing Services Unit that investigates fraud and misconduct related to New and Used Car Dealer, Driving Schools, Auto Body Shops, and Interlock Device Installers,
New Mexico		x	x	x		x	x	x	x			The roles of each unit are described in greater detail in responses to earlier survey questions.
New York	x	x	x	x	x	x	x	x			x	
North Carolina	x	x	x	x	x	x	x	x	x	x	x	Antique and Custom Vehicle Classification Inspections Vehicle Identification Exams Heavy Equipment Investigations
North Dakota												
Ohio			x	x	x	x	x	x	x		x	Medical restriction case review, internal and external training, fraudulent acts regarding certificates of motor vehicle title, odometer fraud, partial hit/ analytical research
Oklahoma DPS	x		x		x	x	x					
Ontario	x	x		x	x	x	x	x	x	x		
Oregon		x		x	x	x	x					
Pennsylvania		x	x	x	x	x	x	x	x	x	x	
Prince Edward Island		X	X	X	X	X	X	X	X	X	x	
Saskatchewan												
South Carolina		x		x	x	x		x	x		x	One investigator is assigned with the issuance of covert credentials to various law enforcement entities
South Dakota DPS (drivers)							x					
South Dakota DMV (vehicles)								X	X			
Tennessee (TDOSHS)	X			X	X	X	X					
Tennessee HP	X	X		X		X		X	X		X	
Texas DPS												
Texas DMV									X		X	Education Provided to Licensee's
Utah (vehicle)	X	X		X	x			X	x		x	
Vermont	X	X	X	X	X	X	X	X	X	X		
Virginia	x		x	x		x		x	x		x	Passenger and property carrier enforcement, external law enforcement support, contract security, IFTA, IRP and Fuel tax audits and enforcement.
Washington					x	x	x					
West Virginia	X	X	X	X	X	X	X	X	X		X	

(continued)

(continued)

3. What are responsibilities of the investigative unit? Please check all that apply.												
Jurisdiction	Background checks for internal staff/third parties	Legislative/internal process review or audit	Review or audit of external entities/processes	Internal fraud invest.	External fraud invest.	Identity theft invest.	Facial recognition matches	Auto theft invest.	Dealer/salesman licensing invest.	Vehicle safety and emissions inspections	Junk/salvage dealer(s) invest.	Other(s)
Wisconsin		x	x	x	x	x	x	x				
Wyoming		x			x	X		X	x		x	Taxi and rental vehicle companies

4. Which of the following investigative tools do you use?											
Jurisdiction	Case/record management systems	Third-party portals or databases	Verification systems	Third-party systems	Data mining tools	Other state/federal systems	Facial recognition system	Social media sites	Social media mining software	Search engines	Other tools
Alberta	x	NLETS AAMVA's FAS NCIC		Craigslist Carfax	x		X	X		x	
Alabama (DL)	x	NCIC		Experian/LN/ Polk				x		x	
Alabama (V)	X	NCIC CJIS	VLS/SAVE Digital image exchange	NADA		X	X	X		X	
Alaska		NMVTIS NLETS AAMVA's FAS	SSOLV Digital Image Exchange	Carfax Experian/LN/ Polk NADA NICB Craigslist, eBay		x	x			x	
Arkansas	x	AAMVA's FAS NMVTIS	SSOLV VLS/SAVE	Experian/LN/ Polk			x			x	Arkansas will begin using the State to State Verification System by June 4, 2016, and the U.S. Passport Verification system starting October 1, 2016.
British Columbia		AAMVA's FAS NCIC		Craigslist/ eBay	x	x	x	x	x	x	ICBC also uses CPIC (Canadian Police Information Centre)
California	x	RISS NMVTIS NCIC CJIS NLETS	SSOLV VLS / SAVE	Carfax Experian/LN/ Polk TLO CLEAR NICB Craigslist/ eBay	X	X				x	

(continued)

(continued)

4. Which of the following investigative tools do you use?											
Jurisdiction	Case/record management systems	Third-party portals or databases	Verification systems	Third-party systems	Data mining tools	Other state/federal systems	Facial recognition system	Social media sites	Social media mining software	Search engines	Other tools
Colorado		AAMVAs FAS CJIS NCIC NMVTIS NLETS	SSOLV	TLO NCIB Craigslist/ eBay Carfax	x	x	x	x	x	x	Accurant Lexis Nexis Colorado Courts CCIC
Connecticut	x	NMVTIS NCIC NLETS	SSOLV VLS/SAVE	TLO NICB Carfax NADA		x	x			x	
Delaware	x	NMVTIS (LEAT) NCIC CJIS NLETS AAMVA's FAS	SSOLV VLS / SAVE	Carfax Experian/LN/ Polk Craigslist/ eBay			x Morphotrust	x Facebook			
D.C.	x			Experian/LN/ Polk Carfax NADA		x	x	x	x	x	
Florida	x	AAMVA's FAS NCIC CJIS NLETS NMVTIS		Carfax TLO NICB Craigslist/ eBay			x	x		x	
Georgia	x	CJIS NLETS NCIC	VLS/SAVE SSOLV	CLEAR Craigslist/ eBay Experian/LN/ Polk			x	x		x	We use Spillman Technologies as our case management system.
Idaho	x	NLETS NMVTIS NCIC		Autocheck Craigslist/ eBay Experian/LN/ Polk NADA Carfax NICB		x					The investigators will use whatever resources are available. We wish we had more, but cost can be an issue.

(continued)

(continued)

4. Which of the following investigative tools do you use?											
Jurisdiction	Case/record management systems	Third-party portals or databases	Verification systems	Third-party systems	Data mining tools	Other state/federal systems	Facial recognition system	Social media sites	Social media mining software	Search engines	Other tools
Illinois	x	AAMVA's FAS CJIS NMVTIS NCIC NLETS	VLS/SAVE digital image exchange SSOLV EVVE	Craigslist/ eBay Carfax NADA TLO Autocheck NICB Experian/LN/ Polk	x	x	x	x		x	
Indiana	x	AAMVA's FAS NMVTIS	SSOLV digital image exchange	NADA Autocheck CLEAR Carfax NICB				x		x	
Iowa	x	NMVTIS NLETS CJIS AAMVA's FAS NCIC RISS	VLS/SAVE SSOLV	Craigslist/ eBay Hamari Carfax Experian/LN/ Polk NADA NICB Autocheck CLEAR	x	x	x	x	x	x	
Kansas		NLETS AAMVA's FAS NMVTIS NCIC CJIS RISS	SSOLV EVVE	Craigslist/ eBay TLO Carfax NICB HAMARI Experian/LN/ Polk		x	x	x		x	
Kentucky	x	NCIC NLETS NMVTIS	digital image exchange SSOLV	NICB Carfax NADA		x	x	x			
Louisiana	X	NCIC CJIS AAMVA's FAS NMVTIS	VLS/SAVE SSOLV EVVE	NADA Autocheck NICB Carfax Experian/LN/ Polk		x		x		x	
Maine	x	NMVTIS RISS CJIS NLETS NCIC	VLS/SAVE digital image exchange SSOLV	NICB Carfax NADA Autocheck TLO	x	x				x	

(continued)

(continued)

4. Which of the following investigative tools do you use?											
Jurisdiction	Case/record management systems	Third-party portals or databases	Verification systems	Third-party systems	Data mining tools	Other state/federal systems	Facial recognition system	Social media sites	Social media mining software	Search engines	Other tools
Maryland	x	AAMVA's FAS NCIC CJIS RISS NMVTIS NLETS	SSOLV	TLO Carfax NICB Craigslist/ eBay				x		x	
Michigan		NCIC NMVTIS CJIS NLETS	AAMVA's FAS	Craigslist/ eBay NADA TLO Carfax	x		x	x		x	
Minnesota							x				
Mississippi (DL)	X	NLETS NCIC	VLS/SAVE				x				
Mississippi (V)		NCIC AAMVA's FAS		Autocheck Carfax Experian/LN/ Polk NADA NICB							
Missouri	x	RISS AAMVA's FAS NMVTIS NLETS NCIC CJIS		NADA TLO Craigslist/ eBay Carfax NICB		x		x		x	
Montana		NMVTIS NLETS AAMVA's FAS	SSOLV VLS / SAVE	.			x				
Nebraska	x	NMVTIS NLETS NCIC AAMVA's FAS CJIS	VLS/SAVE digital image exchange	NADA Carfax TLO Hamari NICB		x	x	x	x		NFIN—Nebraska Fusion Information Network Nebraska Secretary of State Business/ Corporation Database
Nevada	x	RISS NMVTIS NCIC CJIS NLETS	SSOLV VLS / SAVE	Carfax Experian/LN/ Polk CLEAR Craigslist/ eBay		x	x	x		x	

(continued)

(continued)

4. Which of the following investigative tools do you use?											
Jurisdiction	Case/record management systems	Third-party portals or databases	Verification systems	Third-party systems	Data mining tools	Other state/federal systems	Facial recognition system	Social media sites	Social media mining software	Search engines	Other tools
New Hampshire	x	NLETS NCIC NMVTIS		NICB Craigslist/ eBay Carfax		x				x	x
New Jersey	x	CJIS NLETS NMVTIS NCIC AAMVA's FAS	SSOLV VLS/SAVE	Carfax NICB skip tracing sys Experian/LN/ Polk Craigslist/ eBay Autocheck	x	x	x	x		x	
New Mexico		NLETS NCIC NMVTIS	EVVE SSOLV	Experian/LN/ Polk Autocheck NADA NICB Carfax			x				
New York	x	NMVTIS NLETS RISS CJIS NCIC AAMVA's FAS	SSOLV VLS/SAVE	NADA Carfax NICB Experian/LN/ Polk Craigslist/ eBay CLEAR Autocheck	x	x	x	x	x	x	HSIN, we have an internal case tracking system for Auto Related cases and a second system for tracking cases related to Identity/License cases. We utilize Forensic Document Examination tools.
North Carolina	x	NCIC RISS NMVTIS NLETS CJIS RISS	SSOLV	Carfax NADA Craigslist/ eBay TLO Hamari NICB Autocheck Craigslist/ eBay	x	x	x	x	x	x	CJLEADS
North Dakota											
Ohio	x	NLETS RISS NCIC CJIS AAMVA's FAS	SSOLV	Craigslist/ eBay NICB Carfax TLO		x	x	x		x	

(continued)



(continued)

4. Which of the following investigative tools do you use?											
Jurisdiction	Case/record management systems	Third-party portals or databases	Verification systems	Third-party systems	Data mining tools	Other state/federal systems	Facial recognition system	Social media sites	Social media mining software	Search engines	Other tools
Oklahoma	x	AAMVA's FAS NCIC NLETS CJIS	VLS/SAVE SSOLV				x	x		x	
Ontario	x			Carfax			x				MTO Database; LCS (Licencing Control System); ISS (Inquiry Services System)
Oregon	x	AAMVA's FAS	VLS / SAVE	Autocheck Experian/LN/ Polk NICB Craigslis, eBay,	X		X	X		X	
Pennsylvania	x	NCIC NMVTIS AAMVA's FAS	SSOLV digital image exchange	NADA Craigslis/ eBay Carfax NICB		x	x	x		x	
Prince Edward Island	X	AAMVA's FAS IBC – Insurance Bureau of Canada RIV – Registrar of Imported Motor Vehicles	Digital Image Exchange IRE – InterProvincial Record Exchange	Autocheck Carfax Experian/ LN/ Polk NICB	X	X	X	X		x	
Saskatchewan											
South Carolina	x	NMVTIS		Carfax NICB Craigslis/ eBay			x	x			
South Dakota DPS (drivers)		NLETS	VLS/SAVE SSOLV digital image exchange			x	x	x		x	Any documentation found internally or through any sources is referred to law enforcement.
South Dakota DMV (vehicles)		NCIC NLETS		Carfax TLO NADA		x		X			

(continued)

(continued)

4. Which of the following investigative tools do you use?											
Jurisdiction	Case/record management systems	Third-party portals or databases	Verification systems	Third-party systems	Data mining tools	Other state/federal systems	Facial recognition system	Social media sites	Social media mining software	Search engines	Other tools
Tennessee (TDOSHS)	x	RISS NCIC CJIS NLETS		Carfax Experian/LN/ Polk CLEAR NICB Craigslis/ eBay	X	X	X	X	X	x	THP—Identity Crimes Unit
Tennessee (THP)	X	NCIC CJIS NLETS		Carfax TLO CLEAR NICB Craigslis/ eBay		X					
Texas DPS		NLETS	SSOLV VLS/SAVE Digital image exchange			X	X	x			
Texas DMV	x	NMVTIS		Autocheck Carfax Experian/LN/ Polk NADA NICB Craigslis / eBay		X		X		x	
Utah (veh)	X	RISS NCIC CJIS NLETS	VLS/SAVE	Autocheck Carfax Experian/LN/ Polk NICB				X		x	
Vermont	x	RISS NMVTIS NCIC CJIS NLETS AAMVA's FAS	SSOLV VLS / SAVE Digital Image Exchange	Autocheck Carfax Experian/LN/ Polk HARMARI NADA NICB Craigslis, eBay,		X	X	X		X	
Virginia  Virginia, continued	x	RISS CJIS NMVTIS NLETS NCIC AAMVA's FAS	SSOLV EVVE VLS/SAVE digital image exchange	NICB TLO Hamari Craigslis/ eBay NADA Carfax		x		x	x	x	

(continued)

(continued)

4. Which of the following investigative tools do you use?											
Jurisdiction	Case/record management systems	Third-party portals or databases	Verification systems	Third-party systems	Data mining tools	Other state/federal systems	Facial recognition system	Social media sites	Social media mining software	Search engines	Other tools
Washington	x	AAMVA's FAS	digital image exchange SSOLV	TLO Craigslist/ eBay		x	x	x		x	
West Virginia	X	NMVTIS NCIC AAMVA FAS	SSOLV VLS/SAVE Digital Image Exchange EVVE	Autocheck Carfax Experian/LN/ Polk NADA NICB Craigslist/ eBay			X	X		x	Tax Department System. MSCA Dot Registration and update. MCMIS Portal to check DOT numbers. These systems are not normally used during investigations but could be depending on the nature of the incident.
Wisconsin	x	AAMVA's FAS NMVTIS	SSOLV	Craigslist/ eBay Carfax Experian/LN/ Polk CLEAR	x	x	x	x	x	x	x
Wyoming	x	NMVTIS RISS NLETS NCIC		NICB Experian/LN/ Polk NADA CLEAR Craigslist/ eBay Carfax Autocheck		x		x		x	

5. Do you allow state, local or federal law enforcement to access your facial recognition database?			
Jurisdiction	Yes	No	N/A
Alberta	We will assist LE for identified investigative files for "Investigational Purposes" only.		
Alabama (DL)			N/A
Alabama (V)	Request made to our Investigative Tech		
Arizona	Yes, through the FR unit. They do not have direct access.		
Alaska		X	
British Columbia	Only when a Court Order has been provided.		
California			X
Colorado		Not directly. Agencies complete a request form and the request is assigned to an investigator.	

(continued)

(continued)

5. Do you allow state, local or federal law enforcement to access your facial recognition database?			
Jurisdiction	Yes	No	N/A
Connecticut		No direct access to law enforcement. Assistance provided on a case-by-case request basis.	
Delaware		We do not allow direct access but our law allows the unit to share info upon requests by LE, Courts or other DMV's.	
D.C.	Yes		
Florida		No. The process is called the Florida Driver License – Biometric Identification Operating System – Facial Recognition System (FDL-BIOS-FRS) DHSMV also utilizes the Pinellas County Sheriff's Office Facial Recognition Software (FACES)	
Georgia		Not direct access, but we will query information and provide said information to LE agencies.	
Iowa	State Dept. of Public Safety has access to run images through the FR system.		
Idaho	Law enforcement is permitted to receive information and photos, and at the state level have access.		
Illinois		No. We conduct the inquiries on their behalf.	
Indiana	Yes, we provide investigative assistance to any requesting criminal justice agency. They must provide a criminal predicate to receive information. The Indiana Intelligence Fusion Center (IIFC) is the only agency outside the BMV provided with direct access to FRS.		
Kansas		Not directly. We run queries for them.	
Kentucky	Yes, but we only allow the Kentucky State Police to access our facial recognition database.		
Louisiana			We do not have a facial recognition system.
Maine			not applicable
Maryland			We currently do not have a facial recognition database
Michigan			The Facial Recognition database/program is managed by the Michigan State Police
Minnesota		No – unless accompanied by a subpoena	
Mississippi (DL)			
Mississippi (V)			N/A. DPS handles driver licensing
Missouri		No, for security reasons.	N/A
Montana		No	
Nebraska	Yes, direct access on a limited basis. Offer matching services to all law enforcement agencies.		
Nevada		X	
New Hampshire			We don't have facial recognition.

(continued)

(continued)

5. Do you allow state, local or federal law enforcement to access your facial recognition database?			
Jurisdiction	Yes	No	N/A
New Jersey		No. If an entity makes an inquiry of the MVC which would require uploading a foreign image via the MVC FR system, the requesting entity would have to provide credible facts to suggest an objective likelihood or suspicion that the person depicted in the subject image could be maintaining a false identification in the MVC system. This the limited, defining criteria/threshold that must be met before an image will be approved by MVC to be uploaded against the MVC photo image repository. This rule is the result of express deliberation between the MVC Chief Administrator and the NJ Attorney General. Further, when such an upload occurs/is approved, it is executed by and under the strictly under command and control of the MVC FR Center staff. Remote access is never granted to a 3rd party.	
New Mexico		At this time, no.	
New York		No. We work with them on our cases but no outside parties have access to our FR system.	
North Carolina	Yes, on site visits to the ID Fraud Labs		
North Dakota	State patrol and Bureau of Criminal Investigation may access Driver's License photos and system information.		
Ohio			State and federal law enforcement access the Ohio Attorney General's gateway to facial recognition which is not administered or maintained by the Ohio BMV.
Oklahoma		The requesting agency must request, in writing on agency letterhead, to the Commissioner of DPS who will approve IVU to issue. We also use finger imaging along with facial recognition. The agency must have a court order to get the finger image.	
Ontario		No	
Oregon		x	
Pennsylvania	Yes		
Prince Edward Island		x	
Saskatchewan		No, we will not provide any external access to our FR database. When provided with a court ordered document, we will conduct a search on a photo provided by law enforcement on their behalf.	
South Carolina	Yes, the State Law Enforcement Division (SLED).		
South Dakota DPS (drivers)		No, although we are looking at the possibility.	
Tennessee (DOSHS)		No	
Tennessee (THP)		X	
Texas DPS		No – All request for Facial Recognition are sent to the Supervisor of the Record Verification section via email and the results are provided via email to the requesting Agency.	
Texas DMV			N/
Utah (veh)			X. FR program in DLD agency
Vermont		X – They contact us and fill out a form and we do the search for them	
Virginia			No answer - unknown

(continued)

(continued)

5. Do you allow state, local or federal law enforcement to access your facial recognition database?			
Jurisdiction	Yes	No	N/A
Washington		No, prohibited by statute (RCW 46.20.037), however they may access non-facial recognition system photos	
West Virginia	x		
Wisconsin Wisconsin, continued		No, currently we conduct searches for the state DOJ and other federal entities and respond with results. However, we are planning to allow with limited access our WI DOJ Fusion Center to use our tool.	
Wyoming	WYDOT allows access to any official law enforcement agency.		

6. Please provide a telephone number (non-public if available) for the investigative unit or appropriate entity that investigators from other DMVs can use to contact your office?		
Jurisdiction	Contact	Phone Number
Alberta	Darren Hodson	780-441-2000
Alabama (DL)	James Starling	334-242-3015
Alabama (V)	Maria Sledge	334-242-1476
Alaska	Directors Office	907-269-5559
Arkansas	Tonie Shields	501-682-7061 or Tonie.Shields@dfa.arkansas.gov
British Columbia	Ben Shotton, Manager of DL Integrity and Oversight	250-414-7804
California	Chief Frank Alvarez	916-657-8377
Colorado	Supervisor Darin Icardi	303-205-5768 (Darin) 303-205-5959 is the 24-hour Communication Center Line 303-205-8383 is direct to Investigations
Connecticut	James Rio	860-263-5343
Delaware	Kenneth Shock, Chief Compliance/Investigations Unit	Office: 302-857-5727; cell: 302-242-2491
District of Columbia	Tiara Graham	202-727-2200
Florida	Lt. Jacquelyn Hollis Captain Randy Head	813-558-1818 850-617-2361
Georgia	Richard Miller	Iowa
Idaho	Daryl Marler, MVI/Dealer Licensing Supervisor	208-334-8684 or Daryl.Marler@itd.idaho.gov
Illinois	IL SOS Investigations Main #	217-782-7126
Indiana	Fraud & Security Enforcement Division	Phone: 317 234-3501; fax: 317 233-3203 FSE@bmv.in.gov
Iowa	Tina Lewis	515-237-3279
Kansas	Dean Reynoldson	785-296-4194
Kentucky	Paula Freeman Jana Sanchez	502-564-0501 502-564-9900 ext. 4215
Maryland	Nirmala Harry	410-768-7074 or 410-768-7218
Maine	Everett Kaherl	207-624-9257
Michigan	Darryl Hill, Office of Investigative Services Director Peggy Hines, Enforcement Division Director	517-373-3657 517-241-6802
Minnesota	Lt. Ryan Carrol, Minnesota State Patrol Vehicle Crimes Unit	763-279-4002
Mississippi (DL)	Lt. Walker	601-987-1279
Mississippi (V)	Tony Lawler	601-923-7636
Missouri	DOR Compliance & Investigation Bureau	573-526-1525
Montana	Patrick McJannet, Driver Services Deputy Bureau Chief	pmcjannet@mt.gov or 406 444-2001
Nebraska	Betty Johnson	402-471-3790
Nevada	Louis Lanuza	775-684-4682
New Hampshire	N.H. State Police Troop G	03305 603-223-8778

(continued)

(continued)

6. Please provide a telephone number (non-public if available) for the investigative unit or appropriate entity that investigators from other DMVs can use to contact your office?		
Jurisdiction	Contact	Phone Number
New Jersey	Tom Flarity	609-984-5279 or 609-633-7189
New Mexico	MVD Director's Office	505-827-2296
New York	Owen McShane	518-474-8805
North Carolina		
North Dakota		
Ohio	Mark Hoy Russell Rauch	614-752-4885 614-752-4885
Oklahoma	Brenda Mays, Director Identity Verification Unit	405-425-7380
Ontario		verificationMTO@Ontario.ca
Oregon	Jihesheia Hull	503-945-5141
Pennsylvania	Brent Lawson	717-705-9913
Prince Edward Island	Graham Miner	902-368-5255
Saskatchewan	Brandy Bray	306-751-1568
South Carolina	Main Number Senior Investigator Rick Steen Investigator Kevin Worley	803-896-9688 (Main) 803-896-9686 (Steen) 803-896-8131 (Worley)
South Dakota DPS (drivers)	Arin Diedrich Jane Schrank	605-773-6390 (Diedrich) 605-773-4123 (Schrank)
South Dakota DMV (vehicles)	Monica Weischedel, Deputy Director	605-773-3501
Tennessee (THP Identity Crimes Unit)	Lieutenant Roy Brown	Office: 615-687-2351; cell: 615-476-9514
Tennessee (THP)	Lieutenant Dan E. Moore	731-668-9644
Texas DPS	Sara Sandoval	512-424-2245
Texas DMV	David A. George Jr. Chief Investigator DMV Enforcement— Motor Vehicle	512-465-4147 david.george@txdmv.gov
Utah (veh)	Allan Shinney	801-297-2606
Vermont	Kathy Codling	802-828-2067 or email: DMV-Enforcement@vermont.gov
Virginia	N/A	
Washington		fraud@dol.wa.gov (monitored weekdays 7:00 am–5:00pm Pacific time) Message phone: 360-902-3915
West Virginia	Kenneth Cassidy (Investigations) or Mike Maggard (Dealer Investigators)	Investigations: 304-926-3954; dealer investigations: 304-926-3840/3870
Wisconsin	Susan Schliz, Compliance, Audit & Fraud Unit Supervisor	608-267-4524
Wyoming	Robert Stauffacher	307-777-3815

## Appendix B Federal Resources

The following are resources DMV investigators may use.

**Department of Homeland Security (DHS):** DHS's work includes customs, border, and immigration enforcement; emergency response to natural and human-made disasters; antiterrorism work; and cybersecurity. <https://www.dhs.gov>

- **Citizenship and Immigration Services (USCIS):** The U.S. Citizenship and Immigration Services is responsible for processing immigration and naturalization applications and establishing policies regarding immigration services. <https://www.uscis.gov/>
- **Customs and Border Protection (CBP):** CBP prevents people from entering the country illegally or bringing anything harmful or illegal into the United States. <https://www.cbp.gov>
- **Department of Homeland Security/U.S. Immigration and Customs Enforcement (ICE):** Protects America from cross-border crime and illegal immigration that threaten national security and public safety. <https://www.ice.gov>
- **Citizenship and Immigration Services/Systematic Alien Verification for Entitlements Program (SAVE):** <https://www.uscis.gov/save>

**Department of Justice (DOJ):** The DOJ works to enforce federal law to seek just punishment for the guilty and to ensure the fair and impartial administration of justice. <https://www.justice.gov>

- **DOJ Office of U.S. Attorneys (USAO):** The United States Attorneys have three statutory responsibilities under Title 28, Section 547 of the United States Code: the prosecution of criminal cases brought by the federal government, the prosecution and defense of civil cases in which the United States is a party, and the collection of debts owed the federal government that are administratively uncollectible. <https://www.justice.gov/usao>
- **DOJ U.S. Marshalls Service (USMS):** The USMS enforces federal laws, apprehends criminals, exercises custody of federal prisoners and provides for their security and transportation to correctional facilities, executes federal court orders, seizes assets gained by illegal means and providing for the custody, management, and disposal of forfeited assets, assures the safety of endangered government witnesses and their families, and collects and disburses funds. <https://www.usmarshals.gov>
- **DOJ Office of Inspector General (OIG):** The OIG has jurisdiction to review the programs and personnel of the Federal Bureau of Investigation; Drug Enforcement Administration; Federal Bureau of Prisons; U.S. Marshalls Service; Bureau of Alcohol, Tobacco, Firearms and Explosives; United States Attorneys; and all other organizations in the department. <https://oig.justice.gov/index.html>



- **DOJ Office of Attorney General (OAG):** The OAG supervises and directs the administration and operation of the Department of Justice, including the Federal Bureau of Investigation; Drug Enforcement Administration; Bureau of Alcohol, Tobacco, Firearms and Explosives; Bureau of Prisons; Office of Justice Programs; and the U.S. Attorneys and U.S. Marshals Service. <https://www.justice.gov/ag>
- **DOJ Federal Bureau of Investigation (FBI):** The FBI protects and defends the United States against terrorist and foreign intelligence threats; upholds and enforces the criminal laws of the United States; and provides leadership and criminal justice services to federal, state, municipal, and international agencies and partners. <https://www.fbi.gov/>
  - National Criminal Information Center (NCIC): NCIC is a computerized index of criminal justice information (i.e., criminal record history information, fugitives, stolen properties, missing persons). It is available to federal, state, and local law enforcement and other criminal justice agencies and is operational 24 hours a day, 365 days a year. <https://www.fbi.gov/services/cjis/ncic>
  - FBI Criminal Justice Information Service (CJIS): CJIS provides a range of tools and services to law enforcement, national security and intelligence community partners, and the general public. <https://www.fbi.gov/services/cjis>
  - FBI Criminal Justice Information Service/Law Enforcement Enterprise Portal (CJIS LEEP): LEEP is an electronic gateway that provides law enforcement agencies, intelligence partners, and criminal justice entities with centralized access to many different resources and services. <https://www.fbi.gov/services/cjis/leep>
- **National Motor Vehicle Titling Information System (NMVTIS):** <http://www.vehiclehistory.gov/index.html>
  - National Motor Vehicle Titling Information System – Law Enforcement (NMVTIS): [http://www.vehiclehistory.gov/nmvtis\\_law\\_enforcement.html](http://www.vehiclehistory.gov/nmvtis_law_enforcement.html)

**Department of State/Diplomatic Security Service (DOS DS):** The Bureau of Diplomatic Security is the security and law enforcement arm of the U.S. Department of State. <http://www.state.gov/m/ds>

- U.S. Department of State/Office to Monitor and Combat Trafficking in Persons (USDOS TIP): <http://www.state.gov/j/tip>

**Federal Motor Carrier Safety Administration (FMCSA):** <https://www.fmcsa.dot.gov>

**Federal Trade Commission (FTC):** <https://www.ftc.gov> or <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>

**Grants.gov:** Provides a unified site for interaction between **grant** applicants and the U.S. federal agencies that manage **grant** funds. <http://www.grants.gov/web/grants/home.html>

**Internal Revenue Service (IRS):** The IRS administers and enforces U.S. federal tax laws. <https://www.irs.gov>

**National Association for Public Health Statistics and Information Systems (NAPHSIS/EVVE):** Verification of birth and death information. <http://www.naphsis.org>

**National Highway Traffic Safety Administration:** The NHTSA investigates safety defects in motor vehicles, sets and enforces fuel economy standards, investigates odometer fraud, establishes and enforces vehicle antitheft regulations, and provides consumer information on motor vehicle safety topics. <http://www.nhtsa.gov>

**Regional Information Sharing Systems (RISS):** RISS provides services and resources that directly impact law enforcement's ability to successfully resolve criminal investigations and prosecute offenders while providing the critical officer safety event deconfliction necessary to keep the men and women of our law enforcement community safe. <https://www.riss.net>

- **Western States Information Network (WSIN):** Serving Alaska, California, Hawaii, Oregon, and Washington, as well as Canada, Guam, and New Zealand. <https://www.riss.net/Centers/WSIN>
- **Rocky Mountain Information Network (RMIN):** Serving Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, and Wyoming, as well as parts of Canada. <https://www.riss.net/Centers/RMIN>
- **Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLN):** Serving Delaware, Indiana, Maryland, Michigan, New Jersey, New York, Ohio, Pennsylvania, and the District of Columbia, as well as Australia, Canada, and England. <https://www.riss.net/Centers/MAGLOCLN>
- **Mid-States Organized Crime Information Center (MOCIC):** Serving Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, and Wisconsin, as well as parts of Canada. <https://www.riss.net/Centers/MOCIC>
- **New England State Police Information Network (NESPIN):** Serving Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont, as well as parts of Canada. <https://www.riss.net/Centers/NESPIN>
- **Regional Organized Crime Information Center (ROCIC):** Serving Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, and West Virginia, as well as Puerto Rico and the U.S. Virgin Islands. <https://www.riss.net/Centers/ROCIC>

**U.S. Postal Service (USPS):** <https://www.usps.com/>

- **US Postal Inspection Service:** The U.S. Postal Inspection Service supports and protects the USPS and its employees, infrastructure, and customers; enforces the laws that defend the nation's mail system from illegal or dangerous use; and ensures public trust in the mail. <https://postalinspectors.uspis.gov>

**U.S. Secret Service:** <http://www.secretservice.gov/investigation>

**United States Social Security Administration (SSA):** The SSA assigns social security numbers; administers the retirement, survivors, and disability insurance programs known as Social Security; and administers the Supplemental Security Income program for the aged, blind, and disabled. <https://www.ssa.gov>

- **Office of Inspector General/Social Security Administration: Investigations (SSA OIG OI):** The Office of Investigations (OI) conducts and coordinates investigative activity related to fraud, waste, abuse, and mismanagement in Social Security Administration programs and operations. This office serves as OIG's liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. The OI also conducts joint investigations with other federal, state, and local law enforcement agencies. <https://oig.ssa.gov/about-oig/offices/office-investigations>

## Appendix C Working Group Roster

### CHAIR

**Mark Silk**, *Senior Detective*  
Maine Bureau of Motor Vehicles  
[mark.silk@maine.gov](mailto:mark.silk@maine.gov)

### VICE CHAIR

**John Clawson**, *Director of Fraud & Security Enforcement Division*  
Indiana Bureau of Motor Vehicles  
[jclawson@bmv.in.gov](mailto:jclawson@bmv.in.gov)

### BOARD ADVISOR

**Rhonda Lahm**, *Director*  
Nebraska Department of Motor Vehicles  
[Rhonda.Lahm@nebraska.gov](mailto:Rhonda.Lahm@nebraska.gov)

### REGION I REPRESENTATIVES

**Eric Danz**, *Manager*  
Investigative Security Services  
Maryland Motor Vehicle Administration  
[edanz@mva.maryland.gov](mailto:edanz@mva.maryland.gov)

**Brent Lawson**, *Director for Risk Management*  
Pennsylvania Department of Transportation  
[blawson@pa.gov](mailto:blawson@pa.gov)

**Major Christopher Grotton**  
Maine State Police  
[christopher.grotton@maine.gov](mailto:christopher.grotton@maine.gov)

### REGION II REPRESENTATIVES

**Lieutenant Jason Daniel**  
North Carolina Division of Motor Vehicles  
[jwdaniel@ncdot.gov](mailto:jwdaniel@ncdot.gov)

**David George**, *Chief Investigator*  
Texas Department of Motor Vehicles  
[david.george@txdmv.gov](mailto:david.george@txdmv.gov)

**Kevin McCormack**, *Asst. Special Agent in Charge*  
Virginia Department of Motor Vehicles  
[kevin.mccormack@dmv.virginia.gov](mailto:kevin.mccormack@dmv.virginia.gov)

**Lieutenant Cora Gentry**  
Arkansas State Police  
[cora.gentry@asp.arkansas.gov](mailto:cora.gentry@asp.arkansas.gov)

### REGION III REPRESENTATIVES

**Chris Leeman**, *Investigator*  
Iowa Department of Transportation  
[christopher.leeman@dot.iowa.gov](mailto:christopher.leeman@dot.iowa.gov)

**Joseph Tieri**, *Investigator*  
Illinois Secretary of State Police  
[jtieri@ilsos.net](mailto:jtieri@ilsos.net)

## REGION IV REPRESENTATIVES

**Aaron Greene**, *Investigator 1*  
Washington Department of Licensing  
[agreene@dol.wa.gov](mailto:agreene@dol.wa.gov)

**Mike Leonard**, *Assistant Director*  
Service Alberta  
[mike.leonard@gov.ab.ca](mailto:mike.leonard@gov.ab.ca)

**Tom Edwards**, *Supervising Investigator I*  
California Department of Motor Vehicles  
[tom.edwards@dmv.ca.gov](mailto:tom.edwards@dmv.ca.gov)

**Trooper Detective Darrell Noyes**  
Washington State Patrol  
Criminal Investigation Unit, Special Investigations,  
Identity Theft Unit  
[darrell.noyes@wsp.wa.gov](mailto:darrell.noyes@wsp.wa.gov)

## AAMVA STAFF

**Brian Ursino**, *Director of Law Enforcement*  
Lead Staff Liaison  
AAMVA  
[bursino@aamva.org](mailto:bursino@aamva.org)

**Patrice Aasmo**, *Director of Member Support*  
AAMVA Regions I and II  
[paasmo@aamva.org](mailto:paasmo@aamva.org)

**Sheila Prior**, *Director of Member Support*  
AAMVA Regions III & IV  
[sprior@aamva.org](mailto:sprior@aamva.org)

**safe drivers  
safe vehicles  
secure identities  
saving lives!**



**American Association of Motor Vehicle Administrators**  
4401 Wilson Boulevard, Suite 700  
Arlington, Virginia 22203  
703.522.4200 | [aamva.org](http://aamva.org)