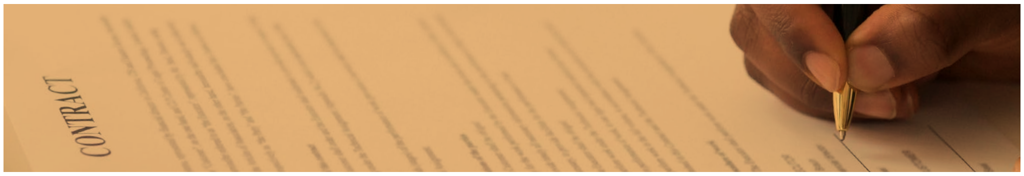
AAMVA

American Association of
Motor Vehicle Administrators

Implementation
THIRD Service
PARTY Delivery
Memorandum of
Understanding
STANDARDS OF PERFORMANCE

Third-Party Agent Administration
Best Practices

*Administering, Expanding, and
Establishing a Third-Party Program*



February 2021

THIRD PARTY AGENTS WORKING GROUP

Cover photo credits: © iStockphoto.com

Contents

Executive Summary

AAMVA jurisdictions utilize third-party agents (agents) to perform driver and/or motor vehicle transactions on behalf of the motor vehicle administration and in compliance with jurisdiction statutes and rules. In some jurisdictions, these agents are the primary service delivery networks for the motor vehicle administration. In other jurisdictions, these agents provide ancillary or specialized services to a specific customer set, such as dealers, or to a specific geographical location. As more jurisdictions expand the offering of services and service delivery options for agents, the AAMVA community recognizes the need for a reference document to share best practices and serve as a resource to enhance the implementation and operation of third-party programs for both the jurisdictions and the agents.

This best practice document is the product of a working group composed of AAMVA member jurisdictions established at the direction of the AAMVA Board of Directors and the Vehicle Standing Committee. Working group members represent both driver and motor vehicle business areas, all four AAMVA regions, and specialized knowledge in the administration and auditing of agents. In addition, industry representatives participated in a stakeholder's forum (Participants listed in Appendix C) and provided background and insight.

An effort was made to acknowledge the various models jurisdictions use when engaging agents. Some of these models stem from long-standing role assignments between the jurisdiction and county or other local agencies. Some derive from a consolidated government "service center" model often used in Canadian provinces. Some also are the result of the development of private-sector services to address the market for more efficient or rapid completion of required government filings and payments. The recommendations in this document do not endorse any single model for administering a third-party agent program that should be adopted by all jurisdictions. Rather, the focus is placed on best practices for setting up the program, the importance of a well-structured contract defining the business relationship, and clear recommendations on maintaining performance standards, including corrective actions, to ensure compliance and to achieve the desired results.

Other than making certain there is a contract or memorandum of understanding (MOU) in place between the jurisdiction and the agent to define the business relationship and responsibilities, there is no single best practice that can be applied to all jurisdictions or situations. However, a jurisdiction seeking to add new third-party services or to improve the quality or performance of existing services will find resources in this document to support its efforts.

The working group placed particular emphasis on auditing and compliance actions jurisdictions have developed to ensure the work performed by agents conforms to the same standards the jurisdiction has in place for its own work product. This specifically includes data quality, data security, and financial integrity. Monitoring, auditing, and enforcement actions will need to be in place so the jurisdiction can identify, correct, mitigate, and, if necessary, terminate noncompliant activity.

The quality expectations and performance standards should be specified in the contract and used during follow-up audit procedures. Measuring and reporting on compliance with agent quality standards also allow the jurisdiction to identify the success of training efforts, the quality assurance process, and overall program success. Failure to comply with performance measures may subject the agent to corrective actions. The recommendations on performance measurements and quality standards are intended to guide the development of required minimum quality assurance standards that all authorized agents are required to conform with.

Fraud detection and deterrence measures provide appropriate internal controls to mitigate the risks of internal and external fraud. The best practices include recommendations for the use of data analytical tools and trained personnel to identify anomalies, bring attention to questionable transactions, and discover potential fraud trends for both internal users and external agents. These tools are very useful in identifying and preventing fraud.

The jurisdictional best practices and shared experiences described in this document will assist jurisdictions seeking to implement or expand agent services. The best practices will also be helpful when looking to upgrade existing policy documents and procedures with a goal of improving oversight. Additionally, best practices recommendations regarding contract or MOU provisions will bring increased standardization for vendors and agents operating in multiple jurisdictions.

Glossary of Terms and Acronyms

For purposes of these best practices, the following definitions and acronyms shall be used:

AAMVA The American Association of Motor Vehicle Administrators is a tax-exempt nonprofit organization that develops model programs in motor vehicle administration, law enforcement, and highway safety. Founded in 1933, AAMVA represents the jurisdictional officials (state, provincial, and territorial) in the United States and Canada who administer and enforce motor vehicle laws. AAMVA's programs encourage uniformity and reciprocity among the jurisdictions.

Agent A third-party entity performing title and registration or driver license and identification card transaction services on behalf of or directly to the jurisdiction. The agent may be a commercial enterprise or government entity.

Audit A review and inspection conducted by authorized jurisdictional employees or official designees of the agent's operations, place of business, and processed motor vehicle titling and registration or driver license transactions

Contract A written agreement that recognizes and governs the rights and duties of the parties to the agreement between a jurisdiction and a third-party agent. The contract can also include a subcontract between a prime contractor and an agent or vendor.

Data breach Intentional malicious act to obtain protected data by circumventing intrusion prevention systems; data are obtained by someone who is not authorized to have them

Dealer A person engaged in the business of buying, selling, or exchanging vehicles

DMV, MVA, and MVD In the United States, a Department of Motor Vehicles (DMV), Motor Vehicle Administration (MVA), or Motor Vehicle Division (MVD) is a state-level government agency that administers vehicle and driver license laws, regulations, and policies. Similar departments exist in Canada. The name "DMV" is not used in every state, province, or territory, nor are the traditional DMV functions handled by a single agency in every jurisdiction, but the generic term is universally understood, particularly in the context of driver license issuance and renewal. Driver licensing and vehicle registration in the United States are handled by the state government in all states and territories except the state of Hawaii, where local governments perform DMV functions. In Canada, driver licensing and vehicle registration are handled at the provincial and territorial government levels. The Uniform Vehicle Code prefers the name "Department of Motor Vehicles."

Driver transactions

Transactions that can include, but are not limited to, issuance of driver licenses, identification cards, and written and/or non-Commercial Driver License (non-CDL) skills testing

Driver's Privacy Protection Act (DPPA)

U.S. federal statute prohibiting the disclosure of personal information as defined in 18 U.S.C. §2721 without express consent of the person to whom such information applies with the exception of certain circumstances set forth in 18 U.S.C §2721. These rules apply to U.S. motor vehicle agencies as well as other authorized recipients of personal information and impose record-keeping requirements on these authorized recipients.

Flow-down clause

A contract provision by which the parties incorporate the terms of the prime contract between the jurisdiction and any subcontractor into the lower tier agreement. It might also be referred to as a pass-through or conduit clause.

Local government entity

An elected or appointed official who performs title and registration and/or driver license transactions on behalf of a jurisdiction. In many jurisdictions, local governmental entities have long-standing and close working relationships with the jurisdiction to process transactions, and these relationships are often spelled out in statute or regulation. Because this type of agent is also a governmental entity, the relationship model and contract or MOU may differ from how the jurisdiction deals with a commercial entity, and the model examples attempt to reflect that difference.

Jurisdiction

Generally, in North America, this refers to a provincial-, state-, or territorial-level government agency that administers vehicle and driver license laws, regulations, and policies. The jurisdiction sets the terms for a business relationship with the agent and be a party to the contract or MOU.

Memorandum of understanding (MOU)

A type of agreement between two or more parties. (Note: An MOU is generally only appropriate for establishing a relationship with another governmental entity. For third-party agents, a contract is important to define the business relationship and terms.)

Performance standards

The objective standards to which the services are to be performed by the agent, as defined in a contract or MOU

Personally Identifiable Information (PII)

Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, Social Security Number (SSN), date and place of birth, mother‘s maiden name, or biometric records, and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information

Quality assurance The program and activities the agent is required to build into the transaction process to monitor and evaluate the services to certify that the jurisdiction's quality performance standards will be met. These include training, manuals and help resources, and program edits to prevent data errors.

Quality control The operational techniques and activities used to verify the jurisdictional requirements for quality are being fulfilled and meet the performance standards. Quality control is performed after the transactions are completed and includes procedures such as audits, anomaly detection, and error tracking to identify trends or patterns of errors.

REAL ID Act Establishes minimum security standards for license issuance and production and prohibits U.S. federal agencies from accepting for certain purposes, driver's licenses and identification cards from states not meeting the Act's minimum standards

SAVE Systematic Alien Verification for Entitlements program (SAVE). The SAVE Program provides a secure verification service for federal, state, and local benefit-granting agencies to verify a benefit applicant's immigration status or naturalized or derived citizenship.

Service-level agreement (SLA) Additional business language added to a contract or MOU that helps to implement the program objectives (e.g., performance metrics, error rates)

SSOLV Social Security Online Verification (SSOLV). A way to electronically verify the name, date of birth, gender, and SSN of those applying for a driver license or identification (ID) card with the records from the Social Security Administration (SSA).

Stakeholder A person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Suspension A sanction that temporarily withdraws an agent's access to do business on behalf of a jurisdiction

Third-party Vendor A provider of transaction capability through a proprietary user interface used by a third-party agent

Training Teaching agents the knowledge and skills to process motor vehicle titles and registrations or driver license transactions on behalf of the jurisdiction

Transaction A sequence of information exchange and related work (e.g., database updating) for the purposes of creating, duplicating, or updating a driver license or identification card, title, or registration record. For the purpose of this best practices document, "transaction" means title and/or registration or driver license transactions (excluding CDL third-party examiners) or identification cards. In some cases, the transaction performed by the agent might only be one step in the process of completing the transaction or fulfilling the request.

User An individual performing title and registration and/or driver license transactions on behalf of or as an employee of an agent

Vehicle transactions Include, but are not limited to, issuance of title, registration, permits, and other credentials related to the ownership of a vehicle or the authorized operation of the vehicle in the jurisdiction. The scope of the transaction also includes collection of fees or taxes associated with the transaction.

Vendor or software provider A vendor provides software services or a system to permit agents to process transactions that meet the jurisdictions requirements for policy, quality and information security

Introduction

Motor vehicle agencies throughout North America are increasing utilization of third-party agents to process motor vehicle and driver license transactions on behalf of their jurisdictions. In some jurisdictions, the agencies are required to use a third party, such as local government entities. In other jurisdictions, the use of third parties is a long-established tradition and an integral component of the service delivery system. Whether administering or expanding an existing program or implementing an entirely new program, a strong framework under which the third parties will operate is vital to a successful program.

Ideally, a third-party agent program fulfills a known service-level need. Agents might be the primary service delivery system for some jurisdictions, either because of the benefits the program provides or because of legislative mandates. In other jurisdictions, the agents provide ancillary or specialized services to a specific customer set, such as dealers, or to a limited geographical location. Therefore, it is important to consider the program goals when establishing or expanding a program.

Jurisdictions grant authority to agents to act on their behalf for specified services or transactions but ultimately oversee the accuracy and completeness of driver and/or vehicle data and transactions. The jurisdiction's administrative responsibility needs to be conveyed to the agents through statutory and contract language that is clear and thorough. Jurisdictions recognize the importance of these steps because the public perception of the jurisdiction may suffer from errors or misuse in the fulfillment of transactions even if they were completed by an agent. The contract or memorandum of understanding (MOU) with the agent or vendor sets the basis of and forms the foundation for fulfilling the operational goals of the program.

The working group recommends that any jurisdiction utilizing agents consider the best practices within this document for existing third-party programs. For an existing program currently meeting program performance goals, the best practices might be a source of new ideas for program enhancements. For a jurisdiction looking to expand or establish a new third-party program, the best practices are a reference for the experience their peer organizations have established for successful operations.

The information and recommendations are grouped into three main topics:

- The operational and legal considerations around administering an existing program, expanding an existing program, or establishing a new program
- The framework under which the third parties will operate
- Last and probably the most important, the jurisdiction's course of action to ensure compliance with program standards, security, and service goals

Chapter 1 Third-Party Business Relationships

The working group recognized the importance of distinguishing who should be considered agents of the jurisdiction and accounting for the various ways they do transactions for the jurisdiction. The working group surveyed government and industry stakeholders to account for as many variations as possible. The definitions of "agent" and "vendor" provided in the Glossary and expanded in the next sections are the result of that research. The working group also identified entities it believed should not be included as agents; these entities are also defined.

Agent

An agent is any entity that processes driver or vehicle transactions on behalf of or directly to the jurisdiction. The agent may be a commercial enterprise or government entity. It is common for a jurisdiction to have different types of agents or models for different transactions. Examples include a county office for vehicle or driver transactions, a school for driver knowledge testing, and a dealer association for title and registration applications for vehicle sales. These and all other relationships outside of the internal operations of the jurisdiction are agents for the purpose of this discussion. The agent may be a party to the contract or MOU as a prime or subcontractor, depending on the model defined by the jurisdiction.

An agent is any entity that processes driver or vehicle transactions on behalf of or directly to the jurisdiction. The agent may be a commercial enterprise or government entity.

Vendor or Software Provider

The vendor, for the purpose of this discussion, is an entity that does not directly process transactions but rather provides software services to permit agents to process transactions that meet jurisdiction requirements for policy, quality, and information security. The working group recognizes that some agents develop and maintain their own proprietary software to process jurisdictional transactions and may also provide the software as a service to other agents. An agent in that circumstance would be in the category of a vendor for the other agent, as well as being their own agent for the transactions they process. The vendor may be a party to the contract or MOU as a prime or subcontractor, depending on the model defined by the jurisdiction. Vendors typically receive fees for their software services from the agent or the jurisdiction.

Entities That Are Not Agents

The following entities were deemed to be out of scope for the purpose of this best practice document because they do not process transactions on behalf of the jurisdiction.

- Commercial websites – entities offering DMV services or information online (or other generic DMV-related websites) that are not sanctioned by a jurisdiction and whose content is not reviewed or approved by the jurisdiction
- Runner services – entities operating services for individuals or businesses to deliver driver or vehicle transactions to the jurisdiction or back to the customer. These services (sometimes called

messenger or concierge services) act as agents to the person or business requesting the activity but not to the jurisdiction. They are not authorized to perform transactions on behalf of the jurisdiction.

- Bulk information requestors – entities purchasing driver or vehicle files for insurance or vehicle title information. Bulk information requestors are not performing transactions or updating or modifying the jurisdiction's record.
- Any motor vehicle dealer **not** submitting electronic data to a jurisdiction – This also applies to a licensed dealer that uses a contract employee or service to assist with completing the paperwork required by the jurisdiction for a sale or transfer transaction.
- Commercial Driver License (CDL) transactions – any transaction related to a CDL, including issuance, written, and skills testing. The CDL third-party testing program is covered in a separate AAMVA best practices document ("Commercial Driver's License Program Best Practices" [2007]).

In the collection and analysis of best practices for this paper, the working group completed a survey of AAMVA U.S. and Canadian member jurisdictions to summarize their usage of third-party agents.

Models

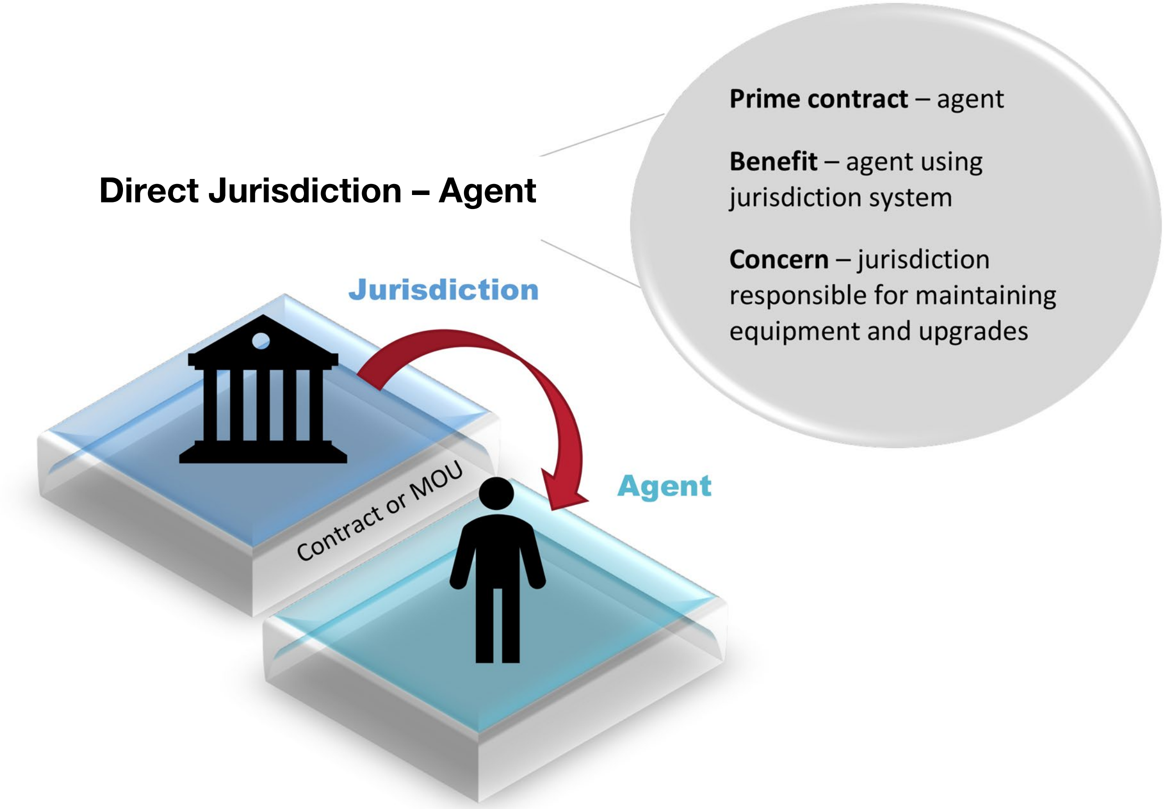
The business relationship between an agent or vendor and the jurisdiction might consist of various models based on the type of transactions being completed and the jurisdiction's approach to the relationship. The parties in this relationship will include the jurisdiction and the agent and sometimes a vendor working on behalf of one or more agents to provide software services, enabling the transaction processing.

The contract will define the relationship between the agent and the jurisdiction. If there is a vendor involved in the relationship, the jurisdiction's contract should also define that relationship, but the working group acknowledges in some cases that the relationship is only defined by a contract between the agent and the vendor.

The jurisdictions within the AAMVA community have established a variety of different approaches to defining the business relationship with the third-party agents. Each approach has its own benefits and challenges. In the collection and analysis of best practices for this paper, the working group completed a survey of AAMVA U.S. and Canadian member jurisdictions to summarize their usage of third-party agents. The compiled survey results are listed in Appendix A, attached to this paper. The responses are from the jurisdictions and should be considered complete as of June 2020. For additional information or sample documentation on a jurisdiction's program, we recommend contacting the jurisdiction directly.

Business Relationship Models for Agents

- In the section that follows, the various models are labeled to identify what group or groups have the **primary contractual relationship to the jurisdiction** and how subcontractor relationships (usually involving a vendor or software provider) also enter into the picture. The depiction of the models is a graphical representation of the more common relationships the working group identified. A jurisdiction may also use different business models for different types of transactions, such as driver services or vehicle services. The number of AAMVA jurisdictions, agents, and vendors in this field means that there are more business models than shown in these representations. The depiction of the models is intended to assist a jurisdiction contemplating a new or expanded program and to give a perspective on some of the more common relationship models.



Direct Jurisdiction – Agent

Prime contract – agent

Benefit – agent using jurisdiction system

Concern – jurisdiction responsible for maintaining equipment and upgrades

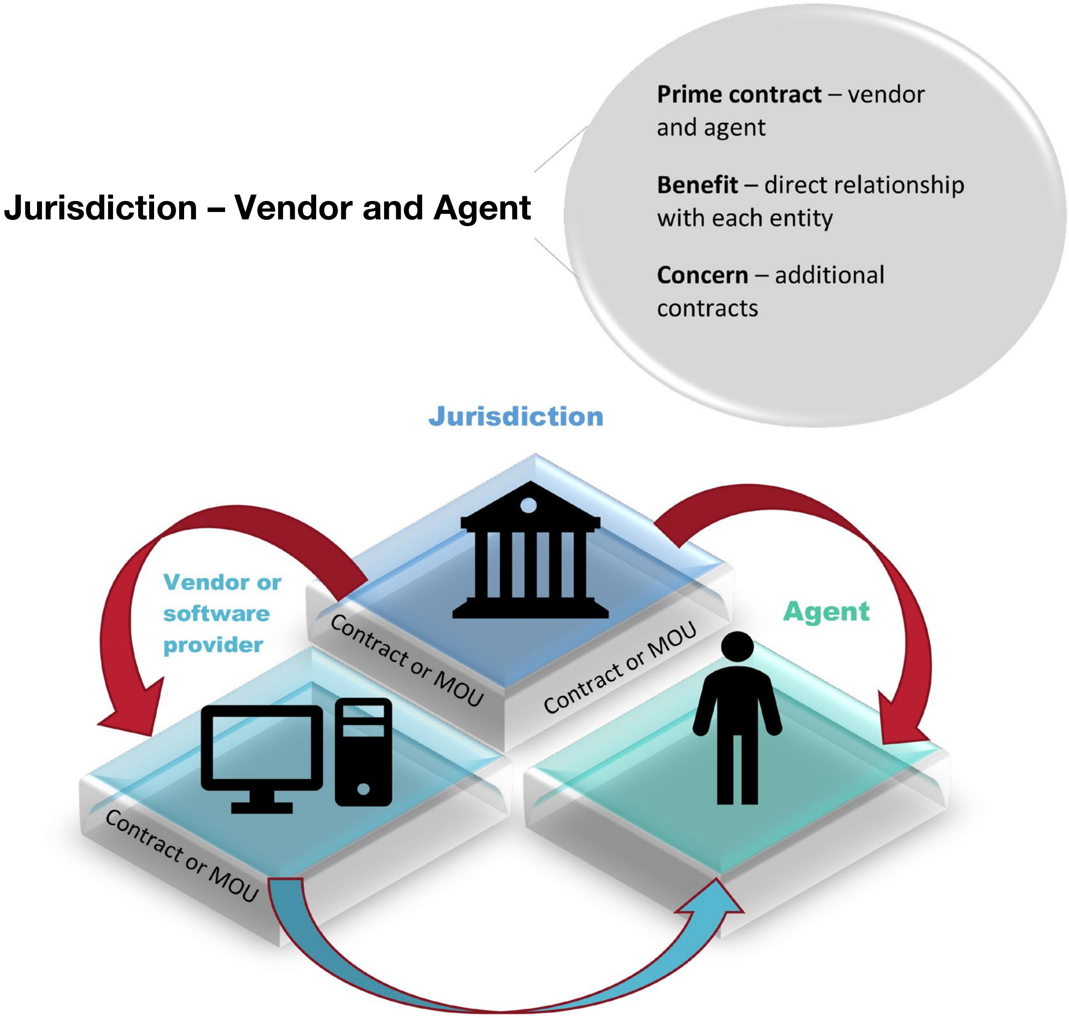
In the “direct jurisdiction – agent” model, the jurisdiction contracts with a local government entity or commercial entity to be the agent and provide services on behalf of the jurisdiction. Typically, in this model, the jurisdiction provides all programming and equipment for the agent to provide the service, eliminating the need to test or certify vendor-supplied equipment and connectivity resources. In some instances, the agent pays fees to the jurisdiction for the cost to set up and operate the hardware and software solution.

BENEFITS OF THIS MODEL

Because the jurisdiction controls the software system used by the agent, the system can be programmed to only permit authorized transactions and include the same jurisdictional quality control checks or “stops” to prevent and mitigate fraud. The jurisdiction has control of the final product that is given to the consumer (e.g., title, plates, test results). No additional vendors are involved, which minimizes effort on the jurisdiction to stand up a third-party program.

CONCERNS WITH THIS MODEL

The jurisdiction may provide equipment, software, and connections to the agent. However, unless the agent has skilled resources available to their users for problem resolution, the jurisdiction will have the burden of delivering immediate assistance for technical questions and service interruptions that result in downtime for the agents.



Jurisdiction – Vendor and Agent

Prime contract – vendor and agent

Benefit – direct relationship with each entity

Concern – additional contracts

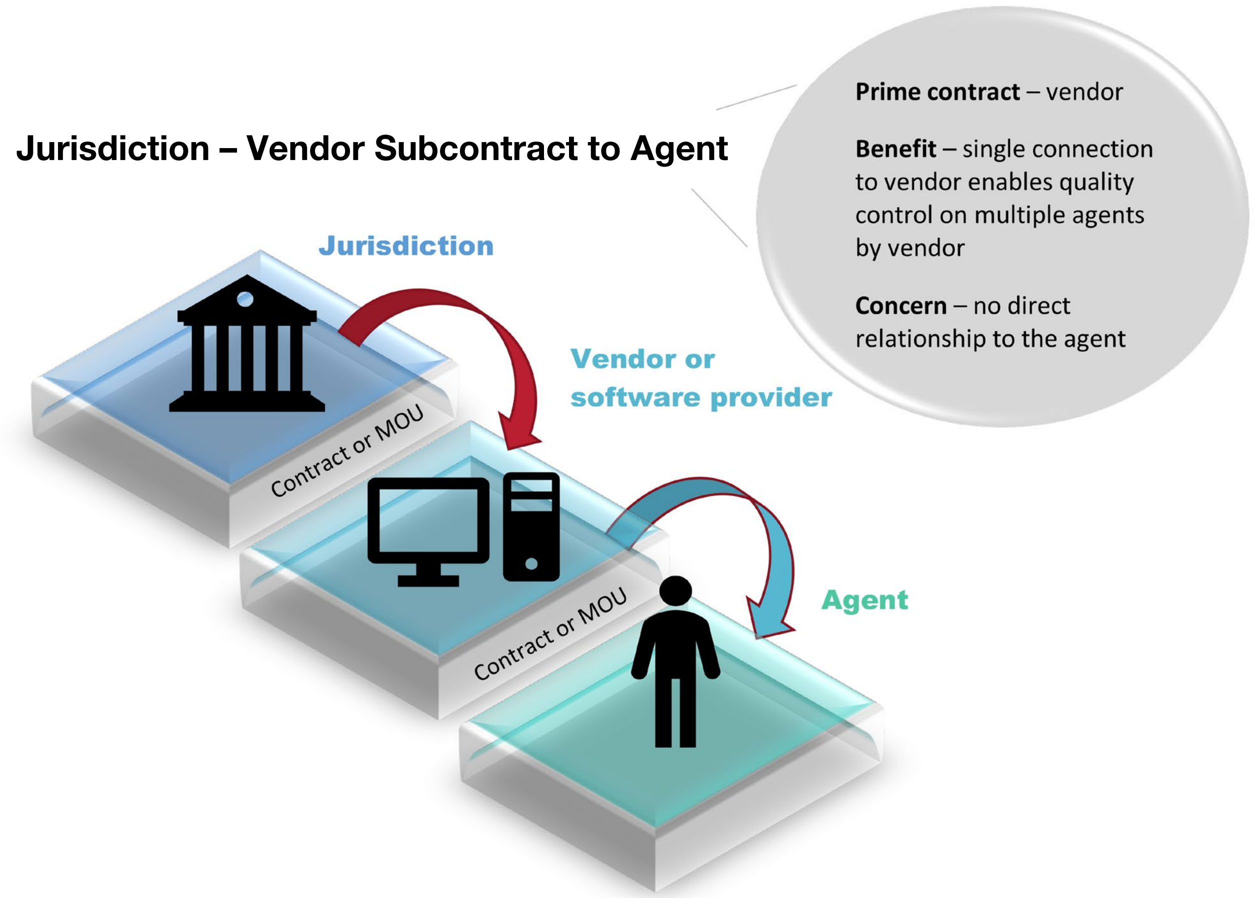
In this model, the jurisdiction contracts directly, but separately, with both the agent and vendor to perform transactions or provide software systems on behalf of the jurisdiction. Each vendor and agent need to contract as a prime contractor with the jurisdiction to access and/or modify motor vehicle and identification card or driver license documents. In addition, any agent would contract directly with the vendor to utilize its software and services.

BENEFITS OF THIS MODEL

The benefit to this model is the direct contractual relationship the jurisdiction has with the vendor or software provider and avoiding the need for examination of subcontractor arrangements for contract terms, such as data security, that need to “flow down” from the prime contract to the subcontractor. The jurisdiction’s relationship with the vendor or software provider also enables a direct relationship in the event of technical issues or data exchange standards.

CONCERNS WITH THIS MODEL

This model requires more contract maintenance by the jurisdiction than other models. Although this affords the jurisdiction direct oversight over all entities in the process, it also creates a need for additional personnel to effectively manage the program.



Jurisdiction – Vendor Subcontract to Agent

Prime contract – vendor

Benefit – single connection to vendor enables quality control on multiple agents by vendor

Concern – no direct relationship to the agent

In the "jurisdiction – vendor subcontracts to agent" model, the jurisdiction would have a prime contract or MOU with the vendor or software provider that sells a product or service to perform transactions on behalf of the jurisdiction. The vendor or software provider does not directly process transactions or operate service outlets. In this scenario, the agent is a subcontractor to the vendor or software provider. The vendor contracts with and maintains a network of agents that utilize the product and provide transaction services directly to customers. The jurisdiction's guidelines and rules on transaction processing flow from the jurisdiction to the vendor and then to the agent. The jurisdiction conducts quality reviews and oversight on the work product of the agent. Enforcement or corrective action resulting from an agent's errors or misuse will be based on the contract terms with the vendor. Vendors operating in this model state that they perform their own quality control before transactions are sent to the jurisdictions and hold the agents to rigorous standards.

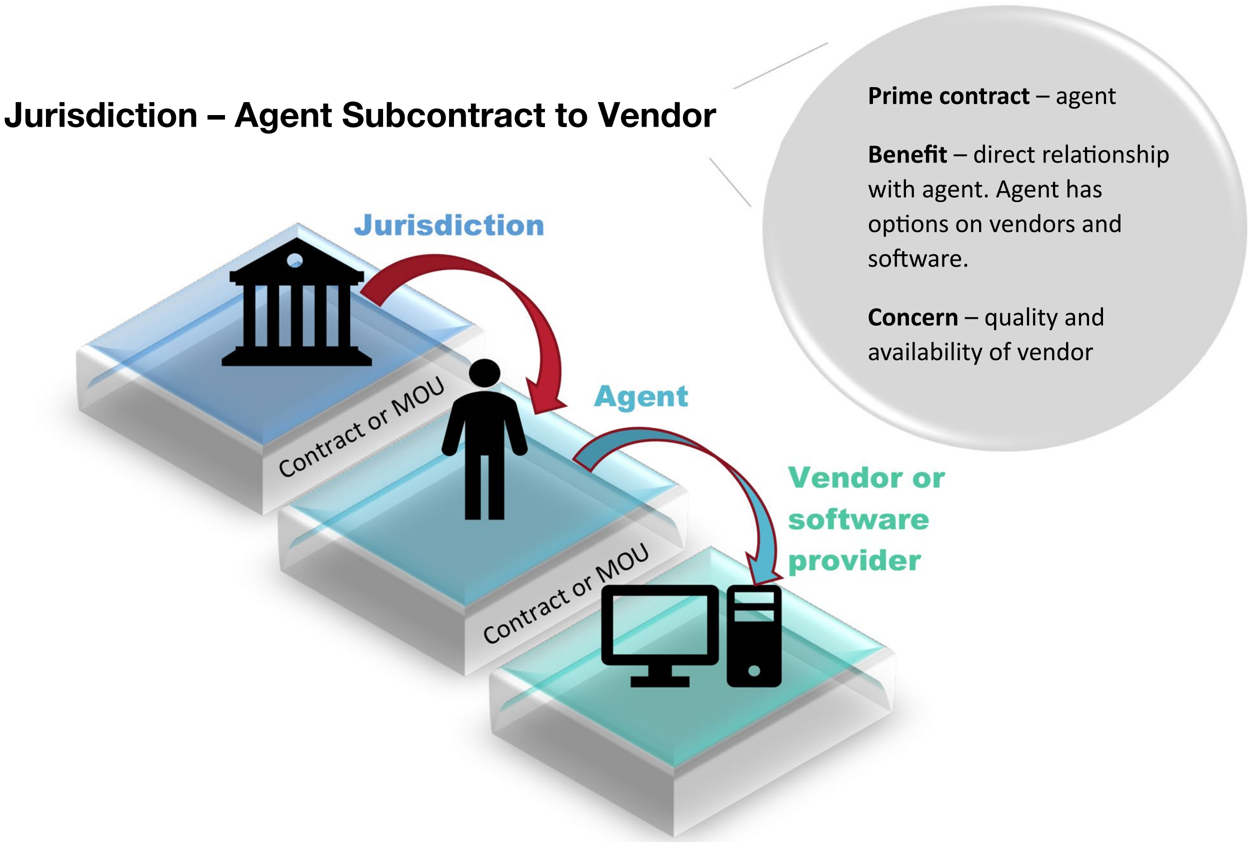
The vendor or software provider is also responsible for any provision of the prime contract with the jurisdiction that affects the agent, such as data security requirements, performed by the subcontracting agent.

BENEFITS OF THIS MODEL

The benefit of this model is the direct contractual relationship the jurisdiction has with the vendor or software provider in the event of technical issues or standards. The jurisdiction will have a less complex technical environment because the vendor delivers transactions from multiple agents using the same application software and connection to the jurisdiction. The vendor also adds a layer of quality control, helping ensure the agent is complying with the jurisdiction's requirements.

CONCERNS WITH THIS MODEL

This model does not give the jurisdiction direct contractual authority over the agents, which presents risks. To offset the risk, the jurisdiction's contract with the vendor needs to define performance expectations for the vendor and agent and specify clear enforcement actions if the agent's performance does not meet standards.



Jurisdiction – Agent Subcontract to Vendor

Prime contract – agent

Benefit – direct relationship with agent. Agent has options on vendors and software.

Concern – quality and availability of vendor

In the “jurisdiction – agent Subcontract to Vendor” model, the jurisdiction would have a contract or MOU with the agent that provides the transaction service to customers. The agent then contracts with a vendor or software provider to assist with transaction processing and information technology (IT) requirements to submit transactions to the jurisdiction. In this scenario, the vendor or software provider is a subcontractor to the agent, and the agent is responsible for any provision of the prime contract with the jurisdiction that affects the vendor or software provider, such as data security requirements, that also involve the subcontractor.

BENEFITS OF THIS MODEL

The benefit to this model is the direct contractual relationship the jurisdiction has with the agent and assuring the agent is complying with the jurisdiction’s requirements. The agent has the option of developing its own software service or platform, in compliance with jurisdiction requirements, or seeking a vendor for that role.

CONCERNS WITH THIS MODEL

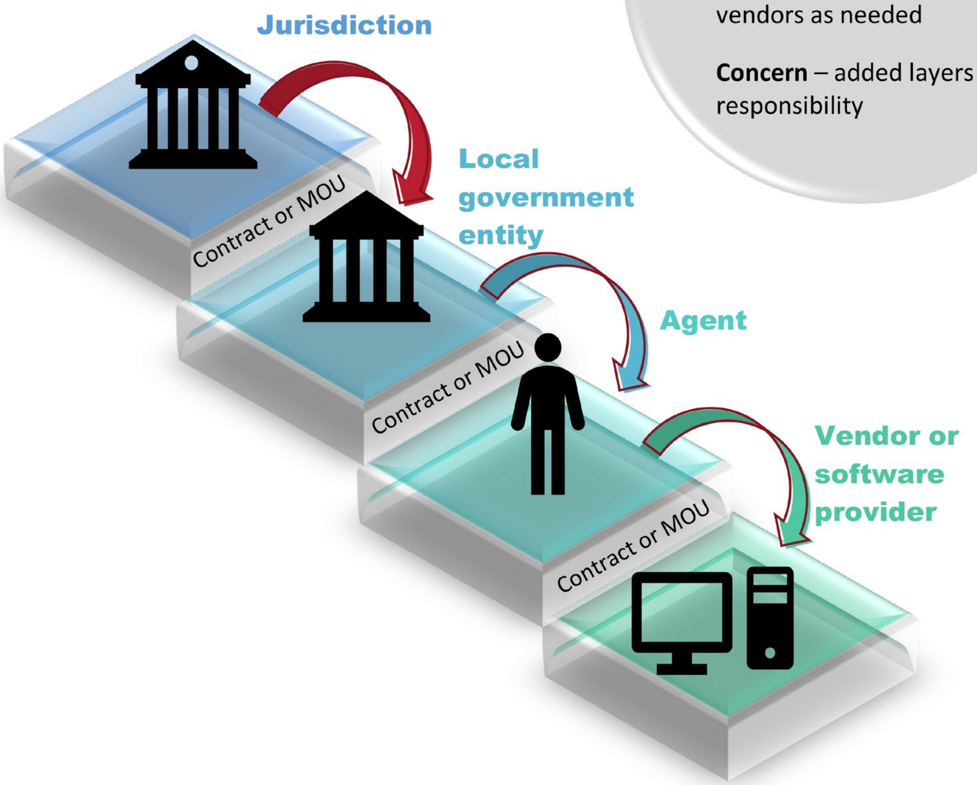
The agent is responsible for maintaining the software service and connection to the jurisdiction through its own resources or from a vendor. The success of the agent’s business operations is dependent on the availability of reliable vendors or software providers. Ultimately, errors or service interruptions from the vendor-supplied system are the responsibility of the agent.

Prime contract – local government entity

Benefits – local government entity engages with agents and vendors as needed

Concern – added layers of responsibility

Jurisdiction – Local Government Entity Subcontract to Agent – Vendor



In the "Jurisdiction – Local Government Entity Subcontract to Agent – Vendor" model, the jurisdiction would have a contract or MOU with the local government entity, often with oversight by an elected official. The local government entity contracts with agents to perform title and registration services on behalf of the local government entity and ultimately on behalf of the jurisdiction. The agent contracts with a vendor or service provider to assist with transaction processing and IT requirements to submit transactions to the jurisdiction. In this scenario, the vendor or software provider is a subcontractor to the agent, which is a subcontractor to the local government entity, which has a contract or MOU with the jurisdiction.

BENEFITS OF THIS MODEL

This model is best used by jurisdictions with specific laws delegating the responsibility for title and registration processing services to local government entities. The benefit of this model is the autonomy it provides the government entities to contract with agents that best fit their local needs. It also provides agents the ability to choose from approved vendor or software providers to provide the system software and support.

CONCERNS WITH THIS MODEL

This model adds an additional layer of services and contracts that can make oversight by the jurisdiction more challenging. Although the relationship with the local government entity may be established in statute, the added layers of agents and vendors creates additional opportunities for human and technical complexity, impacting the delivery of services.

1.1 Recommendations for Contacting Similar Jurisdictions

The working group recommends a jurisdiction preparing to establish or expand an agent program should consider contacting other jurisdictions that use third-party agents in a similar business process. Peer jurisdictions can be a resource for contract language and preparing a business case analysis of a new or expanding program. Some recommended areas of inquiry include, but are not limited to

- Achieving program benefits, cost savings, service improvements, etc.
- Identifying stakeholder groups to include, as well as identifying legislation or regulatory requirements
- Selecting, training, and evaluating agents
- Evaluating Requests for Proposal (RFPs), contracts, MOUs, standards of performance, and compliance documentation to determine if the jurisdiction should apply any of its program approaches in the development or expansion of the third-party program
- Evaluating contract issues and recommended language to prevent issues or to confirm compliance
- Anticipating staff impacts

Chapter 2 Expanding or Establishing a Third-Party Program

How a jurisdiction expands or establishes a program and chooses a model will later impact the jurisdiction's ability to successfully perform necessary oversight and administer the program effectively. The jurisdiction should seek to design a program that will both engage successful agents to participate and fulfill the jurisdiction's service objectives. A thoroughly developed third-party program structure is important. This section focuses on three areas:

- Recommendations for building a business case
- Recommendations for establishing the program framework
- Recommendations for a pilot program

Whether a jurisdiction is seeking to establish a new third-party program or to expand an existing program to process additional transactions, the steps to build the business case and roll out the new requirements are mostly the same. If a jurisdiction is facing service constraints, extending the services or locations of an existing third-party program could address the needs without adding new jurisdiction resources. For an entirely new program, researching successful models in other jurisdictions can bring additional insight into the development process.

Some examples of new or expanding program components are

- Driver license transactions
- Title transactions
- Vehicle registration and renewal transactions
- Dealer transactions
- Driver training programs (non-CDL)

How a jurisdiction expands or establishes a program and chooses the model will later impact the jurisdiction's ability to successfully perform necessary oversight and administer the program effectively.

Before allowing current agents to expand services or before onboarding additional agents, the jurisdiction should review the agents and program to determine:

- Agent compliance with the agreed performance standards and service-level agreements (SLAs)
- Agent audits and error results are reporting satisfactory results
- Agents have the ability to meet customer service expectations now and in the near future

2.1 Recommendations for Building a Business Case

The jurisdiction should conduct a thorough analysis of the business case and then prepare recommendations to support the decision to expand or establish a third-party program and engage third-party providers to fulfill the service objectives. The business case should include a description of the current service environment along with a thorough analysis of the recommended topics below:

- Assess the legislative and regulatory changes needed to enable agents or vendors to perform transactions on behalf of the jurisdiction.
- Evaluate current service-level deficiencies and how they will be addressed and measured in the third-party program. This might include service-level indicators—such as wait time, backlog,

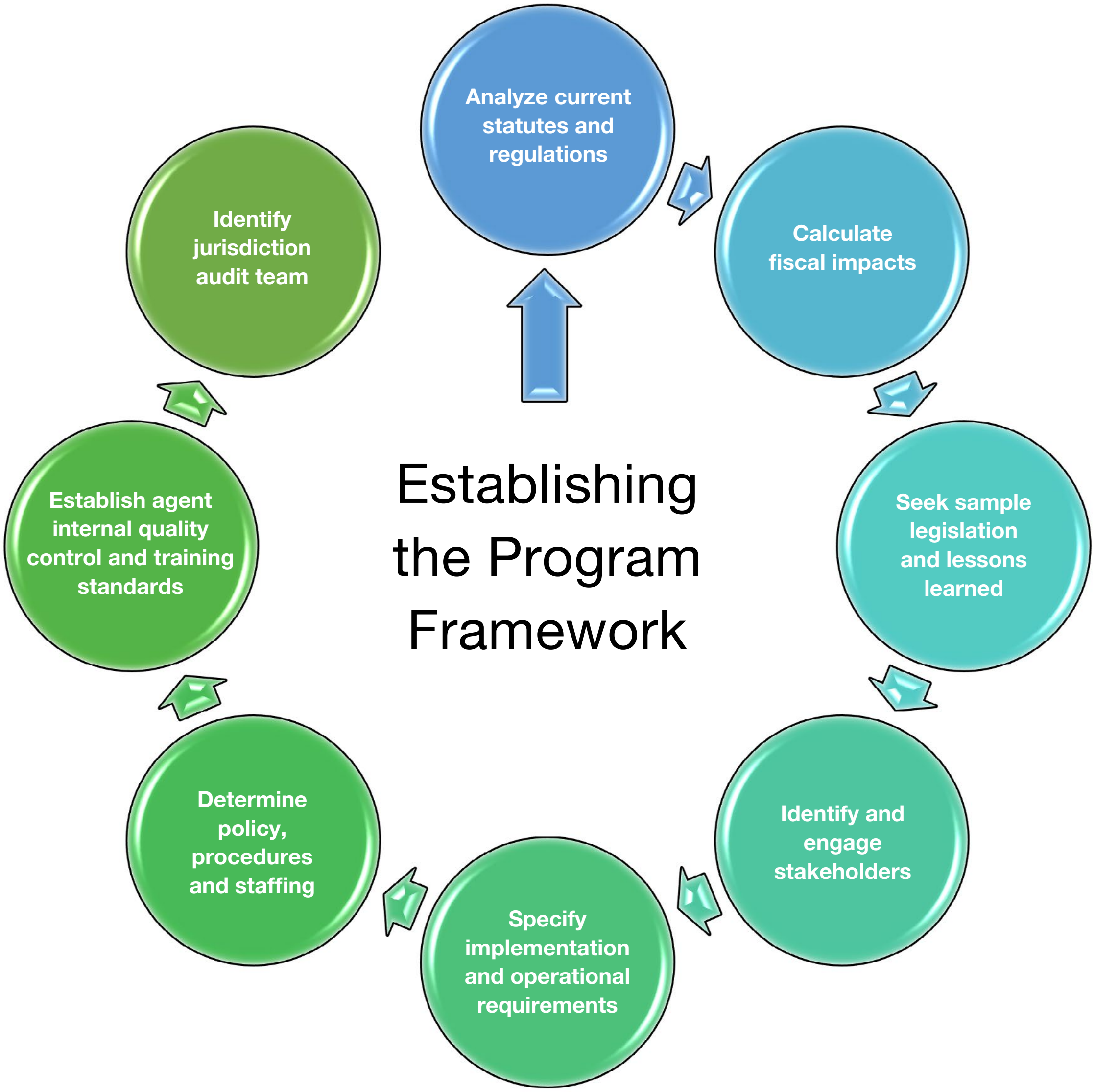
error, or rework—or the availability of services in specific geographic or demographic areas.

- A reduction in jurisdictional resources or increased workload might also drive the need for a third-party program. These resource constraints can be the result of cost-cutting requirements or situations when resources are reallocated for higher-priority efforts, resulting in a decline in service capability for the jurisdiction.
- Identify if a shift or increase in service demand has resulted from population or economic changes. The working group members found that a private-sector operation might be more flexible and responsive to economic shifts than the acquisition and training of new jurisdictional resources.
- If government offices are closed in an emergency event, agents may provide customers an additional option for motor vehicle and driver services at alternative locations or during extended hours.
- Determine how and where services should be provided and if agents are available that could be qualified to perform the needed transactions according to the jurisdiction's requirements.
- Analyze the structure of the compensation program to establish the availability of agent resources and to allow them to succeed. Although local government entities (e.g., counties, towns) are usually compensated by receiving a portion of the jurisdiction fees, agents set up as private enterprises primarily rely on service or convenience fees, over and above the jurisdiction fees, to support their operation. These additional fees might be set or capped by the jurisdiction or based solely on market forces.
- Identify request by business partners—such as dealers, banks, or fleets—for more direct involvement and control over the transactions associated with their business operation. Often, these businesses have evolved highly automated systems to manage their vehicle and driver qualification requirements and are looking to fulfill the regulatory and financial compliance activity as efficiently as possible.

2.2 Recommendations for Establishing the Program Framework

Upon completion of the approval of the business case, several steps are needed to establish a successful framework for a third-party agent program:

- Analyze current statutes and regulations to determine if specific legislative action is required or desired. If statutes do not prohibit the use of third-party agents, specific language enabling the program might still be desired to authorize the use of agents.
- The working group recommends that if enabling legislation is needed, it should be written to avoid being too prescriptive. Specifying detailed procedures in regulation or policy will allow the jurisdiction options for growth and appropriate oversight of the program without having to modify the underlying legislative text.
- Calculate the fiscal impact on the jurisdiction for any applicable agent or vendor expenses, such as
  - Agent training
  - Materials and supplies
  - Software modifications
  - Additional software licensing or upgrades to enable agent access
  - Retraining costs to cover legislative or policy changes
  - Additional costs to audit agent transactions and travel for on-site inspections
  - Revenue lost from processing fees retained by jurisdiction


Analyze current statutes and regulations
Calculate fiscal impacts
Seek sample legislation and lessons learned
Identify and engage stakeholders
Specify implementation and operational requirements
Determine policy, procedures and staffing
Establish agent internal quality control and training standards
Identify jurisdiction audit team
Establishing the Program Framework

- Seek sample legislation and lessons learned input from other jurisdiction with similar program models.
- Identify and engage with stakeholders needed to build support for the proposed changes. Some examples of stakeholders include:
  - Dealers and dealer associations
  - Lenders and lender associations
  - Agents or vendors, potential and current
  - Local government entities and applicable associations
  - General public
- Specify implementation and operational requirements that might be needed through a regulatory rule-making process. Jurisdictions should consider drafting rules to cover the following topics:
  - Agent processing fees (retained by the agent)
  - Agent training or certification requirements
  - Bond requirements
  - Insurance requirements, including cybersecurity and data breach protection
  - Background checks for the third-party agent and staff

- Any limitations that will be placed on the number or location of agent facilities

If there is only a single agent for a critical service or location, the jurisdiction might find it difficult to enact strong enforcement measures in the event of a serious breach of the policies or contract because of the negative impact it could have on customer access to services. Correspondingly, adding additional agents in an established market may be perceived by current agents as competition for their market share.

- Determine the type of procurement process that will be required to select qualified agents for the program:
  - RFP
  - Invitation for bid (IFB)
- Create and finalize additional items by the jurisdiction:
  - Agent-related business processes, policies, and procedures
  - Agent and vendor contract terms and conditions
  - Jurisdictional-provided training programs for transactions
  - SLA metrics and monitoring practices to comply with quality control activity
  - Staffing and training requirements for jurisdictional audit staff (experienced internal staff can be reallocated to audit and training duties)
  - Public information plan to notify customers of additional service options and locations
- Require the agent to submit internal quality control and training programs to the jurisdiction for review and approval before implementation.
- Create a jurisdiction audit team with associated policies and procedures for enforcing the standards of performance requirements and fraud prevention. The jurisdiction's quality control and auditing process might be enhanced by additional software tools.

2.3 Recommendations for a Pilot Program

Jurisdictions find it beneficial to conduct a pilot or limited rollout of a new program as a way to provide a gradual adoption of the changes to current operations. Recommendations for the pilot program include

- Limit the number of transaction types with the flexibility to add additional types as the agent successfully meets SLAs.
- Limit the geographical area, including locations that are easily visited, to observe and monitor operations.
- Start with a single line of business, such as registration renewal or driver knowledge testing, before expanding to business operations that require more program knowledge and training, such as title transfers or driver skills testing.
- Test and evaluate the SLA compliance process between the jurisdiction and the agent to make certain performance levels are being met prior to declaring the pilot a success.
- Schedule frequent (daily, then progressing to weekly) check-ins with the piloting agents.
- Create a report at the completion of the pilot to make improvements to the program going forward based on what was learned in the pilot.

Benefits of Implementing the Best Practices for Establishing or Expanding a Third-Party Program

The benefits of establishing or expanding a third-party program can include:

- Cost savings to the jurisdiction – The jurisdiction might be able to avoid adding additional office locations or closing current sites. The jurisdiction may also be able to repurpose staff currently processing transactions to other duties, such as auditing.
- Additional options for citizens – Adding agents can give citizens the option of shopping for services based on location, price, or customer service.
- Full-time equivalent (FTE) caps – In the event a jurisdiction is unable to add additional staff, third parties can support service delivery needs in areas where workload is increasing.
- Third-party solutions will be easier to manage.

Enforcement Considerations

SLA verbiage in the contract should allow jurisdictions to enforce the requirements of the agent error rates, customer service level, and fraudulent transactions.

Risks of Not Implementing the Best Practices

The risks of not implementing the best practices include

- A greater potential of program failure if careful analysis and planning outlined in the best practices is not followed
- A loss of public confidence in the jurisdiction resulting from poor performance by agents
- A requirement for additional jurisdiction resources to correct agent errors
- The potential of loss of tax revenue if fees are not correctly calculated or submitted to the jurisdiction

The availability of a complete business case supporting the third-party program will enhance public legitimacy and acceptance of the program.

Challenges of Implementing the Best Practices

The challenges faced by the jurisdiction in implementing the best practices include:

The time and resources necessary to prepare the business case and operational procedures might be perceived as delaying the implementation of a needed program.

- Not all issues or possibilities can be anticipated. Amendments or requests for exceptions should be expected, and time should be built into the plan to address them.
- The expanded base of newly trained third-party users might expose previously undisclosed risks of fraud and errors that were not evident in jurisdictional-controlled resources and facilities because of differences in procedures or oversight.
- The availability of a complete business case supporting the third-party program will enhance public legitimacy and acceptance of the program.

Chapter 3 Contracts and Memorandums of Understanding

Background

The following section contains a list of recommended contract provisions that the working group has compiled as a reference for jurisdictions to use in developing or amending their contracts with third-party agents. This list is not intended to provide legally sufficient contract language; instead, it is intended to be a checklist of provisions, terms, requirements, and so on.

> *The working group recommends a jurisdiction always have a contract or MOU with any third-party agent processing driver or vehicle transactions.*

A thorough contract between the jurisdiction and the third-party agent is necessary to make certain the residents of the jurisdiction receiving the third-party services know that the service is in compliance with applicable jurisdiction rules, regulations, and procedures—and that their personal information is protected. The contract further serves to protect the jurisdiction from liability that could arise with the third-party agent's transaction processing activity. For these reasons, the working group recommends a jurisdiction always have a contract or MOU with any third-party agent processing driver or vehicle transactions.

The recommended contract provisions below are separated by the functional section that might correspond to a jurisdiction's contract template.

3.1 Recommendations for General Contract Conditions

The general conditions will include the jurisdiction's standard provisions, along with specific recommendations regarding the third-party program. These should include:

- Terms and Definitions – All necessary terms and definitions need to be provided to avoid confusion within the contract, especially when acronyms are used.
- Term or duration of agreement – Set number of years, with renewal terms. Each jurisdiction should determine the appropriate length of the contract with the third-party agent. The working group recommends the contract should be valid for a minimum of not less than one year and more if the agent is expected to make a significant investment in starting a new business. The contract terms should also include provisions for renewal or extension of the agreement.
- Suspension or termination section – This section outlines how each party can terminate the agreement, including terms such as notification period, obligations after terminations, and so on.
- Statement of work – This provides a detailed description of the activities, deliverables, and timelines required for the third-party agent.

3.2 Recommendations for Equipment and Inventory Provisions

An important feature of establishing the program is a determination by the jurisdiction regarding which entity is responsible for providing the necessary equipment and inventory to be utilized by the third-party agents. Many jurisdictions include the equipment and inventory in the contract to ensure that the processing of products is uniform across the service outlets and that the platform meets security requirements defined by the jurisdiction. If the third-party agent is responsible for providing any equipment or inventory, the jurisdiction should be prepared to provide specifications for each item to comply with existing standards. The agreement should also consider which party will be responsible for the cost of periodic upgrade or replacement of hardware and software, or other peripherals.

3.3 Recommendations for Banking and Financial Terms

The contract needs to have clear language covering all fees that can be collected by the agent, including service, convenience, or additional fees that can be charged to the customer.

If the third-party agent is collecting fees on behalf of the jurisdiction, electronic deposits should be established to submit the funds directly into the jurisdiction's account. Reconciliation reports are to be generated and maintained on premise, matching the funds that were transferred. The frequency of the transfer of the jurisdiction funds needs to be specified in the contract terms (e.g., daily, weekly).

The third-party agent should be the responsible party for any uncollected funds owed or any insufficient payments made. There should be an established set of procedures and consequences for any missing funds from the third-party agent.

The jurisdiction's program might permit third-party agents to charge an additional processing fee for the transactions processed; this should be established through statute or rule along with provisions to modify the fee. If the jurisdiction caps the service fees that agents are permitted to collect, the "not-to-exceed" provision should also be included in the contract language.

3.4 Recommendations for Bonding and Insurance Requirements

The contract should specify requirements for financial bonds and insurance the third-party is responsible for obtaining prior to the contract becoming effective. This should include the type of bond or insurance, coverage amount(s), and designation of loss payee entity in the event of a claim.

Insurance or bond provisions that are subject to change, such as the amount of the bond or the term date, need to be monitored by the jurisdiction to ensure continuing compliance with the contracted requirements. If the bond amount is conditional on another data value, such as the number of transactions processed in a six-month period or the value of vehicle transactions, the jurisdiction should notify the agent of the new bond amount and due date for compliance.

Any provision of the bond and insurance requirements that falls out of compliance during the term of the contract should be cause for immediate correction by the third-party. Notice of pending renewal or change should be given with sufficient advance notice to avoid last-minute challenges with maintaining the third-party status.

Additional insurance considerations include

- Cybersecurity insurance that will cover response and recovery costs in the event of a breach. Jurisdiction statute or rules might also require credit monitoring services, a call center, and a breach notification website for individuals affected by the breach.
- Commercial general liability insurance, including bodily injury, personal injury, and property damage, with liability limits in normal jurisdiction practice
- Workers' compensation insurance

3.5 Recommendations for Approval of Advertisements for Services

The contract should grant the jurisdiction the right to approve advertising and use of the jurisdiction's logo in any promotional material. An attachment to the contract might offer specific guidelines for approved advertising, as well as for statements or language that will not be approved.

3.6 Recommendations for Additional Administrative Terms and Conditions

The contract should also list any additional administrative requirements the third-party agent will be required to comply with, such as subcontracting limitations, co-located businesses or conflicts of interest, access to facilities, and relocations.

- Permitted co-location with other businesses and whether prior approval by the jurisdiction is required before the other business is permitted to operate at the requested location
- A conflict of interest policy to ensure employees, shareholders, and directors do not engage in specific prohibited business ventures. The policy should require covered persons to report criminal convictions or other activities that impact their abilities to fulfill their obligations to the contract.
- Ownership changes and relocations and whether approval by the jurisdiction is required prior to the change
- Notification by the parties regarding the impact of a natural disaster or governmental declaration of emergency on business operation
- Permitted access to the third-party business premise by authorized jurisdiction personnel without notice, warrant, or court order, at any reasonable time
- The agreement amendment process, including notification period
- Compliance with Americans with Disabilities Act (ADA) and equivalent rules in Canadian provinces, building access, smoke-free environment, rest room requirements, and parking availability
- Secure location to store inventory
- Provision regarding whether subcontracting of contracted services is permitted and whether prior approval is necessary
- Compliance with REAL ID Act requirements

3.7 Recommendations for Data Privacy and Security Requirements for Third Parties

The data privacy and security requirements should include terms covering jurisdictional data accessed by the third party, stored temporarily on the agent's site during the transaction process and while in transit to and from the jurisdiction. Recommendations for contract provisions regarding data privacy and security and the associated training on these topics include

- Minimum facility standards as determined by the jurisdiction, potentially including physical security, alarms, remote monitoring, and surveillance cameras (including retention time for surveillance footage)
- Data connectivity intent and usage. The third-party will be specifically prohibited from access to the jurisdiction's information systems or any jurisdictional data for any purpose other than as specified in the contract.
- A statement that both the manner in which information is released from the records contained in driver license or title and registration databases and the manner in which the company might access or utilize such information, are regulated by federal, state and provincial laws, including the Federal Driver's Privacy Protection Act (DPPA), 18 United States

Code (U.S.C.) §§ 2721-2725, and equivalent Canadian provincial acts.

- The responsibility of the third party and any individual who acts on the third party's behalf to acquire sufficient working knowledge of all applicable laws and policies that govern access to and the use of customer records

- The penalties for knowingly obtaining, using, or otherwise disclosing personal information obtained from the information systems for a use not permitted under 18 U.S.C. §§ 2721 or Canadian rules. Furthermore, anyone requesting the disclosure of personal information who misrepresents their identity or makes a false statement in connection thereto with the intent to obtain such information in a manner not authorized by law is subject to criminal penalties.

- The penalties for violation of the DPPA or any other applicable federal or state law on the part of the third party or any person acting on its behalf. These types of violations might also constitute grounds for imposing appropriate corrective action(s), including cancellation of the individual's certification, cancellation of the third-party's agreement, and termination of information systems access.

- Confidentiality provisions regarding the disclosure, distribution, or utilization of any confidential or personal information that is connected or otherwise associated with the agreement without prior written consent. The confidential provisions should apply to the company, its current or former officers, its employees, its agents, its subcontractors, and other representatives for the term of the contract.

- Specifications regulating computer equipment and software that are compatible with information systems and connectivity requirements and that allow access only to the specific information systems authorized.

- Requirements that third-party user passwords meet jurisdiction security standards and not be shared between users

- Training requirements for agents and their users on the importance of the safekeeping of records and records management. This training may be delivered by the jurisdiction or the agent or vendor in compliance with jurisdiction requirements. The contract should specify any costs or reimbursement associated with the training.

- Users performing certain transactions might also be subject to certification requirements. If certification is required, the records should indicate the individual meets the qualifications for the certification, has been certified, and the certification remains in good standing.

3.8 Recommendations for Jurisdiction Computer Hardware and Software, Licenses, and Network Connection Requirements

The third party is responsible for complying with the jurisdiction's requirements for computer hardware and software configurations, as well as with maintaining licenses, required upgrades, and network connection standards. These hardware and software requirements may include

- Require the third party to keep a copy of all software licenses related to the performance of the agreement, whether obtained now or in the future, at each established place of business.

- Provide a copy of any vendor or service provider agreement for installation or maintenance of the computer equipment or software that it uses in performing the authorized activities.

- Prior to authorization to commence business, the jurisdiction needs to certify any interface or network access paths that the third party will use to access jurisdictional systems or records. This includes comprehensive testing and evaluation of the technical and nontechnical security features and other safeguards.

- Requirements to correct security deficiencies found during evaluation. Security deficiencies will be corrected at the third party's expense prior to the performance or continuation of any authorized activities.
- The jurisdiction's specifications to establish and maintain hardware, software, and network configuration that complies with the jurisdictional technical requirements.
- The jurisdiction might, without notice, use a remote configuration management tool to evaluate the third-party's configuration to ensure continued compliance.
- Any required changes, upgrades, or maintenance required by the jurisdiction will be at the third-party's expense.
- The third party assumes all risks associated with its connectivity to the jurisdiction, including any disconnection or downtime that might cause the jurisdiction to be temporarily inaccessible.
- The third party pays all line installation, connectivity, maintenance, and other charges related to access to the jurisdiction. Upon termination of the agreement, the third party is responsible for promptly discontinuing access to the jurisdiction information systems and records. The third party will pay for the cost of removing network access.
- The third party also pays all costs incurred in the establishment, acquisition, and operation of the equipment and software utilized to perform the authorized activities, including any fees or charges from a bank or financial institution, and liabilities associated with the status as a credit card merchant.
- The third party will notify the jurisdiction of user termination, suspension, or similar actions within a specified period of time to enable the jurisdiction to disable system access.
- Third-party users will complete the jurisdiction's SSA and security awareness training, as required.

3.9 Recommendations for General Conditions for Maintaining Standards of Performance and Compliance

These recommendations include the administration of the performance standards, how they will be adjusted during the term of the contract, and communication expectations between the parties. These additional provisions should be included as an appendix or addendum to the base contract so they can be updated or modified without amending the base contract. These recommendations might include:

- Reserve the right for the jurisdiction to periodically modify performance objectives and minimum targets. Jurisdictions should provide at least 21 business days' notice to agents before implementing the new requirements.
- Define how feedback will be provided by the jurisdiction to the third party within a specified number of business days after each month or after a quality control audit has been conducted. The feedback should include compliance with quality and performance measurements.
- Third-party compliance with applicable federal, jurisdiction, and local statutes and regulations, including all procedures, training materials, operation manuals, guidelines, and other directives provided in writing.
- A progressive disciplinary process, including participation in all discussions and hearings regarding performance, with escalating enforcement options if the third-party fails to comply with contract provisions or standards of performance.

- Third-party cooperation with the jurisdiction, contractors, subcontractors, law enforcement agencies, and all other state, county, and local government officials when required.

- The third party should maintain data and reports relating to its compliance with the standards of performance and provide those upon request by the jurisdiction.

Benefits of Implementing the Best Practices for Contracts and MOUs

The benefits of following the recommended best practices for these contract and MOU provisions include

- Allows the jurisdiction the ability to terminate the agreement, for cause, and allows the third-party agent to terminate if it does not wish to continue the business venture

- Applies uniform and consistent standards and security requirement across all service outlets

- Provides the third-party with a clear understanding of its responsibility for fee collection and fee submission

- Establishes primary insurance coverage requirements that will cover claims resulting from an act, omission, or negligence of the agent or its officers, representatives, or employees

- Ensures agent advertisements fall within jurisdiction policy and guidelines

- Establishes the principal of pre-approval of co-locations to ensure they meet jurisdiction requirements

- Enables the jurisdiction authorization to access the premise for auditing

- Provides the third-party agent with its responsibilities for customer information confidentiality

- Establishes the corrective actions for violation of these provisions

- Defines a framework to allow third-party agents and the jurisdiction's system to interface with each other and work together

- Reduces and mitigates noncompliance

- Ensures compliance with state and federal laws

Risks of Not Implementing the Best Practices

The risks of not following the recommended best practices for these contract and MOU provisions include

- Risk for claims that might be caused by an act, omission, or negligence of third-party agents

- Risk of cybersecurity breach(s) and jurisdictional liability for customer data being released

- Risk of a location not meeting ADA requirements

- Risk of damage to the image, respect, and public perception of the jurisdiction by poor or inaccurate agent service

- Customers impacted financially by potential fraud implications from loss of Personally Identifiable Information (PII) and other data

- Limited or omission of a "right to audit" clause will restrict the jurisdiction's ability to perform quality control on the agent's work

Challenges of Implementing the Best Practices

- Current rules, laws, and policies might limit the jurisdiction's authority to specify certain contract or MOU terms.

- Existing agents might have employee contract agreements limiting the corrective action that can be taken for errors or poor performance.

Chapter 4 Standards of Performance

A key provision of the program for a third-party agent is the definition of performance standards that the agent will need to comply with to maintain the authorization and to continue to process jurisdictional transactions. This is supported by provisions outlined in the Chapter 3 (Contracts and Memorandums of Understanding) of this document.

The third-party program should include quality assurance and quality control activities (see the Glossary of Terms and Acronyms) to ensure a high level of integrity when completing transactions and to permit the early identification of any issues and problems related to staff performance. Both parties will have responsibility in conducting quality control and maintaining records of the activity.

The third-party program should include quality assurance and quality control activities to ensure a quality process in the completion of the transaction and to permit the early identification of any issues and problems related to staff performance.

Quality Assurance

The following quality assurance provisions are recommended for ensuring the third-party contract supports the jurisdiction quality and training standards for documents issued on the jurisdiction's behalf.

The quality assurance provisions in the contract enforce the jurisdiction's quality standards for transactions completed by a third-party. The provisions shown here are recommended for inclusion in the supporting documents attached to the contract.

- A definition of the quality standards, as well as the data security and data privacy enforcement conditions that are required by the third party
- A detailed specification of all data security and data privacy requirements

4.1 Recommendations for an Agent Quality Assurance Program

The agent will establish its own quality assurance plan to ensure that jurisdiction policies and procedures are being followed to quickly identify and rectify issues. Individuals acting on the third-party's behalf are required to process transactions in such a manner that consistently demonstrates a satisfactory degree of knowledge, skill, and competence in the motor vehicle program requirements applicable to the work being completed. (NOTE: The working group solicited and received input from a stakeholder group of vendors and third-party agents, both in writing and at an in-person meeting, where the vendor community offered examples of quality assurance practices that are designed to meet or exceed jurisdiction requirements.)

4.2 Recommendations for Background Checks

The jurisdiction should require individuals processing transactions to undergo initial and periodic background checks. These might include fingerprint-based background checks, financial credit checks, or both. For any staff involved in the issuance or production of REAL ID driver licenses and identification cards, these checks must comply with the REAL ID Act.

4.3 Recommendations for Certification Requirements

Individuals performing certain transactions might be subject to certification requirements. If certification is required, the records need to indicate the individual meets the qualifications for the certification, the individual has been certified, and the certification remains in good standing. For example:

- Individuals conducting driver license testing will be required to (1) hold a valid driver license and all necessary endorsements for the operation of the vehicle in which written or demonstrative skills tests are to be administered and (2) not have had his or her driving privileges revoked or suspended in any jurisdiction.
- Upon notification that an individual who conducts driver license skills and written testing or processing has (1) a suspended, revoked, canceled, or disqualified driver license or (2) a vehicle registration suspended or cancelled by the department in connection with a moving violation or a failure to maintain insurance, the individual will no longer be authorized to perform the authorized transactions by the third party.

4.4 Recommendations for Training Requirements

Training and proof of completion requirements for agents support the objectives of a quality assurance program by providing knowledge on standards and written procedures. Agent training covers the transaction processing procedures and documentation requirements to produce accurate credentials consistent with requirements set forth by the jurisdiction and the safekeeping of records and records management.

The jurisdiction will require all authorized users or agents to attend the necessary training to ensure the driver license or motor vehicle services performed by the agent are consistent with state, provincial, and federal laws and conform to the policies and procedures identified by the jurisdiction.

The jurisdiction should require authorized users and agents to complete ongoing training when necessary because of changes in law, policies, procedures, or data security practices. Additional training might also be necessary in the event of a system upgrade or enhancement. Remediation training should be provided as well as in the event of poor performance or noncompliance with standards of the jurisdiction.

Agents should review the jurisdiction policies and procedures on an annual basis to ensure familiarity with the proper issuance protocols. Each authorized user will be required to sign an annual acknowledgement of understanding.

The third party and all individuals performing transactions will maintain compliance with all training requirements and will participate in all educational and support sessions and other informational meetings prescribed, at their own expense. This includes both training for new hires, ongoing training on new laws or procedures, and safekeeping of records.

Agents attending training conducted at a jurisdictional site will comply with specified rules, policies, and procedures.

4.5 Recommendations for User Accounts

The third party should make prompt notification when there is a change in either an agent's application information or the status with the company. To make certain the agent's user accounts are being maintained with only authorized individuals:

- The jurisdiction should conduct an annual user audit to determine if users are still employed with the third-party agent and that their roles are still appropriate.
- If there is no user activity in a specified period of time, then the account should be suspended until the status of the user is determined.

4.6 Recommendations for Certification Retention

All certification and training documents should be maintained for a determined period at the third-party's business address and made available upon request of the jurisdiction.

4.7 Recommendations for Support Resources

The third-party agent and individuals processing the records on behalf of the jurisdiction should be provided with specific contacts or a dedicated help desk for assistance with unusual transactions or suspected fraud. The agent should also have access to printed or online resources from the jurisdiction regarding current policies and procedures.

When a vendor is providing a software system for third-party agents to use in preparing transactions for the jurisdiction, the vendor should support a first-level help desk to field agent questions on transaction processing or connection issues and so on. The agents should be required to direct those inquires to the vendor resource before elevating an issue to the jurisdiction.

4.8 Recommendations for Fraud Prevention Analytics

The jurisdiction should use software that prevents third-party agents from making unauthorized overrides and ensures data is accurate and complete. (See also Chapter 5, Program Compliance, Oversight, and Sanctions and Chapter 6, Fraud and Fraud Deterrence.)

4.9 Recommendations for Data Security and Data Privacy Requirements

The jurisdiction may ultimately be accountable in the event of a data leak or misuse of data due to fraud. This means that the quality assurance process needs to include verification of the agent's compliance with the jurisdiction's data security and data privacy requirements. Compliance includes training and certification requirements, access to confidential personal information, unauthorized disclosure of information, and provisions in the event of a data breach.

For additional information and specific recommendations on data security and data privacy, please see Managing Data Privacy and External Access Best Practice *from the AAMVA Managing Data Privacy and External Access working group for the most current discussion of this topic.*

Quality Control

This section includes recommended conditions for quality control, data security and data privacy enforcement, transaction quality control, and compliance audits. The standards of performance provisions provided in this section will enable the jurisdiction to verify the third party is in compliance with the contract terms and that the completed transactions meet the jurisdictions requirements.

The following quality control items are recommended for the supporting documents attached to the contract.

- A Quality Expectations Matrix defining what constitutes an error and identifying how severity ratings are assigned to different types of errors
- How transactions or documents submitted by a third-party will be selected for a quality review. This could include both a random selection and a frequency based on past performance.
- A requirement to keep complete and accurate records available for inspection by the jurisdiction
- When applicable, ensure all required documents have been submitted or scanned prior to destruction and follow the contract's record retention requirements.

4.10 Recommendations for Reporting Errors

Errors should be reported to the agent within the defined time frame determined by the jurisdiction or after the scheduled quality control audit is completed. The report should include the accuracy rate for each user reviewed and an accuracy error rate for the sampled transactions. The report should identify each error that was found so the agent is aware of the areas that need improvement. The report should include the expectations on accuracy and describe disciplinary action of poor performance.

4.11 Recommendations for Correcting Errors

A quality control audit of third-party transactions will be conducted by the third-party as a part of its quality program or as a step in the jurisdictions audit program. During the quality control review, any errors that affect the customer record, such as incorrect name entered on a title or driver license, should be corrected. Depending on the contract or MOU with the third-party agent, the agent might be asked to make the correction, or the correction will be completed by the jurisdiction and the error reported to the agent.

The accuracy of the corrected errors should be reviewed to ensure satisfaction of the jurisdiction.

4.12 Recommendations for Record-Keeping

Third-party agents need to comply with jurisdiction record-keeping requirements for complete and accurate records relating to the provision of the transaction services and the administration of the agreement. The agent will be required to follow jurisdictional record retention policies. In the event of the contract terminating prior to scheduled destruction of the records, the agent will return all records to the jurisdiction.

Jurisdictions should confirm all required documents have been submitted or scanned prior to destruction.

Benefits of Implementing the Best Practices Regarding Standards of Performance

The benefits of following the recommended Best Practices for contracts and MOUs include

- Reduction and mitigation of noncompliance or fraud risk
- Improvements in data quality and data reliability that enhance program efficiency and effectiveness
- Prevention of errors and detection of potential issues before they become impactful
- Compliance with state and federal laws
- Engagement and empowerment of staff through ongoing training and performance accountability

Risks of Not Implementing the Best Practices

- Ineffective penalties and sanctions for noncompliance result in not meeting jurisdiction quality standards.
- Poor performance is allowed to continue.
- Errors and quality problems diminish the image, respect, and public perception of the jurisdiction.
- Data breach or release of customers' PII results in financial loss or identity theft.
- The jurisdiction faces civil liability resulting from improper credential issuance.

Challenges of Implementing the Best Practices

- Current rules, laws, contracts, or policies might impede the jurisdiction's authority to impose corrective actions.
- Limited jurisdiction audit and IT staff resources are needed to implement, operate, and manage quality control programs.
- Costs and resources are needed for initial and ongoing training.

Chapter 5 Program Compliance, Oversight, and Sanctions

The contract sets the requirements for the agent and defines the performance requirements for the user to maintain compliance with those provisions. For the jurisdiction to effectively manage the program, the contract will need to contain quality assurance processes, quality control steps, and a contract compliance process, including audits and other oversight to monitor performance. In this section, the recommendations focus on the operation of the contracts and conducting audits or other oversight of third-party agents.

> *For the jurisdiction to effectively manage the program, the contract will need to contain quality assurance processes, quality control steps, and a contract compliance process, including audits and other oversight to monitor performance.*

Compliance Audit

The compliance audit is a quality control review completed by the jurisdiction. The compliance audit is used as a tool for monitoring the quality rating of an agent, contract compliance, financial compliance, and fraud prevention. The compliance audit will also review the overall security of inventory issued to the agent and security of PII. Many inspection techniques can be used, including error flags generated by the system or manual inspections of documents to compare what was entered in the customer record to the actual document. Compliance audits can be completed at the agent's location or, often, designated staff at the jurisdiction site perform the reviews as a part of the overall compliance audit program.

The reviews evaluate the quality of the transactions submitted by the agent and compliance with all regulations, policies, procedures, and contract terms.

Process for Selecting Agents or Transactions to Review

Agents might be selected for review based on the fact they are new to the third-party program, the jurisdiction has a routine periodic review cycle, or they come to the attention of audit staff because of special circumstances.

- New agents are a focus of special attention to make certain they understand, and are applying, rules and procedures for completing the transactions.
- Auditing agents within a regular cycle ensures quality standards are being met.
- Quality control and compliance audits may occur outside the periodic cycle when evidence indicates a reason for attention. If the jurisdiction encounters suspicious transactions, alerts coming from system monitoring tools, fraud tips, or other sources, this can trigger a closer look at the agent or work products.
- The percentage of documents reviewed depends on the quality review success rate of the agent or user. All transactions processed by a new user should be reviewed until the reviewer can be assured the new user meets the performance standards. In ongoing operations, a user with a higher error rate should be subject to a higher percentage of review to identify skill or knowledge deficiencies.

Whether the audit is a routine periodic review or being performed for another reason, the recommendations below cover the types of reviews and the important content.

5.1 Recommendations for New Agent Audits

After a contract has been signed and inventory has been issued to an agent, an audit should be conducted within 30 to 60 business days to confirm transactions are completed accurately. New agents should receive continued oversight until the standards of performance are achieved.

5.2 Recommendations for Regular Cycle Audits

Typically, a jurisdiction will assign each third-party agent to a regular cycle for periodic audits. The agent might expect to have a review of its completed transactions through either an on-site or remote audit on a yearly or other periodic basis.

5.3 Recommendations for For-Cause Quality Control Audits

A for-cause quality control audit is initiated by the jurisdiction, law enforcement, or customer or by a complaint to the jurisdiction. These can be requested for any number of reasons by different areas within the jurisdiction. Often, these audits are the result of routine daily quality control reviews or in response to a complaint about an error or incorrect issuance action.

5.4 Recommendations for Agent-Requested Audits

An agent can request a quality review audit if it has suspicions of noncompliance or wants to take a proactive approach to ensure compliance.

5.5 Recommendations for Quality Control Re-audits

These audits are performed when an agent's quality rating is below the jurisdiction's standard. After notification to the agent of the audit findings, additional training is conducted. A re-audit is then completed to determine if the agent has implemented corrective actions and is now within an acceptable quality rating.

5.6 Recommended Quality Control Items to Review

Jurisdictions conduct a quality control review based on statutes, administrative rules, policies, and procedures. When selecting transactions for audit, it is helpful to have a system-generated random sample of items subject to the quality review. Multiple tools are available to assist the jurisdiction staff create the unbiased sample set, including Microsoft Excel formulas and other data analytical tools.

Items subject to review should include the following, when applicable:

- All forms and applications are completed in full and included, attached, or scanned.
- Owner, vehicle, driver and other information from the application are accurately captured.
- Applicable policies, procedures, and so on are followed for the processed transaction.
- Proof of vehicle ownership documents are present and completed in full.
- Odometer disclosure is properly completed.
- Any odometer brand or designation is accurate (e.g., Actual, Not Actual, Exceeds Mechanical Limits, Exempt).
- Vehicle Identification Number (VIN) verification is accurate.
- Applicable taxes and fees are collected.

- Valid proof of identify was presented with transactions.
- Valid notarization is completed by the authorized party.
- Power of attorney is provided, when applicable.
- Lien status is properly recorded.
- Brands are recorded.
- Death certificates, wills, and so on are included with supporting documentation, when required.
- Review was completed for any fraudulent documents or fraudulent identification.
- Data privacy requirements have been adhered to.
- Proof has been provided of legal name, date of birth, SSN, and address for driver license and identification card issuance.
- Proof of legal presence has been documented.
- REAL ID–required identification documents were verified and included.
- External systems verifications, such as SAVE and SSOLV, are completed.
- Driver endorsement privilege documentation is provided.
- Sanction and insurance documentation is provided.

5.7 Recommended Financial Audit (Fees Due to Jurisdiction)

The financial audit of fees that are due to the jurisdiction should be part of both routine audits and unannounced audits.

5.8 Recommendations for Voided Transactions

The best practice is that third-party agents should not be permitted to void transactions. System or resource limitations in some jurisdictions might require the agent to have a void capability. In the event the agent has the ability to void the transaction, the procedure should limit the capability (e.g., same day only) and require a manager or supervisor override on voided transactions. If this is not possible, all voided transactions should be reviewed to verify proper documentation was submitted and to certify revenue is properly accounted for.

5.9 Recommendation for Fee Adjustments

A sample of fee overrides, reversed payments, waivers, and payment adjustments should be reviewed to ensure the integrity of the transaction and that the alteration in fees collected was appropriate.

5.10 Recommendation for Deposit Audit Requirements by Location

Review of the daily Automated Clearing House (ACH) transfers being conducted is accurate, and the documentation is being maintained at the agent's location.

5.11 Recommendation for Random Drawer Audit

Randomly select drawers to reconcile with daily activity to confirm proper collection of funds.

5.12 Recommendations for Site Visits

Site visits are conducted by the jurisdiction at the agent's location. These audits might be scheduled or unannounced. The recommended on-site audit includes a review of completed transactions and will make certain the location is in compliance with terms and operating procedures. A checklist of on-site audit items might include:

- Required signage or certifications displayed in public view

- Documented completion of current criminal history checks for applicable users
- Compliance with REAL ID Act facility requirements
- Verification of updated training certificates
- Signed confidentiality agreement for applicable users
- Adherence to physical security requirements and inventory of registration decals, title paper, credentials, license plates, other controlled documents, and other equipment
- Verification of current list of user access credentials (to prevent someone from using a previous user's credentials)
- Internal (agent) quality assurance plan showing agent is monitoring its users
- Sample of internal audit documentation
- Agent compliance with documentation retention, destruction, and scanning requirements
- Verify deposit documents are being retained based on the respective retention schedule

Quality Review Accuracy Standards

A quality expectation should be established for the agents based on similar accuracy standards for jurisdictional staff performing similar work. For example, the working group reviewed jurisdiction-established quality ratings, and they range from 90% to 98% for transactions processed. The quality expectations and standards should be identified within the contract. Furthermore, the working group found that after creating an established quality rating, jurisdictions were able to monitor the agents via the dashboard view of the quality review process. This can be used for further follow-up procedures and to identify success of training, quality assurance process, and overall program success.

The following is an example of a quality rating dashboard display and items that should be tracked at a minimum.

Quality Rating Dashboard Example

	Green	Yellow	Red
Quality rating of transactions processed	90–100	85–89	1–84
Quality rating of paperwork completed by the agent	90–100	85–89	1–84
Supporting documents submitted and scanned (in business days)	1–10	11–19	20 or more
Fee waiver compliance quality rating	90–100	85–89	1–84

Quality Expectations Matrix

The quality expectations matrix defines errors, the severity of errors, and corrective actions needed to mitigate further noncompliance. At a minimum, the following should be included in the quality expectations matrix:

- Error definition – Errors may be counted or weighted differently depending on the impact on the product or the corrective action necessary. (For example: Can one transaction have multiple errors? What is the severity or impact of the error for quality control purposes?)
- Critical errors – errors placing the jurisdiction or stakeholder at risk of financial loss or claim against their bond or resulting in the recall or cancelation of credentials
- Noncritical errors – errors requiring correction to the record, resulting in special handling or requiring refresher training

Correcting Poor Performance

Effective oversight of the agent requires the jurisdiction handle poor performance on a transaction level, as well as on a contract level. The corrective action for poor performance can range from increased audit and monetary penalties to suspension or cancellation of the user or agent contract. The contract should define the error and corrective process, steps to escalate the correction of poor performance, and time frames for correcting the performance deficiencies. Some jurisdictions might charge a monetary fine for agent errors. Assessing and collecting monetary penalties can be challenging with a commercial agent and might not be an option with governmental agents. At a minimum, the agent should be required to pay any title or registration fee to print the corrected customer credentials when an error affects the customer's record.

The third-party agent needs to agree to participate in and comply with the jurisdiction's performance measures and reporting requirements. Failure to comply with performance measures will subject the agent to corrective actions the jurisdiction deems necessary and appropriate. These corrective action measures should be identified within the third-party contract or MOU. The performance measurements or quality rating is intended to specify the required minimum quality assurance standards that all authorized agents conform and adhere to.

Although many jurisdictions have an instant or over-the-counter title issuance process, the working group identified that inserting a holding period before the title is printed and mailed promotes error detection and self-reporting by agents. If the jurisdiction provides a five-business-day holding period for a title print (for non-electronic title records) and allows the agent to report an error to the jurisdiction for correction of the data or fees, then the correction should be completed without penalty during that period. This will promote a better awareness and quality review from the agents themselves.

Failure to comply with performance measures will subject the agent to corrective actions the jurisdiction deems necessary and appropriate.

5.13 Recommendations for Steps to Handle Poor Performance

Third-party agents need to receive training prior to processing transactions. Training should involve knowledge of jurisdiction policies and procedures, documentation requirements, data privacy, and fraud detection and prevention. Additional training should be required when an agent falls below the quality standard ratings for at least two consecutive audit time frames. If training issues arise in a train-the-trainer approach, the jurisdiction should retrain the trainer.

Additional quality reviews might be required based on low quality ratings or poor performance to make certain the poor performance is fully remedied to the satisfaction of the jurisdiction.

Additional training should be required when an agent falls below the quality standard ratings for at least two consecutive audit time frames.

Recommended corrective actions might include

- Written warnings – identifying the prohibited acts or poor performance to the agent in a documented format
- Probation – jurisdiction conducting additional quality reviews or restrict certain functions during a period of probation
- Suspension – temporarily withdrawing a user's or an agent's access to do business on behalf of the jurisdiction
- Termination – permanently withdrawing a user's or an agent's access to do business on behalf of the jurisdiction

Additional corrective actions might be appropriate for financial misconduct or fraud. Corrective actions might include

- Monetary compensation
- Termination
- Criminal charges

If an agent has not remedied the conduct resulting in the suspension by the stated time frame, the suspension should continue until the act or omission is fully remedied to the satisfaction of the jurisdiction. Providing a listing of poor performance and prohibited conduct establishes the expectation from the jurisdiction to the agent. This list should identify warnings or specific periods of suspension for each prohibited act. This ensures a consistent approach for any violations found during the quality control and audit review process and allows for equal treatment between agents that might have conducted similar prohibited acts.

For agents involved in the issuance of driver license documents, the REAL ID Act contains a specific list of prohibited acts for covered employees that provides for permanent and interim disqualifying criminal offenses related to a person's ability to be involved in the manufacture or production of REAL ID driver licenses and identification cards. This is provided for in 49 Code of Federal Regulations (CFR) 1572.103(a) and 49 CFR 1572.103 (b).

5.14 Recommendations for Imposing Sanctions

Certain serious activities or actions by an agent or user of the agent may be cause for a sanction being placed on the agent. The jurisdiction should identify all prohibited acts or omissions within its third-party agents' policy framework. An example of how the jurisdiction may describe prohibited acts or omissions and the appropriate sanction that could be applied is below.

Prohibited Acts and Sanctions Example

Prohibited Act or Omission	Sanction for First Violation	Sanction for Second Violation	Sanction for Third or Subsequent Violation
The agent's user has sold, published, disclosed, reproduced, or used a customer record obtained through online access to jurisdiction records.	Termination of the user's access and permanent ban on future access with any agent	Termination of the agent's online access	
The agent has sold, published, disclosed, reproduced, or used a customer record obtained through online access to jurisdiction records.	Termination of the agent's access and permanent ban on future access with the jurisdiction		
The agent's user has failed to maintain a 90% average accuracy quality rating in processing motor vehicle or driver licensing transactions.	Written warning and the user required to attend mandatory refresher training	Suspension of online access for a period determined by the jurisdiction	Termination of the agent's online access
The agent or their user has committed fraud or accepted payments for falsifying the administration or reporting of driver skills or knowledge tests.	Termination of the agent's agreement and permanent ban on future driver license third-party services		

Benefits of Implementing the Best Practices

The benefits of following the recommended best practices for program compliance and oversight include

- Identifying noncompliance in issuance transactions and mitigating risks resulting from noncompliance with procedures and rules
- Improving data quality and data reliability to enhance program efficiency and effectiveness
- Complying with state and federal laws and jurisdiction policy and procedures

Enforcement Considerations

- Determine who is responsible for program quality enforcement and provide appropriate authority and resources to enforce sanctions.

Risks of Not Implementing the Best Practices

- Penalties and sanctions for poor quality might be limited or nonexistent in jurisdiction rules or statute.
- Poor performance will continue without repercussion.
- Jurisdiction might face civil liability by allowing improper issuance processes.

Challenges of Implementing the Best Practices

- Current rules, laws, and policies limiting authority and implementation opportunities
- Existing employee contract agreements limiting implementation and corrective action
- Staff and IT resources needed to implement, operate, and manage programs
- Costs and resources needed for training
- Local government entities may have processes and agreements that would impede program implementation.

Chapter 6 Fraud and Fraud Deterrence

Fraud detection and deterrence measures provide appropriate internal controls to help mitigate the risk of internal and external fraud. A well-versed team assigned to detect and deter fraud can become a valuable resource to the jurisdiction and should be consulted prior to changing any product issuance processes. Documents issued by the jurisdiction can be highly valuable to criminals. Driver licenses and identification cards are prime targets for fraud because when they are obtained by an individual acting deceitfully, the documents can be used to perpetrate other types of fraud. Vehicle fraud, also a common crime, occurs when persons committing acts of fraud obtain a vehicle title or other documentation that could be utilized to obtain illegal ownership of the vehicle or to drastically change a vehicle's value (e.g., brand washing, odometer tampering, stolen vehicle cloning). In most jurisdictions, fraud requires an intent to commit actions deceitfully with personal gain.

Internal Fraud

Internal fraud occurs by perpetrators who are employed by the jurisdiction, in association with the jurisdiction or agents of the jurisdiction. These types of internal fraud crimes include altering existing records, creating fictitious records, performing unauthorized overrides, and illegally providing documents to those not entitled.

External Fraud

External fraud occurs by perpetrators who receive services from the jurisdiction or agents of the jurisdiction. External fraud is committed by consumers obtaining legitimately issued credentials from the jurisdiction through illegitimate means. This can result from criminals submitting counterfeit or altered documents, impersonation, or forgery.

Fraud Prevention Tools

The resources listed below provide tools and processes available in detecting and deterring fraudulent activity involving the jurisdiction and its agents. Please note that this listing is not comprehensive because tools and processes for the detection and deterrence of fraud are always advancing.

The AAMVA community has produced three best practices documents addressing fraud prevention and resources available on the AAMVA website. These documents have recommendations for fraud detection and prevention practices that can also be applied to the management of third-party agents and help prevent fraud from occurring in these programs. These include

AAMVA Best Practices for the Deterrence and Detection of Fraud (March 2015)

- An investigative unit assigned to DMV-related fraud
- Regular and routine auditing of agents
- Regular rotation of staff duties
- Mandatory leave for administrators and auditors

AAMVA Facial Recognition Program Best Practices, Edition 2 (December 2019)

- Facial recognition software for program development and enhancement

- Benefits to detect internal and external fraud
- Value of locating clerical and data errors

AAMVA Best Practices for the Prevention of Abandoned Vehicle & Mechanic's Lien Fraud (March 2020)

- Fraud elements during the possessory lien vehicle registration and title process
- Verification and audit procedures utilized to review the application process
- Training and resources

Additional AAMVA Fraud Prevention Resources

Over the years, AAMVA's focus on security has resulted in several resources that are available to jurisdictions to deter, prevent, or identify fraudulent actions and to enhance the trust of jurisdictional data and credentials. These resources and recommendations include the following:

- Recommendations on the use of biometric login software for jurisdictions staff and external agents, such as fingerprint readers – The use of these items prevents the misuse of login credentials used to commit fraud.
- AAMVA resources, including – National Motor Vehicle Title Information System (NMVTIS), SSOLV, State-to-State Verification Service (S2S), Problem Driver Pointer System (PDPS), and so on. For a link to each available resource, see *AMVAA.org/Law-Enforcement.*
- AAMVA Fraud Detection and Remediation (FDR) training – AAMVA's premier fraud training containing lesson modules and supplements that develop skills in the authentication of documents and detection of imposter fraud, internal fraud, and more. To learn more about FDR, visit https://www.aamva.org/FDR-Training.
- Partnerships with law enforcement entities, other AAMVA jurisdictions, and other groups, such as the National Insurance Crime Bureau (NICB), to identify and deter new and upcoming fraud trends
- Recommendations on the separation or splitting of key duties in the handling of cash or funds, document verification, jurisdictional assets, and transaction overrides

Data Analytical Tools for Fraud Detection

Data analytical tools identify anomalies, bring attention to questionable transactions, and discover potential fraud trends for both internal and external agents. These tools are very useful in identifying fraud. However, identifying the problem is only the first step. Fully leveraging the value of the data produced by the analytical tools requires the jurisdiction to allocate resources to review the data and apply the results to detect and deter fraud. Examples of how data analysis can be used to detect fraud include

- Comparing the reported sales price of a vehicle with vehicle valuation service data can identify potential tax fraud if the purchaser reports a price that is substantially lower than the market price. NOTE: Analysis such as this may require a MOU between state agencies if the collection of vehicle sales data and tax collections are completed by separate agencies (e.g., the jurisdiction collects sales data via title applications and provides that information to a Department of Revenue for further investigation).

> *Data analytical tools identify anomalies, bring attention to questionable transactions, and discover potential fraud trends for both internal and external agents. These tools are very useful in identifying fraud.*

- Comparing an individual's driver license address with their vehicle(s) registration address can identify fraudulent activity related to misreporting a vehicle's location. For example, a person may attempt to avoid emission testing requirements or local property tax by claiming a vehicle is garaged or used in a different location than the resident's home address. This requires FTE resources to follow up on discrepancies and take administrative action.
- Searching for anomalies between personal identity and vehicle transactions to uncover suspicious transactions and patterns of fraud within a defined geographical area or issuance office or by specific staff. If a person committing fraud is colluding with someone at the jurisdiction or going to multiple offices to try to get a suspect transaction approved, the pattern of transactions or other activity may look different from comparable offices or staff.
- Analyzing data to identify high volumes of user fee overrides or disproportionate transaction types tied to one individual can point to potential fraud.

6.1 Recommendations for Having a Dedicated Fraud Enforcement Staff Within the Jurisdiction

Specific jurisdiction staff should be assigned for internal and external fraud detection and deterrence. For times when potential criminal activity is found, having access to law enforcement resources with the ability to complete a criminal investigation and pursue criminal charges is important for the success of the case. It is valuable to identify these resources when developing fraud prevention and detection tools; without following up on the findings, results will be limited, and long-term fraud deterrence might be hindered.

6.2 Recommendations for Equipment and Support

A skilled team of fraud investigators needs to be supported by analysts and have access to technology to effectively fulfill the team's tasks. The overall fraud prevention program for a jurisdiction should include the tools and staff to extend those capabilities to the third-party agent oversight.

6.3 Recommendations for Training

Methods in which fraud is committed is continuously evolving. It is important that jurisdictions provide ongoing training, such as AAMVA's FDR training. (See Section 6.4.) The training should be conducted with staff and a team of investigators to ensure the agents are current on trends in the industry.

6.4 Recommendations for AAMVA FDR Training

AAMVA has developed and deployed a resource to assist jurisdictions by training agents and staff to identify fraudulent documents and practices, both internally and externally. Jurisdictions with third-party agent programs should require all users with direct contact or oversight of vehicle and identification-related documents to complete the AAMVA FDR training.

Benefits

A successful fraud detection and deterrence program ensures proper controls are in place to mitigate the risks of not implementing, as identified below.

Risks of Not Implementing the Best Practices

- PII may be vulnerable to misuse or fraud.
- A clean (nonbranded) title may be issued for a vehicle that is not safe to operate or result in financial losses for the buyer.

- The issuance of driver licenses and personal identity credentials containing false or inaccurate information might result in someone being granted privileges they may not be entitled to.
- Persons committing fraud to obtain driver license or vehicle credentials may use the documents to commit financial crimes or other crimes.
- The jurisdiction, agent, or both might be exposed to increased liability claims resulting from inadequate fraud protection processes.
- The jurisdiction, agent, or both might experience significant negative media attention and public scrutiny as a result of internal and external criminal activity.

Challenges of Implementing the Best Practices

- Training staff in fraud prevention and detection requires financial resources and time. This training will need to be ongoing.
- Offices might need to be closed to provide staff training. This requires public notice and education to other government leaders.
- Fraud prevention and detection tools require an investment in hardware and software, as well as ongoing operational costs, such as staff time.

Appendix A Third-Party Agent Usage by Jurisdiction

AAMVA member jurisdictions and vendors were asked to respond to a survey on how they engage third-party agents. The table below is a compiled list by jurisdiction. This information is believed to be current as of April 2020. The columns show the types of transactions agents perform for the jurisdiction using the following guidelines. NOTE: Lien records are recorded separately in Canadian jurisdictions, and they do not issue vehicle titles.

Third-party agent transaction types:

1. Financial Electronic Lien and Title (ELT) – add, modify or delete lien transactions submitted by or on behalf of a financial institution
2. Dealer ERT/EVR – electronic registration and title/electronic vehicle registration transactions submitted by or on behalf of a licensed dealer. These transactions can be submitted using a vendor or through a jurisdiction portal or access point.
3. Registration renewal transactions fee collection and renewal transaction update, with or without renewal decal issuance, by a third party. These include auto club, retail outlet, inspection station, kiosk located outside of the motor vehicle premises, and so on.
4. Title and registration – include title transfer, renewals, duplicates, and so on completed by third-party agent(s)
5. Driver testing – knowledge or skills testing for non-CDL, instruction permit, or motorcycle endorsement
6. Driver license and ID issuance – include eligibility determination, identity verification, and recommendation for the jurisdiction to complete the issuance
7. Driver control – include evaluation and recommendations regarding driver competency, medical qualifications (not CDL), or habitual violator status

State	1 Financial ELT	2 Dealer ERT/EVR	3 Registration Renewal	4 Title and Registration	5 Driver Testing	6 Driver or ID Issuance	7 Driver Control	Notes
Alabama	N	N	Y	Y	Y*	N	N	*Noncommercial third-party personnel only administer the skills portion of the test.
Alaska	N	N	Y	Y	Y	Y	N	Business partner services vary by location
Alberta	N/A	Y	Y	Y	Y*	Y	N	*Driver license skills testing is done by the jurisdiction; knowledge testing is done by the third-party agent.
Arizona	Y	Y	Y	Y	Y	Y	Y	
Arkansas	N	N	N	N	N	N	N	

(continued)

State	1 Financial ELT	2 Dealer ERT/EVR	3 Registration Renewal	4 Title and Registration	5 Driver Testing	6 Driver or ID Issuance	7 Driver Control	Notes
British Columbia	N	Y	Y	Y	Y	N	N	
California	Y	Y	Y	Y	N	N	N	
Colorado	Y	Y	Y	Y	Y	N	N	
Connecticut	N	Y*	N	N	Y†	Y	N	*Dealers perform titling and registration services directly from their own premises. † Driving schools skills testing
Delaware	N	N	N	N	N	N	N	
District of Columbia	N	N	N	N	N	N	N	
Florida	Y	Y	Y	Y	Y	Y	Y*	*Driver control section, which falls under the Bureau of Motorist Compliance
Georgia	Y	Y	Y	Y	Y	N	Y*	*Medical accommodations
Hawaii	Y*	N	N	N	N	N	N	Oahu County only
Idaho	Y	N	Y	Y	Y	Y	N	
Illinois	N*	Y	Y	Y†	Y	N	N	*Pending legislation to enable ELT †Processing by agent; audit and issuance by Secretary of State
Indiana	N*	Y	Y	Y	N	N	N	*ELT may be planned for 2020
Iowa	Y	Y	N	N	Y*	N	N	*High school students
Kansas	Y	N	Y	Y	Y	N	N	
Kentucky	N	N	N	N	N	N	N	
Louisiana	Y	Y	Y	Y	N	Y	N	
Maine	N	N	N	Y	N	Y*	N	*Limited renewal transactions at AAA
Manitoba	N/A	N	Y	Y	N	Y	N	
Maryland	Y	Y	Y	N	N	N	N	
Massachusetts	Y	Y	Y*	Y*	N	Y*	N	*RMV offers limited services (e.g., duplicate, renewal) at the auto club
Michigan	N*	Y	N	N	Y	N	N	*ELT is planned; all skills testing is done by third-party services
Minnesota	N	Y	Y	Y	N	Y	N	
Mississippi	N	N	Y*	Y*	Y	Y	Y	*Department of Revenue processes all title transactions
Missouri	Y	N	Y	Y	N	N	N	
Montana	Y	N	Y	Y	N	Y*	N	*Limitations on transaction type

(continued)

State	1 Financial ELT	2 Dealer ERT/EVR	3 Registration Renewal	4 Title and Registration	5 Driver Testing	6 Driver or ID Issuance	7 Driver Control	Notes
Nebraska	Y	Y	Y	Y	Y*	N	N	*Teen and motorcycle school training programs
Nevada	Y	N	Y	Y	N	N	N	
New Brunswick	N/A	N	N	N	N*	N	N	*Motorcycle knowledge tests at select training programs for COVID-19 backlog
Newfoundland and Labrador	N	N	N	N	N*	N	N	*Motorcycle knowledge tests at select training programs
New Hampshire	N	N	Y	Y	N	N	N	
New Jersey	N	Y	Y	Y	Y*	N	N	*Knowledge tests in high schools
New Mexico	N	Y	Y	Y	Y	Y	N	Some transactions such as REAL ID and original titles only at MVD
New York	Y	Y	Y	Y	Y	N	N	County DMV offices are agents for services; very limited auto club services
North Carolina	Y	Y	N	N	N	N	N	By phone
North Dakota	N	N*	Y	Y	Y	N	Y	*ERT/EVR planned for the coming year
Northwest Territories	N/A	N	Y	Y	N	Y	N	Contract offices provide motor vehicle services in smaller communities.
Nova Scotia	N/A	N	N	N	N	N	N	Services provided by Access Nova Scotia
Nunavut	N/A	N	Y*	Y*	N	N	N	*Local government offices
Ohio	Y	Y	Y	Y	Y	Y	Y	
Oklahoma	N	Y	Y	Y	N	N	N	Driver license is done at DPS office; title and registration services are offered at tag agents
Ontario	N/A	N	N	N	Y*	N	N	All services though Service Ontario *Driver testing at private contract test centers
Oregon	N	Y	Y*	N	Y	N	N	*Emissions inspection stations only
Pennsylvania	Y	Y	Y	Y	Y	N	N	
Prince Edward Island	N/A	N	N	N	N	N	N	All services completed by service center and highway safety; no third party
Quebec	N/A	N	N	N	N	N	N	
Rhode Island	N	N	Y	Y*	N	Y*	N	Vehicle renewals and limited registration and driver services at the auto club

(continued)

State	1 Financial ELT	2 Dealer ERT/EVR	3 Registration Renewal	4 Title and Registration	5 Driver Testing	6 Driver or ID Issuance	7 Driver Control	Notes
Saskatchewan	N/A	N	Y	Y	N	Y	*Y	*A driver ability assessment can be performed by a third-party occupational therapist
South Carolina	Y	Y	Y	N	Y	N	N	
South Dakota	Y	N	*Y	Y	Y	Y	N	*Kiosks for registration renewal
Tennessee	N	N	Y	Y	Y	Y*	N	*Duplicate and renewal driver license transactions only
Texas	Y	*Y	Y	Y	Y	N	N	*DMV-operated website, not vendor
Utah	Y	N	Y	Y	Y	N	N	
Vermont	N	Y*	N	N	N	N	N	*Limited vehicle renewal services at selected town clerks
Virginia	Y	Y	Y	Y*	N	N	N	*Limits on transaction types
Washington	Y	Y	Y	Y	N	Y	N	
West Virginia	N	Y	Y	Y	N	N	N	
Wisconsin	Y	Y	Y	Y	N	N	N	
Wyoming	N	N	N	N	N	N	N	
Yukon	N/A	N	N	N	N	N	N	

Appendix B Working Group Members

CHAIR

Steve Murphy
Director, Registries Administration and Accountability
Service Alberta

VICE CHAIR

Robert J. Smith
Administrator
Arizona Department of Transportation
Motor Vehicle Division

MEMBERS

Eric Alsvan
Manager, Online Programs
Pennsylvania Driver and Vehicle Services

Dale P. Berube
Internal Auditor
New Hampshire Division of Motor Vehicles
Administration

Brian Carlson
Deputy Director, Titles & Registration
South Carolina Department of Motor Vehicles

Michael Domke
Section Chief
Wisconsin Department of Transportation

Michael Hogan
Director, Driver Services Division
Tennessee Department of Safety & Homeland Security

Jody M. Isaak
Audit Services Director
North Dakota Department of Transportation

Doane Rohr
Bureau Chief of Motorist Services Support
Florida Department of Highway Safety & Motor Vehicles

Sky Schaefer
Deputy Administrator
Motor Vehicle Division
Montana Department of Justice

David Thompson
Investigator
Iowa Motor Vehicle Division
Bureau of Investigation & Identity Protection

AAMVA STAFF LIAISON

Casey Garber
Project Manager
Manager, Vehicle Programs

Paul Steier
Manager, Law Enforcement Programs

CONSULTANT

Barry Goleman
BerryDunn

Appendix C Third-Party Agents Stakeholder Participants

Kellie Benoit Kerstetter
General Manager – LA
NIC Inc.

Beth Caro
Secretary
Maryland Vehicle Titling Association

Dan Cinnamon
Sr. Director Government Affairs
Title Technologies, Inc.

Janice J Lucero
President & CEO
MVD Express

Rikki McBride
Association of Alberta Registry Agents

Jennifer Morris
Ginger's Auto Title Service LLC

Dan Pullium
Manager, Government Affairs
DealerTrack

Christine Rooney
Director, Compliance & Operations
Computerized Vehicle Registration

Betty L. Serian
TML Information Services, Inc.

Barry Shack
Board Member
Motor Vehicle Providers Association of Arizona

Lisa Thompas
Maryland Vehicle Titling Association

Kathryn Trimmer-Westcott
VP, Product Management and Training
Vitu

Susie Weisend
Lead Processor and Office Manager
Jan Korsten Ins., LLC
(dba Shotton Insurance Agency)

J. Ryan Williams
Missouri Association of License Offices

John Yarbrough
Director of Business Development
PDP Group, Inc.

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**