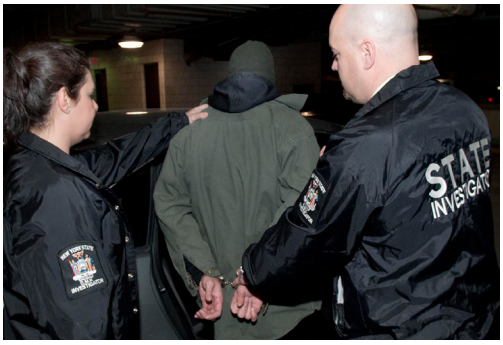
AAMVA

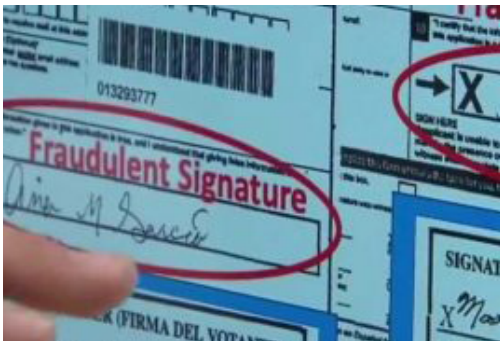
American Association of
Motor Vehicle Administrators

Security Integration
Law MISSION
Enforcement
Investigations
OPERATIONS
Guidance



MVA Investigative Unit Resource Guide

Edition 2



October 2022

MVA Investigator Working Group
Law Enforcement Standing Committee

Contents

Cover photos credit: iStockphoto.com

Executive Summary

The importance of fraud deterrence, detection, and remediation cannot be overstated. The motor vehicle administration (MVA) investigator role is therefore critical to the mission of each AAMVA member agency.

This MVA Investigative Unit Resource Guide (hereinafter referred to as the *Resource Guide*) is a product of the MVA Investigator Working Group (hereinafter referred to as the *Working Group*). There were two documents published in 2017, the *DMV Investigator Integration Strategies* and *DMV Investigative Unit Resource Guide*. A new working group was established to update and integrate these documents into this single *Resource Guide*.

This *Resource Guide* includes general organizational and operational principles and guidance for MVA investigative units based on the research, experiences, and practices of Working Group members and the agencies they represent. The *Resource Guide* can be used by MVA investigative units as a benchmark to improve current operations. Additionally, if an agency is planning to establish a new investigative unit, this resource can be used as a blueprint for building an effective fraud investigation 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 MVA investigator community.

NOTE: For purposes of this document, the term *motor vehicle administration (MVA)* is meant to be inclusive of all motor vehicle agencies that address driver licensing, identity management, and/or vehicle registration and titling that employ fraud investigators, either sworn or non-sworn.

Chapter 1 The Investigative Unit

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

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

MVAs are on the front lines of national security and identity protection, and the need is greater than ever to address fraud and other inappropriate activities by enhancing or creating functional, stand-alone investigative units. With a sufficiently staffed and properly equipped investigative unit, the MVA keeps an eye on critical identification processes. Investigative units can swiftly identify and address fraud problems and should have the authority to do so. The benefits of combating fraud and non-criminal policy violations far outweigh the cost. Only with the proper staffing, resources, and technologies in place can MVAs be successful in the ever-increasing challenge of fighting fraud.

The investigative unit will likely be tasked with conducting investigations related to employee and third-party administrator 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.

Beyond Investigations: Benefits of Having an Investigative Unit

In addition to handling investigations and addressing fraud challenges, investigators can provide valuable assistance in many other areas, including but not limited to:

- Analysis for proposed legislation
- Input to improve policies, processes, and training
- Education and training for front-line staff
- Identifying areas of vulnerability
- Assisting with internal audits
- Undercover testing (both internally and with third parties)
- Assisting with development and analysis of requests for proposals
- Insight into the overall design and security features of driver's licenses and identification cards (DLs/IDs)
- Sharing findings to improve MVA functionality
- Working with the information technology (IT) division to modernize existing databases and identifying elements that should be recorded and tracked

- Working with auditors to show potential vulnerabilities both inside and outside the organization
- Conducting background checks
- Establishing relationships with and educating prosecuting attorneys on MVA fraud. See AAMVA Resource, Successful Prosecutor Partnerships Whitepaper, Educational Slides, Handouts.
- Expert testimony on MVA-related cases
- Serving as a resource and provide training for outside law enforcement agencies, prosecutors, and/or Crown Counsel (Canada)
- Identifying fraudulent records to prevent titles and licenses from being issued to ineligible applicants
- Having access to intelligence briefings by other law enforcement agencies
- Employing document examination experts (identity credentials from other jurisdictions and countries)

Investigators can assist and provide valuable insight into the overall design and security features of DLs/IDs, title stock, license plates and vehicle registration stickers during the request for proposal/information (RFP/RFI) process. This insight can ensure vendor proposals adequately address areas of concern and potential problems are minimized. Obtaining input from 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.

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

MVAs should 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 MVA procedures, laws, systems, and processes	✓	✓	✓
Regular collaboration among fraud, audit, and other units	✓	✓	✓
Chief of investigative unit reports directly to MVA agency head	✓	✓	✓
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 MVA 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			✓
Experts in identifying forged and/or counterfeit documents			✓

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

The culture of the organization will change with the establishment of an investigative unit, and such change must be proactively managed. 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.

Responsibilities of the Investigative Unit

Agency administration should establish the investigative unit's roles and responsibilities to include the scope of investigations they conduct. The scope should consider the lifecycle of the investigation and whether the investigators are responsible for the investigation from its beginning to prosecution or if they will refer a case out to an allied law enforcement agency.

Both internal and external fraud should be considered when defining the responsibilities of the Investigative Unit. Investigative responsibilities may include:

- Facial recognition
- Title and odometer fraud
- Dealer regulations and compliance inspections
- Written and road driver testing fraud
- Driver license and other document fraud
- Identity theft
- Data privacy and misuse
- MVA tax and financial fraud
- Online transactions and digital fraud
- Dyed fuel investigations
- Salvage-rebuild inspections
- Salvage yard and tow and wrecking company inspections
- Lien-related fraud
- Monitor MVA tip lines
- Third-party services fraud (e.g., driving schools, registration services, vehicle inspections)

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. 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.

Staffing and Equipping an Investigative Unit

A crucial requirement in the fight against fraud is an appropriately sized and adequately equipped investigative unit. The appropriate size of the unit depends on the size of the MVA, 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 the responsibilities for which the unit is charged. Tracking performance and publicizing successes can help justify the unit and potential expansion. When analyzing the impact of new legislation or policies, consideration should always be given to the potential need for additional staff for the investigative unit to fulfill its responsibilities.

Investigator Qualifications and Authorities

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 law 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 some grants, data access, and reimbursements from federal and state agencies that non-sworn personnel are not.

Investigators with arrest authority may not have to rely on outside agencies to make an arrest (although coordination or deconfliction is recommended). Having the ability to make arrests assures cases will be handled in a more efficient manner because they are not dependent on other agency workloads or priorities.

Additionally, MVA 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, interview witnesses, develop confidential informants, transport and interview arrestees, and present investigative findings to prosecutors, grand juries, or Crown Counsel.

Support Staff Qualifications and Authority

Although investigators are critically important in the fight against fraud, they cannot do the job alone. Adequate support staff is a fundamental need for any good investigative team. Analysts, auditors, forensic accountants, IT forensic analysts, and document experts bring unique skills and 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 exist within the organization and 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.

Some benefits of having an adequate support staff include:

- Obtaining background information for investigators
- Providing investigative leads
- Conducting forensic analysis
- Identifying emerging trends
- Obtaining MVA records from other jurisdictions
- Running various database queries
- Developing reports that identify potential fraud
- Conducting audits

Staff should have access to sensitive or restricted data and social media to proactively identify fraud and assist with data mining. This access might include:

- MVA systems and databases
- External law enforcement databases
- Online marketplace websites
- Other agency intelligence reports
- Dark web
- Other government databases (e.g., vital statistics, immigration)

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

Investigative Unit Review and Assessment

If an investigative unit already exists within an MVA, it is important 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 MVA 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.

The investigative unit should conduct an annual assessment to measure 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
- Staff specialties in alignment with fraud trends

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 measure outcomes should also be included.

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. MVA administrators should appoint appropriate personnel to be responsible for

fraud matters and regularly meet with the director of the jurisdiction's public safety or state police agency to discuss how the agencies can partner in the deterrence and detection of fraud. Sharing information among agencies can provide insight into how MVA 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.

Chapter 2 Hiring and Retaining MVA Investigators

The success of an MVA investigative unit will largely depend on selecting and hiring individuals who have the required education and investigative experience. Ideally, investigators should have law enforcement experience, including specific experience in investigations that would augment the MVA investigative unit.

Job Descriptions

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

- Conducting investigations pertaining to imposter fraud, synthetic fraud, counterfeits and alterations, licensing, and regulation of businesses (e.g., dealers, vehicle safety and emissions inspections, third party service providers)
- Conducting investigations related to stolen vehicles, organized theft rings, Vehicle Identification Number (VIN) removals, and other auto-related crimes
- Conducting investigations relative to digital transactions and payments
- Conducting investigations related to internal fraud
- Making criminal arrests and initiating other enforcement action(s)
- Providing court or administrative hearing testimony
- Preparing comprehensive investigative case reports (this may include disseminating intelligence to the information fusion center)
- Inspecting rebuilt salvage vehicles and specially constructed vehicles
- Participating in impaired driving, underage drinking, and other traffic safety–related programs, if authorized to do so

Retaining the Team

For continuity and efficiency of operations, agencies should make every effort to retain experienced staff. The cost of training may be 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 overloading remaining personnel. Retention strategies may include:

- Competitive salary
- Positive work culture or environment
- Continuing education and training
- Professional development and advancement opportunities
- Employee recognition and reward
- Telecommuting opportunities
- Flexible work schedules
- Employee feedback and suggestion protocol
- Mentoring program

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.

Awards and Recognition

An employee recognition program can help improve morale and assist in retaining employees. The program should be designed to fairly and equitably recognize and reward individuals for excellence in fulfilling the unit's mission of combating fraud.

Employees or teams that 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 program should be designed to fairly and equitably recognize and reward individuals for excellence in fulfilling the unit's mission of combating fraud.

Chapter 3 Training

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

A variety of training delivery options can be offered by the agency, including but not limited to:

- New employee orientation or onboarding
- Basic law enforcement training (e.g., academy or Police Officer Standardized Training)
- In-service training
- On-the-job training (e.g., field training officer)
- Specific task–related training

AAMVA offers a variety of training tools to assist investigators. Training for investigative staff should include review of AAMVA best practices and training modules, including:

- **Fraud Detection and Remediation Training**

  AAMVA's Fraud Detection & Remediation (FDR) program is the industry's premier fraud training used by MVAs, law enforcement, federal agencies, and corporations worldwide. With training modules and supplements that develop skills in the authentication of more than 12 document categories—Imposter Fraud, Internal Fraud, Fraud for Managers/Administrators, and more—the FDR is the most comprehensive anti-fraud toolbox available. The modularized eLearning suite is critical to everyone handling secure documents or sensitive transactions and is applicable to all agency staff.

  For more information, visit the AAMVA's FDR website at AAMVA – Fraudulent Document Recognition Training.

- **Facial Recognition Best Practices**

  Customer privacy and the protection of personal information is paramount and should be consistent with the laws of the jurisdiction. Identity fraud and identity theft are continuing problems. Facial recognition is a fraud prevention, fraud detection, business integrity, and risk mitigation tool used by the majority of U.S. and Canadian MVAs.

  For information on facial recognition best practices, please visit Facial Recognition Program Best Practices.

- **Best Practices for the Deterrence and Detection of Fraud**

  MVAs are on the front lines of national security and identity protection. MVAs need to create environments that endorse ethics and encourage employees to do the right thing at every turn, making the perpetration of fraud as difficult as possible. The benefits of combating fraud far outweigh the cost. Only with the proper staffing, resources, and technologies in place can MVAs be successful in the ever-increasing challenge of fighting fraud.

  For information on deterrence and detection of fraud, please visit Deterrence and Detection of Fraud Best Practices (available only to AAMVA jurisdiction and federal members).

- **Best Practices for the Prevention of Abandoned Vehicle & Mechanic's-Lien Fraud**

  The processing of vehicle titles for abandoned and mechanic's lien vehicles by MVAs is an important responsibility, but unfortunately, it can be taken advantage of by individuals seeking to obtain financial benefits by deception. These vehicles can be nuisances to communities and consume considerable resources by those seeking to dispose of them. While conducting investigations involving suspected fraud in these applications, law enforcement and MVA investigators may be challenged by the lack of information in the title application as well as inadequate laws relating to enforcement, making successful investigations and prosecution difficult.

  For information on best practices for the prevention of abandoned vehicle and mechanic's lien fraud, please visit Best Practices for the Prevention of Abandoned Vehicle and Mechanic's Lien Fraud.

- **National Motor Vehicle Title Information System (NMVTIS) and the Law Enforcement Access Tool (LEAT)**

  NMVTIS is an electronic system designed to protect consumers from fraud and keep stolen vehicles from being resold. NMVTIS captures specific pieces of vehicle information from state motor vehicle titling agencies, automobile recyclers, junk and salvage yards, and insurance carriers into one system. The LEAT is intended to provide local, state, and federal law enforcement with the information necessary to investigate, deter, and prevent vehicle-related crimes.

  For further information on NMVTIS and the LEAT, including how to access this database, visit our website (https://www.aamva.org/vehicles/nmvtis/law-enforcement).

- **Attendance at AAMVA and other conferences or trainings that allows for networking with peers**

Chapter 4 Supporting Investigations Through Partnerships

Internal Partnerships

(Subsections listed under internal partnerships may be responsibilities that in some jurisdictions are the function of a different agency.)

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 can provide resources to assist with early deterrence and detection of fraud and bring prosecutions to successful outcomes.

Motor Vehicle Operations

The vehicle operations department is charged with maintenance of motor vehicle registration and title records that may be vital during 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 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.

The vehicle operations department is charged with maintenance of motor vehicle registration and title records that may be vital during an investigation.

Vehicle 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, 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 tax evasion. Many times, vehicle operations maintain the records, which are presented when the title or ownership record is changed.

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 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? 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?

Furthermore, as technology continues to evolve in the vehicle arena (advanced driver assistance systems and automated driver system–equipped vehicles; mileage-based user fee programs, and so on), MVA motor vehicle operations and investigative unit partnerships are critical to address fraud that may occur.

Vehicle Dealer and Business Licensing Operations

Vehicle dealer and business licensing operations is usually responsible for licensing of motor vehicle dealers, motor vehicle recyclers, motor vehicle demolishers, auto parts dealers, junk and salvage yards, and more depending on the jurisdiction.

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 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 vehicle 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 Identification Card Operations

DL/ID card operations is responsible for maintaining documents used in support of the issuance of DL and nondriver ID cards. In addition, many jurisdictions are making mobile drivers Licenses an option for their constituents. Contained within these documents (traditional or digital) 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, generally including vehicle titling, interstate registration, and interstate fee collection. Information they can provide for investigative purposes includes inter- and intrastate records on the following:

- CDL information
- Oversize or overweight permitting
- Trip permits
- Heavy vehicle use tax
- Fuel tax fraud
- International Registration Plan
- International Fuel Tax Agreement
- Taxicabs, transportation network companies, and other livery entities
- Fees and payment information

DL/ID card operations is responsible for maintaining documents used in support of the issuance of driver license and nondriver ID cards.

Field Operations and Third-Party Partners

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

Many field offices are equipped with cameras, electronic access controls, and other tracking systems that may be of use to the investigations unit. In cases of internal fraud, such records can be accessed to review the transactions of a particular clerk, determine office entry and exit dates and times, research electronic transactions, and 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 MVA 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. See Third-Party Agent Administration Best Practices.

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 entities to access their records when needed. The data are particularly helpful in determining vehicle information, ownership, odometer information, physical location, and presumed condition at the time of inspection. Records can be used for both audit and investigation purposes.

Information Technology

IT may be managed within the MVA 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 MVA investigators. At a minimum, IT departments may provide information related to the following:

- Employee or customer online transaction tracking
- Offline searches (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 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
- Alerts for abnormal or unusual transactions (e.g., after-hours activity, short road test times)

Human Resources

It is important to establish a positive working relationship with the agency's human resources (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.

Legal Services

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.

Public Information Office

Agency websites, social media platforms, and press releases may provide an effective way to inform and gather information from stakeholders These platforms 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.

External Partnerships

Forming partnerships with federal, state, provincial, and local agencies, as well as other stakeholders can provide value to the unit. Partners can bring resources, expertise, and database access the unit may not possess. Partners can also provide information on related cases or trends that may otherwise be missed. After the partnership has been established, discussions between the unit and its partners should take place on a regular basis.

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, and overtime are a few of the advantages such partnerships provide, including the ability to file federal charges. In addition, federal law enforcement agencies bring specialized expertise and can provide additional resources such as manpower and equipment to MVA investigations.

Federal agents frequently receive tips through confidential informants, federal prosecutors, and other law enforcement agencies regarding fraud schemes at MVAs and are often willing to work with MVA investigators to uncover and explore fraud schemes.

Some federal agencies have task forces dedicated to the investigation of identity and benefit fraud and other specific crimes relevant to MVA investigations. For many MVA investigative units, concerted efforts have been made to include MVA investigators on such task forces. The benefits of participation on federal task forces for the MVA include asset sharing, overtime pay for investigators, vehicle fleet usage, intelligence sharing, use of office space, and the ability to network

with numerous agencies daily. Asset sharing can be a significant inducement for working with federal agencies. Many federal investigations, including those related to MVA fraud, often result 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.

Department of Justice and Treasury Equitable Sharing

The U.S. Department of Justice and the U.S. Department of the Treasury offer equitable sharing programs for law enforcement who assist in federal investigations and prosecutions. Numerous MVA investigation units with sworn officers have obtained funds because of participation in criminal cases. The Department of Justice and the Department of the Treasury are two separate federal agencies with two separate forfeiture funds. The federal document *Guide to Equitable Sharing for State, Local and Tribal Law Enforcement Agencies* applies to both programs. The guide provides a program overview, permissible uses of the funds, and reporting and compliance information. Approved uses of the funds include training and education, operations and investigations expenses, equipment, computer upgrades, and many other law enforcement related purposes. This funding allows the investigation units to obtain needed equipment and training.

Partnerships with Fusion Centers

Fusion centers are composed of law enforcement personnel and analysts from a variety of federal, state, and local agencies. Their purpose is to share intelligence, correlate information, and identify threats. Fusion centers can also help identify connections between MVA fraud cases and other cases.

Other Governmental Agencies

There is significant value in establishing relationships with other governmental agencies as it relates to the deterrence and detection of fraud. Many branches of government may not be aware of the benefits partnering with MVA investigators can provide. Establishing these mutually beneficial relationships can greatly enhance the detection and prosecution of fraud. Examples of potential partnerships include:

- Health and human services agencies
- Secretary of State offices
- 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
- Department of Justice
- Vital statistics
- Immigration services
- Passport agencies
- Border enforcement agencies
- State and local prosecutors
- Office of Insurance Commissioner (or equivalent)

Memorandums of Understanding

Memorandums of understanding can be established and maintained between agencies exchanging information and providing access to service and data to ensure compliance with jurisdiction privacy laws.

Outreach and Education

Openly sharing information provides transparency and builds trust. Delivering an effective outreach and education program will educate, engage, and enable stakeholders to understand how MVA programs contribute to the integrity of the MVA.

Communication to and education of partners and other stakeholders will enhance the investigative unit's effectiveness, garner support, and increase the chance of successful prosecutions. It is critical the investigative unit create, promote, and foster an active program to educate and inform stakeholders 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.

Outreach may take the form of a high- 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.

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 MVA is mentioned as a party to the investigation.

Celebrate and Publicize Unit Successes

An effective outreach strategy involves not only the dissemination of information regarding available products and services but also an active effort to celebrate and publicize success. By publicizing successful investigations, the visibility and reputation of the investigative unit can be enhanced. Consumers will gain confidence in the ability of the unit and encourage the reporting of illegal activity. And criminal justice partners and policymakers will see the unit's effectiveness.

Chapter 5 Tools

Equipping the investigative unit with the tools necessary to conduct an effective investigation is just as important as having the proper skill sets. In addition to traditional law enforcement equipment, essential tools may include:

- Onboard diagnostic tools
- Black lights (ultraviolet light)
- Magnifiers
- Flashlights
- Binoculars
- Smartphones
- Audio and video recorders
- Barcode readers
- Still and video cameras
- 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 MVA 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.

Case Management

Effectively managing a caseload is difficult without a case management system. Such a system can maintain written reports, investigative findings, and other information deemed necessary. Investigators must 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.

A case management system provides the ability to retrieve facts about cases, both open and closed, and is a vital piece of the fraud management program. 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. These programs also serve as deconfliction tools to assist in avoiding duplication of case work and enhance officer safety.

Fraud Reporting Mechanism

Hotlines, emails, and other reporting mechanisms 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 facilitate the reporting of suspicious activity witnessed by anyone inside or outside the agency. 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. Determine if the reporting entity is willing to be a witness or 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.

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

Data Tools

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.

It is imperative for an MVA to establish information sharing, both internally and externally. Numerous databases are available, but it is important to identify sites containing reliable information. Listed in the table are several reliable databases made available to investigators to both gather and exchange information. (Readers unfamiliar with any of the tools in the table should access via the link to learn more.) Resources without links and those requiring further explanation are described in the table.

DRIVERS	VEHICLES	BOTH DRIVERS AND VEHICLES
• AAMVA Card Design Standard • AAMVA Secure Card Design Principals • Commercial Skills Test Information Management System (CSTIMS) • Commercial Driver License Information System (CDLIS) • Digital Image Access and Exchange (DIAE) • Driver License Data Verification Service (DLDV) • Electronic Verification of Vital Events (EVVE) • National Driver Register (NDR)/Problem Driver Pointer System (PDPS) • Social Security Online Verification (SSOLV) • State-to-State (S2S) Verification Service and Driver History Record (DHR) • U.S. Passport Verification Service (USPVS) • Verification of Lawful Status/Systematic Alien Verification for Entitlements (VLS/SAVE)	• National Motor Vehicle Title Information System (NMVTIS)/Law Enforcement Access Tool (LEAT) • National Insurance Crime Bureau Theft File (NCIB) • Insurance Claim Search • National Odometer and Title Fraud Enforcement Association (NOTFEA) • International Association of Auto Theft Investigators	• AAMVA Member Directory • AAMVA's Fraud Detection and Remediation Training Program (FDR) • International Public Safety & Justice Network (NLETS) • National White Collar Crime Center (NW3C) • Regional Information Sharing System (RISS) • AAMVA's Fraud Alert Site • Document ID databases and guides • Third-party data brokers

Document Identification Databases and Guides

Several organizations offer products and services that provide an electronic or printed guide to the credential specifics for DLs/IDs currently being issued by AAMVA members, as well as past versions of their documents. These tools provide a quick overview of the overt security features that can then be validated in the MVAs or at the roadside.

Fraud Alert Site

The AAMVA Fraud Alert Site was developed as a means of sharing document intelligence alerts issued by the Department of Homeland Security with driver licensing authorities. The Fraud Alert Site includes both United States and Canadian federal and jurisdictional and provincial alerts and updates, including vehicle alerts, lost or stolen materials and equipment, and document updates. The site provides

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

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

National Insurance Crime Bureau and Insurance Service Office

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 MVAs 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 Insurance Services Office 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. Building and maintaining a relationship with the jurisdiction's NICB supervisory special agent in charge is key in leveraging NICB resources to the fullest extent possible.

National Motor Vehicle Title Information System

The NMVTIS is a system that allows the titling agency to verify the information instantly and reliably on a paper title with the electronic data from the jurisdiction that issued the title. The 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.

MVA Investigator access to NMVTIS/LEAT is granted through either the Regional Information Sharing System (RISS) or the Law Enforcement Enterprise Portal (LEEP). For more information and LEAT access, visit our website (https://www.aamva.org/vehicles/nmvtis/law-enforcement).

Regional Information Sharing Systems

The RISS Program—*A Proven Resource for Law Enforcement*™—is a nationwide information-sharing and investigative support program that serves

thousands of local, state, federal, and tribal law enforcement and public safety agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, England, and New Zealand. Officers, analysts, and other criminal justice partners rely on RISS for its proven and secure information-sharing capabilities, as well as its professional, innovative, and critical investigative support services. RISS serves as a force multiplier, effectively and efficiently aiding agencies in tackling crime problems in their areas.

RISS consists of six regional centers as well as a technology support center. The six RISS Centers are:

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

Third-Party Data Brokers

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

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

Canadian Tools

Some of the many tools available to Canadian investigators are described in this section.

Canadian Police Information Centre

Much like the United States' 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 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 the 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 (https://justice.gov.bc.ca/cso) electronic court registry. Free online access allows a user to search criminal, civil or traffic courts by name, file number, or agency.

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 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 specific 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 who 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 the Insurance Bureau of Canada 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 in 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.

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 November 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.

Insurance Corporation of British Columbia Vehicle Claims History Report

This is a no-cost online serviceå for looking up the status assigned to a vehicle on British Columbia's vehicle registry (https://onlinebusiness.icbc.com/vdwqs/VDWQSServlet/WelcomeAction). 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.

Appendix A Strategies for Continued Integration of Motor Vehicle Administration Investigators into the AAMVA Community

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." *MVA Investigator Integration Strategies* was originally a standalone whitepaper. Significant progress has been made in integrating MVA Investigators into the AAMVA law enforcement discipline specifically since that time.

Following are three integration strategies and four recommendations. Some of the integration strategies recommended will require more resources than others; therefore, adoption and implementation will occur over time. The implementation of these strategies supports AAMVA's vision for "Safe Drivers, Safe Vehicles, Secure Identities, and Saving Lives."

Strategy 1 – MVA Investigator Recurring Fraud Awareness Calls

AAMVA has implemented recurring fraud awareness calls to engage MVA investigators throughout North America and to allow them to share best practices, challenges, and investigatory successes on a regular basis. In addition, these calls allow AAMVA members to learn about the most up-to-date initiatives in keeping our best practices in securing identities and MVA and law enforcement best practices. To be added to the Fraud Awareness Call invitation list, contact the AAMVA's law enforcement program manager.

Recommendation 1.1: MVA investigator fraud awareness calls be conducted at least quarterly but monthly if possible.

Strategy 2 – Ensure MVA Investigator Content Is Included in AAMVA Conferences

The Working Group views attendance at AAMVA conferences—the Annual International Conference, regional conferences, and the Workshop and Law Institute—as a valuable way to integrate investigators into the AAMVA community. Participating in sessions, as presenters and attendees, will be beneficial. Moreover, the networking and contacts made through attending these conferences will add value to the professional development of investigators. Fraud content relevant to MVA Investigators will provide justification for MVA Investigator attendance and participation.

Recommendation 2.1: Conference planning committees should seek guidance from the Law Enforcement Standing Committee to ensure a robust "Law Enforcement/MVA Investigator Track."

Strategy 3 – Continue MVA Fraud or Investigator Representation on the AAMVA Combined Standing Committees

Recommendation 3.1: During the committee selection process filling fraud discipline vacancies, involved staff should ensure priority is given to MVA Investigators.

Recommendation 3.2: Future Working Groups created under any of the three standing committees that have a nexus to the fraud discipline should be chartered to include at least one MVA investigator as a member.

Singularly, implementation of any one of these strategies will contribute to the goal of more fully integrating investigators into both the AAMVA community and the AAMVA law enforcement discipline. Implementation of all four strategies, as time and resources allow, will strengthen MVA investigator integration exponentially.

Appendix B Motor Vehicle Administration Investigative Unit Survey

1. Number of licensed drivers

STATE	TOTAL DRIVERS
Alabama	4,026,151
Alaska	529,281
Arizona	5,369,210
Arkansas	2,153,929
California	27,213,650
Colorado	4,235,384
Connecticut	2,608,061
Delaware	812,529
District of Columbia	535,579
Florida	15,560,628
Georgia	7,261,266
Hawaii	943,173
Idaho	1,252,535
Illinois	8,546,932
Indiana	4,589,405
Iowa	2,274,431
Kansas	2,154,260
Kentucky	3,030,329
Louisiana	3,435,168
Maine	1,046,129
Maryland	4,463,862
Massachusetts	4,950,056
Michigan	7,141,494
Minnesota	4,273,027
Mississippi	2,058,036
Missouri	4,274,389
Montana	811,851
Nebraska	1,430,818
Nevada	2,054,421
New Hampshire	1,195,211
New Jersey	6,377,413
New Mexico	1,449,711
New York	12,194,360
North Carolina	7,620,001
North Dakota	556,064
Ohio	8,032,792
Oklahoma	2,522,670
Oregon	3,002,014
Pennsylvania	8,987,676
Rhode Island	761,046
South Carolina	3,877,968
South Dakota	648,663
Tennessee	4,786,973
Texas	17,822,760
Utah	2,121,099
Vermont	472,633
Virginia	5,888,196
Washington	5,711,136
West Virginia	1,130,389
Wisconsin	4,296,646
Wyoming	424,115
Total	**228,915,520**

Source citation: https://www.fhwa.dot.gov/policyinformation/statistics/2019/dl1c.cfm

2. Number of registered vehicles

STATE	ALL MOTOR VEHICLES		
	PRIVATE AND COMMERCIAL	PUBLICLY OWNED	TOTAL
Alabama	5,208,055	112,285	5,320,340
Alaska	773,487	19,339	792,826
Arizona	5,994,049	59,732	6,053,781
Arkansas	2,873,523	39,846	2,913,369
California	29,772,776	625,473	30,398,249
Colorado	5,289,701	61,007	5,350,708
Connecticut	2,861,733	5,821	2,867,554
Delaware	1,000,965	5,170	1,006,135
District of Columbia	319,157	37,380	356,537
Florida	18,170,725	293,781	18,464,506
Georgia	8,670,440	159,156	8,829,596
Hawaii	1,222,626	22,309	1,244,935
Idaho	1,906,586	11,091	1,917,677
Illinois	10,489,500	98,225	10,587,725
Indiana	6,174,483	25,418	6,199,901
Iowa	3,747,148	40,076	3,787,224
Kansas	2,587,402	16,141	2,603,543
Kentucky	4,364,808	94,877	4,459,685
Louisiana	3,771,473	89,731	3,861,204
Maine	1,105,912	15,194	1,121,106
Maryland	4,134,474	76,903	4,211,377
Massachusetts	5,021,482	15,204	5,036,686
Michigan	8,378,579	74,660	8,453,239
Minnesota	5,638,650	52,099	5,690,749
Mississippi	2,044,918	14,057	2,058,975
Missouri	5,531,016	56,006	5,587,022
Montana	1,948,225	4,328	1,952,553
Nebraska	1,888,168	47,189	1,935,357
Nevada	2,525,687	23,670	2,549,357
New Hampshire	1,346,800	10,735	1,357,535
New Jersey	5,944,293	61,954	6,006,247
New Mexico	1,755,205	27,946	1,783,151
New York	11,259,986	64,769	11,324,755
North Carolina	8,595,707	143,573	8,739,280
North Dakota	880,524	18,559	899,083
Ohio	10,481,200	111,117	10,592,317
Oklahoma	3,708,789	21,458	3,730,247
Oregon	4,014,446	80,996	4,095,442

Pennsylvania	10,563,010	127,177	10,690,187
Rhode Island	849,912	16,713	866,625
South Carolina	4,356,396	204,903	4,561,299
South Dakota	1,271,188	23,094	1,294,282
Tennessee	5,699,910	155,463	5,855,373
Texas	22,100,167	319,323	22,419,490
Utah	2,443,052	36,552	2,479,604
Vermont	596,297	11,593	607,890
Virginia	7,464,143	142,309	7,606,452
Washington	7,068,917	188,484	7,257,401
West Virginia	1,617,933	39,429	1,657,362
Wisconsin	5,532,287	83,984	5,616,271
Wyoming	845,095	15,933	861,028
Total	**271,811,005**	**4,102,232**	**275,913,237**

Note: This includes automobiles, buses, trucks, and motorcycles.

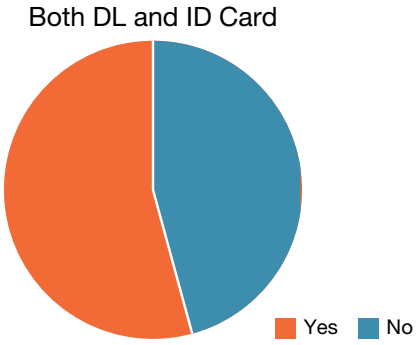
Source citation: https://www.fhwa.dot.gov/policyinformation/statistics/2020/mv1.cfm

3. Do you allow an individual to have both a DL and a non-drivers ID card?

37 respondents:

Yes = 17

No = 20

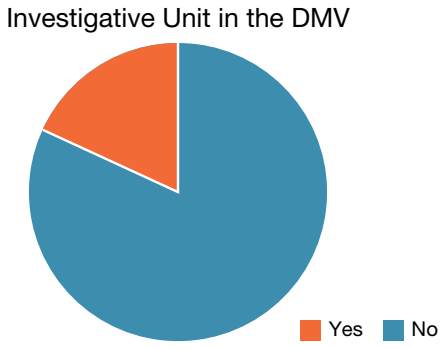


4. Do you have an investigative unit in your MVA?

39 respondents:

Yes = 32

No = 7



The information in this appendix is a portion of that gathered through the survey. The full survey and responses by jurisdiction can be accessed here on the AAMVA's website. (AAMVA's Survey Tool requires log in and is only available to jurisdiction members).

Appendix C Other Resources

The following are additional resources MVA 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

- **U.S. Citizenship and Immigration Services (USCIS):** The UUSCIS 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 the United States 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 provides 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. Marshals 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 Crime Information Center (NCIC):** The NCIC is a computerized index of criminal justice information. 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 Services (CJIS):** The 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 Services/ 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
- **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. https://www.state.gov/about-us-bureau-of-diplomatic-security
- **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 (MAGLOCLEN):** 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/MAGLOCLEN
- **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/ 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 aged, blind, and disabled individuals. 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 SSA programs and operations. This office serves as the OIG's liaison to the DOJ 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 D Motor Vehicle Administration Investigator Working Group Roster

CHAIR

Ricky H. Rich
Deputy Commissioner
Georgia Department of Driver Services

MEMBERS

Randy S. Belasic
Special Agent
Tennessee Department of Revenue

Charles Hopps
Senior Investigator
Nevada Department of Motor Vehicles

Cristian Machidon
Senior Motor Vehicle Investigator
Florida Department of Highway Safety & Motor Vehicles

Desiree Steele
Management System Analyst
Kansas Division of Vehicles

Karen A. Carson
Chief of Compliance and Investigations
Delaware Division of Motor Vehicles

Peggy Hines
Director, Enforcement Division
Michigan Department of State

Albert Rangel
Supervisor, Troop Z Criminal Investigations
Oklahoma Highway Patrol

AAMVA PROJECT MANAGER

Brian Ursino
Director, Law Enforcement Programs

AAMVA STAFF

Thomas Foster
Law Enforcement Program Manager

Patrice Aasmo
Director, Member Services, Regions 1 and 2

OUR VISION

Safe drivers
Safe vehicles
Secure identities
Saving lives!

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