The Keys to Fighting Fraud: Deterrence, Detection, and Remediation
Facilitator:

Paul Steier,
Director, Bureau of Investigation & Identity Protection,
Iowa Department of Transportation and
Member, Vehicle Standing Committee
Presenters:

Paul Steier,
Director, Bureau of Investigation & Identity Protection, Iowa Department of Transportation and
Member, Vehicle Standing Committee

Betty Johnson,
Driver and Vehicle Records Administrator, Nebraska Department of Motor Vehicles

Steven Sebestyen,
Principal, Apex Consulting
The Keys to Fighting Fraud: Deterrence, Detection, and Remediation
The Keys to Fighting Fraud: Deterrence, Detection, and Remediation

Wednesday, August 27, 2014
General Session: 1:30 pm – 2:45 pm
The Challenge

- Google search of term, “DMV Employee Arrested” yields over 200,000 results

- Samplings reveal that fraud:
  - Is committed by employees (both new and long-term), 3rd party agents, business partners, externals as individuals or working in collusion
  - Occurs in all facets of DMV business
    - Driver
    - Vehicle
    - Testing/certification/retraining
    - Emissions/safety inspections
    - DMV-regulated business
  - Occurs across the nation, in metropolitan and rural settings, crossing jurisdiction and national borders
  - Includes improper credentialing/business licensing, theft, embezzlement, bribery, extortion, mail fraud, and other crimes
  - Is unearthed by DMV, law enforcement, media investigations
Local

DMV Employee Arrested, Accused Of License Fraud

April 10, 2014 4:55 PM

DMV employee, Tiffany Sanders, arrested for license fraud
DMV clerk pleads guilty to stealing $100K

News Tribune

POSTED: 03/20/2012 12:01:00 AM CDT
UPDATED: 03/20/2012 06:20:35 PM CDT

A former city employee pleaded guilty Monday, March 19, to stealing approximately $100,000 while working as the city’s deputy motor vehicle clerk.

Sheila Marie Jerry, 51, pleaded guilty to a single felony count of theft of public funds in County District Court. She also gave the court $112,734 in restitution. She is scheduled to be sentenced on April 30.

Jerry had been deputy motor vehicle clerk for 16 years.

According to the criminal complaint, Jerry told investigators in fall 2011 that she had stolen money for the past five years by keeping the paperwork and fees for titles on new automobiles. She stamped the title paperwork but not the original copies later sent to the state, keeping the cash from the title transfer.

The theft ended when another woman noticed discrepancies in paperwork. The woman confronted Jerry, who admitted stealing money, the complaint said. Officials searched Jerry's motor vehicle and residence, recovering 73 vehicle titles and associated fees valued at $99,671.
MV Project Manager Sentenced for Extortion and Mail Fraud

U.S. Attorney’s Office
November 19, 2013

```markdown
Mark C. LaFrance, 51, of [redacted], was sentenced by U.S. District Court Judge George A. O'Toole to three years in prison, two years of supervised release, a $12,500 fine, and forfeiture of $50,000 in illegal proceeds. In August 2013, LaFrance pleaded guilty to mail fraud and conspiracy to extort money under color of official right.
```
DMV guards, proxy test-takers arrested in driver’s license scam

Corrupt test-takers paid $2,000 to $2,500 for the easy road to getting licensed to operate school buses, big rigs and heavy equipment. Guards in on the plot allowed wannabe license-holders to leave testing rooms and have surrogate test-takers look up exam answers.

BY JOHN MARZULLI, BILL HUTCHINSON / Wednesday, September 25, 2013, 10:28 PM
DMV employee arrested for alleged theft

Posted: Dec 20, 2013 3:48 PM CST

A 23-year-old DMV Employee has been arrested after allegedly taking funds from the branch.

Shasta Gray, 23, was cited for the charge of a Public Employee Fraudulently Taking Funds.

Gray, a resident, has been placed on paid administrative leave pending completion of the State's employment investigation. Gray has been a full-time DMV employee since March of 2012.

The DMV Investigations Unit initiated a case earlier this month regarding the possible internal theft of money from the DMV branch office. At present it is believed less than $150 from cash customer transactions was involved.

If convicted, Gray faces a fine up to $1000 and, or imprisonment for up to 10 years. She is scheduled to be arraigned on February 4, 2014.
DMV OFFICIAL PLEADS GUILTY TO GIVING ILLEGALS DRIVER'S LICENSES

Three people in [redacted], including a DMV employee, pleaded guilty this week to conspiring to get state IDs or driver's licenses for at least 300 illegal immigrants.
2 Laurel DMV Employees Arrested

Posted: Jan 17, 2014 4:08 PM CST
Updated: Feb 07, 2014 4:08 PM CST

By Donesha Aldridge, Web Content Manager/Producer - bio | email

- A 12-week investigation by the Bureau of Investigation and the U.S. Homeland Security sends two Laurel driver's license examiners to jail.

48-year-old Yolanda Perkins and 55-year-old Deborah Stewart are charged with five counts of forgery each.

Both women are employees with the department of public safety.

Officials say the investigation is ongoing and additional arrests are possible.
License Examiner Arrested For Theft

POSTED 11:42 AM, MARCH 18, 2014, BY GEORGE BROWN AND SABRINA HALL, UPDATED AT 12:46PM, MARCH 18, 2014

DMV WORKER ARREST
CONSTANCE SLATER

- Reinstatement fee: $140
- Submitted: $65
- Pocketed: $75
Former DMV employee accused of taking bribe for illegal license

May 5, 2014 by Radio Network

State police have charged a former state Department of Motor Vehicles employee after investigators say she agreed to create a fraudulent driver’s license in exchange for $800.

A news release from the State Law Enforcement Division said Monday that Kelly Medina, 38, was arrested after she admitted issuing a fake license to Ariel Guerra, 36. According to warrants, Guerra is not a legal resident of.

Investigators said Guerra approached Medina in December about obtaining the license at the DMV’s main offices in . Initially, Guerra promised $1,000 for the license but agreed to $800. However, Medina told investigators she has only received $200 of that money. Guerra was charged with Influencing the Action of a Public Official.
DMV employee booked with theft, malfeasance in office
Commercial Driving School Owner/Instructor and Two Brokers Indicted for Taking Money in Turn for Giving Passing Grades to Driver’s License Applicants

U.S. Attorney’s Office
April 30, 2012

last week returned an indictment charging three defendants with mail fraud and bribery concerning programs receiving federal funds in connection with the illegal sale of documents that enabled the purchaser to obtain a driver’s license or learner’s permit, the U.S. Department of Justice
Former Kent County DMV Employee Will Be Sentenced in Bribery, Fraud Case This Spring

Posted by Michelle Mowad (Editor), January 29, 2014 at 03:54 PM

Patch file photo.

Sentencing is scheduled April 25 for a former Department of Motor
FBI makes arrests in phoney driver's license ring

February 25, 2014

Today, the Federal Bureau of Investigation [www.fbi.gov](http://www.fbi.gov), issued a statement that a DMV employee in the State of [xyz], had been indicted on charges of using illegal driver's licenses. According to the [FBI](http://www.fbi.gov), for at least three years between 2009 and 2012, using corrupt DMV employees, at the driver's exam point, multiple driver's licenses were issued for people who had either failed the driver's exam or the employee would just issue a new legal license for the right amount of money.
Former County worker to be charged with theft

June 29, 2012 By O. Kay Henderson

A state investigation shows a County clerk hired to replace an embezzler ended up stealing about $37,000 in auto fees that were to be paid to the county and the state.

“She would either collect money for issuing license plate tags or for vehicle registrations and once that was done and they’d collected money from people, she’d void them out — so the system did not show money being owed,” says Deputy State Auditor Warren Jenkins, “and she would pocket the money.”

Tammy Gammon began working in the County Treasurer’s Office in 2003. She was fired in April of last year after she admitted to the theft. The audit reviewed records from the last six years of her employment and Jenkins says 182 people in County were driving around with expired plates at some point, because they’d paid the annual fees to Gammon, but she had pocketed the money.

“If somebody got stopped by law enforcement, had their registration checked, found out it was invalid, but the law enforcement would tell them to just talk to the treasurer’s office,” Jenkins says. “...There were opportunities that it could have been caught earlier, but no one circumstance was deemed to be serious enough that they looked at a system-wide problem.”
Man Arrested For Selling Fraudulent Documents Out Of Traffic School
August 3, 2012 8:30 AM

(credit: County Sheriff's Department)

Related Tags: Arrest, DMV, Fraudulent Documents, OK Driving School, Otto Escobar, Passport, Traffic School
Local

DMV Employee Allegedly Sold Dozens Of Phony Driver’s Licenses To Illegal Migrants

November 6, 2013 3:52 PM

Tamra Burns-Sutphen, DMV employee arrested for selling driver’s licenses to dozens of illegal migrants.
Charges Three with Fraudulently Obtaining Vehicle Titles, Registrations

License and Theft Bureau inspectors on Tuesday, Aug. 28, arrested three residents for fraudulently obtaining vehicle titles and registrations.

The investigation, which has been ongoing for two months, identified people who were obtaining assumed name filings from the County Register of Deeds Office and using those fictitious business names to title and register motor vehicles, providing false information to DMV.

With the assistance of agents from the Department of Homeland Security and the Secretary of State’s office, DMV inspectors arrested the three after serving search warrants at three different locations in . Investigators estimate the group processed more than 600 transactions.
Police: Translator gave drivers the answers during their license tests

An interpreter who gave immigrants driving lessons is charged with also giving them answers to their driving test.

Mostafa Wadud Jamal, 45, of Monroe Drive in , is charged with 12 counts of tampering with public records, six counts of obstruction of justice, six counts of false swearing and six counts of making an unsworn falsification to authorities by forging or altering documents.

Jamal was an official interpreter for through the Lutheran Children and Family Services agency and spoke Hindu, Bengali and Urdu, according to court records. He also owns and operates his own driving school, Deshi Driving School in , state police said. As part of his services, Jamal sat with test-takers and translated the English language tests into Hindi, Bengali and Urdu.

State police got a tip that Jamal was providing people with answers during the driving tests and began investigating in June.

Jamal arranged to meet an undercover state trooper posing as a client in the area June 20, police said. The trooper was fluent in a foreign language and pretended not to know English. The agreement with Jamal was that the undercover trooper would bring $644.50 with him to cover cash for Jamal and fees to get the license. Jamal drove them to the New World Association of Emigrants from Eastern Europe on Bustleton Avenue in . There, they met with an employee of LCFS who collected $130 and provided Jamal with a letter stating he was a valid interpreter and was assigned to translate for the client.
Former [Redacted] License Office Employee Indicted; More Than 100 Illegal Aliens Used False ID To Obtain Licenses

FOR IMMEDIATE RELEASE

— David M. Ketchmark, Acting United States Attorney for the Western District of [Redacted], announced today that a former employee of the license fee office in St. Joseph, Mo., operated by a contractor for the [Redacted] Department of Revenue, along with a [Redacted] husband and wife, have been indicted by a federal grand jury for their roles in a conspiracy to provide false identity documents so that more than 100 illegal immigrants could fraudulently obtain driver’s and non-driver’s licenses from the license office in [Redacted].
Guilty plea in fake license scam
Former MV worker faces 15 yrs

By Lee Hammel TELEGRAM & GAZETTE STAFF
Add a comment

— A woman who worked at the state Motor Vehicles pleaded guilty Wednesday in U.S. District Court to producing false driver’s licenses.

Vanessa Peguero, 27, allegedly helped people who produced the legitimate Puerto Rican driver’s licenses of other people to obtain drivers licenses to conceal their identity, according to assistant U.S. Attorney Eugenia M. Carris. She admitted to agreeing to receive $200 per license from a man who sent people to her work station, while investigators found that two people in were charging $4,000 per license, including one traced back to Ms. Peguero, according to an affidavit filed in the case.
Ex-city employee forged paperwork for free license plates

Patrick Colleary admits breaking the law to obtain fee-exempt government license plates for more than a dozen vehicles, authorities said.

BY SARAH BURGE / STAFF WRITER
Published: April 30, 2013 7:42 p.m.

A former city employee accused of filing false paperwork to obtain fee-exempt government license plates for more than a dozen vehicles pleaded guilty to forgery Monday, April 29, in an agreement with prosecutors, court records show.

Patrick Joseph Colleary, 62, of Canyon Lake, was arrested in November after Department of Motor Vehicles officials said he submitted paperwork registering vehicles to a nonexistent agency.
mechanic charged with selling fake inspection stickers

July 24, 2013 | By Manuel Gamiz Jr., Of The Morning Call

An mechanic was charged Tuesday with putting fake inspection stickers on cars.

Simos E. Vavladellis, of 817 Main St., was charged with four counts each of fraud by altering an inspection sticker and violation of use of certificate of inspection. He was arraigned by District Judge Charles Crawford and sent to County Prison under $15,000 bail.
County woman sentenced for embezzling from DMV

Associated Press

Woman sentenced for embezzling from DMV

Media outlets report that 47-year-old Rhonda Ann Thomas of Bluefield, was sentenced Wednesday in County Circuit Court.

Judge Derek Swope sentenced Thomas to one to 10 years in prison and then suspended the entire term. Swope placed Thomas on five years' probation and ordered her to pay $13,000 in
The Tools

• Publications & Best Practices
  • Best Practices in the Deterrence and Detection of DMV Fraud
  • Facial Recognition
  • DL/ID Card Design Standards

• Fraud Detection & Remediation (FDR) Training
  – Includes current & upcoming resources
  – Administrators FIFTEEN
External Fraud Working Group
Update

Best Practices in the Detection and Deterrence of DMV Fraud

presented by:

Paul Steier
Internal / External Fraud
Best Practices

• Internal Fraud Working Group published Best Practices document in October 2010
  – terrific response from members

• External Fraud Working Group formed to finish the fraud picture
  – Final meeting held in June 2014
  – Best Practices document slated for release by December 2014
    • will combine internal and external fraud info
Best Practices Contents

• Revised / updated internal fraud information
• Internal vs. external fraud
• Why people commit fraud
  – motive, opportunity, rationalization
  – behavioral factors
  – the economy and event driven occasions
Keys to Fraud Deterrence

- Right size fraud unit
  - staff qualifications, make-up, tools, authorities, accesses
  - responsibilities can include more than fraud
- Fraud working group
- Policies / code of ethics
- Background checks
- Separate duties / job rotation
Deterrence, continued

- Hotlines
- Audit / investigate
- Social media / web
- Partnerships
  - Examples – federal, state, local
- Publicize success
Available Tools

- Card Design Standards
- CSTIMS
- CDLIS, EVVER, NDR/PDPS, SSOLV, US Pass, VLS, NMVTIS
- Digital Image Exchange
- State to State Verification
- ELT
- Courtesy Verification Program
- Document ID Databases
- Fraud Alert Site
- FDR
- NLETS, RISS, NICB
- Third Party Data Brokers
- Third Party Vehicle History Providers
Vulnerabilities Checklist

• Area of vulnerability
• Specific risk / general recommendation
• Process recommendation / solution
• IT recommendation / solution

• Can’t implement them all; pick and choose solutions that work best for your organization
Facial Recognition Working Group Update
August 27, 2014

By: Betty Johnson, Nebraska DMV, FRWG Co-Chair

(George Theobald, Georgia DDS, FRWG Chair)
Facial Recognition Working Group

FRWG Members:
George Theobald, Georgia DDS, Chair;
Betty Johnson, Nebraska DMV, Co-Chair;
Miguel Arellano-Hernandez, Kansas DOR;
Catherine Brooks, Ontario Ministry of Transportation;
Gord Bryant, Service Alberta;
Tom Flarity, New Jersey Motor Vehicle Commission;
Sydney Roberts, Illinois Office Secretary of State;
JoAnna Shanafelt, Washington Dept. of Licensing;
Ken Shock, Delaware DMV;
Steve Williams, Florida Dept. of Highway Safety & Motor Vehicles;
Sean Jowell, Pinellas County Sheriff’s Office
Facial Recognition Working Group

FRWG Technical Advisors:
Dave Coleman, IBG, Novetta Solutions;
Walter Hamilton, Identification Technology Partners;
Mike Neumann, Gemalto;
Kevin O’Leary, MorphoTrust USA;
Richard Vorder Bruegge, Federal Bureau of Investigation;
John Drago, U.S. Department of Justice

AAMVA Staff Liaisons to FRWG:
Brian Ursino, Director of Law Enforcement;
Geoff Slagle, Director of Identity Management;
Sheila Prior, Regional Director, Member Support
Facial Recognition Working Group

The purpose of the Facial Recognition Working Group is to review the methods utilized by driver license and motor vehicle agencies (MVA) to capture, review, and share facial images; and when appropriate, investigate potential matches and pursue prosecution when fraudulent activity is discovered. Or when an MVA does not have an investigative arm, establish a protocol with the applicable law enforcement agency to conduct such investigations. The Working Group will develop a best practices document related to the capture and utilization of images.

Members of the AAMVA Legal Services Discipline are developing model enabling legislation to assist jurisdictions without current Facial Recognition programs who wish to pursue legislative authority to implement. This model legislation will be included in the best practices publication.
Facial Recognition Working Group

An AAMVA **policy statement** supporting Facial Recognition was drafted by the FRWG, approved by the Law Enforcement Standing Committee; vetted during the regional conferences, and up for approval at this AIC.
Facial Recognition Working Group

PROGRESS:

First Meeting was conducted November 20 – 21, 2013; Second Meeting was conducted March 5 – 6, 2014; Third Meeting is scheduled for October 8 – 9, 2014; Publication is anticipated prior to September 2015.
Fraud Detection & Remediation
People, Processes, Technology

2014 Annual International Conference
Steven Sebestyen
What is FDR?

• Interactive computer-based training accessed by all US/CAN DMVs

• Content developed by jurisdiction experts and federal partners with oversight by FDR Maintenance Comm. (Chair, Major Paul Steier Iowa DOT)

• Includes significant material from HSI Lab & ICE DMV Outreach Program

• Updated annually

• Fully-narrated, self-paced, modularized eLearning in multiple formats

• Part of overall Fraud Strategy that includes People, Processes, Technology
What is FDR?

Originally addressed “Fraudulent Document Recognition” only

- Security Features
- Birth Certificates
- Vehicle Documents
- DLs and IDs
- Travel Documents
- Social Security Cards
- Immigration Documents
- Military IDs
- Canadian Documents
- Mexican Documents
- Counterfeits and Alterations
- High-Quality Counterfeits
- Introduction to Covert Features
What is FDR?

Has expanded to also include “Fraud Detection and Remediation”

<table>
<thead>
<tr>
<th>Introduction to Fraud</th>
<th>Internal Fraud for Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>People and Actions</td>
<td>Internal Fraud for Managers</td>
</tr>
<tr>
<td>Expanding the Review</td>
<td>Administrator’s “Fifteen”</td>
</tr>
<tr>
<td>Law Enforcement and the DMV</td>
<td>External Fraud (in progress)</td>
</tr>
<tr>
<td></td>
<td>NMVTIS Investigation Tools (ip)</td>
</tr>
<tr>
<td></td>
<td>AAMVA Fraud Tools (ip)</td>
</tr>
</tbody>
</table>
Recent Activities

Annual Update released January 1, 2014

• **NEW** Updated courseware interface

• **NEW** Mexican Passport content

• **NEW** Canadian Passport content

• **NEW** Consular and Diplomatic Credential content

• **UPDATED** indexed, searchable, and comprehensive job aid

• **Critical** Document Updates

• **2014 Update Only** Module for refresher training
Upcoming Activities

• New content research/development

• Publication of FDR Annual Report

• Meeting with FDR Maintenance Committee and Federal Partners scheduled for September 17, 2014

• Updated courseware release January 1, 2015
FDR: Your Fraud Toolbox
Welcome

For AAMVA Jurisdiction Members ONLY

Fraud Detection & Remediation Level II
Administrator's FIFTEEN

Fighting Fraud Through Engineering, Education, and Networking

This material is copyrighted by the American Association of Motor Vehicle Administrators, Inc. All rights reserved.
Welcome to FDR's Administrator's FIFTEEN. This course is part of an ongoing initiative to raise awareness of the multitude of fraud-fighting tools available to Administrators in a convenient and sharable format.

The material reflects FDR's member-driven evolution beyond Fraudulent Document Recognition to an expansive tool for global Fraud Detection and Remediation.

Unfortunately, the targets of fraudulent activities within DMV operations are not limited to the Driver License counter. As a number of jurisdictions have discovered, internal and external elements will manipulate ANY system or process that provides an opportunity for personal gain.

The Administrator's FIFTEEN will help you to assess vulnerabilities and implement prevention, detection, and remediation tools across all DMV products and areas of operation.
Introduction

Approach

As the course title suggests, we will approach the subject of fighting fraud globally by examining:

**Engineering** products, systems, and processes to reduce exposure to fraud.

**Education** about fraud issues for your staff, agency partners, or customers.

**Networking** through a host of available relationships to help efficiently target solutions to any fraud issue.

Please note: The course will not attempt to detail volumes of information. Instead, it will bring salient points to the forefront while raising awareness (by reference) of the many fraud-fighting tools available.

As emerging trends and new tools become available, FDR will release "Administrator's FIFTEEN Focus Modules" that will address specific topics so that you will be armed with the most current information available for your integrity assurance programs.
Contents

ENGINEERING
- Products
- Processes
- Procurement

EDUCATION
- Staff
- Customers
- "Users" of Your Products

NETWORKING
- Local Partnerships
- Federal Partnerships
- Vendors
- Regional, National, and International Fraud Communities

IMPORTANT NOTE: Throughout this course, you will see a number of items noted with the ☰ icon. All of these notations are presented in a single “Fraud Resource Links” attachment. You can access, save, and distribute this resource (and a number of original documents) by clicking the Attachments tab in the upper right.
Engineering products and processes that are resistant to attack is, to say the least, extremely challenging. As technology evolves to provide tools to enable better documents, products, processes, and safeguards, unfortunately, criminals quickly become more sophisticated in their approaches.

Let’s examine some of the basics surrounding an approach to Engineering.
We often think of the driver’s license (DL) when discussing a secure DMV product. While the DL is certainly the target of many sophisticated attacks, other DMV products ranging from vehicle, IRP and Dealer documents, plates, temporary tags, decals and more are also vulnerable to misuse.

The creation or improvement of these products can be engineered to better withstand attacks with a consistent use of some basic analytical tools. Of course, budgetary and other considerations will guide final decisions, but understanding risks, possible solutions, and limitations, product longevity can be better managed.

*Click the arrows in the upper right to learn more.*
Standards and Best Practices

In addition to reviewing any legislative requirements, a good practice in the beginning analysis of current (or planned) products and processes is to seek out existing standards that may exist. Reviewing established baselines can greatly diminish the need for independent research.

When published standards do not exist, reviewing best practices and lessons learned from others in the community can prove to be very valuable.

AAMVA actively manages a number of standards, best practice guides, and model legislation on a host of DMV operational issues. These are housed on the AAMVA website in convenient categories, with links included in this course's Attachments.
2 DL/ID Card Standard

When contemplating DL/ID revisions, an invaluable tool is the DL/ID Card Design Standard (CDS), developed by the AAMVA Card Design Standard committee made up of jurisdictional and federal government members. The group is guided by work done by the International Standards Organization (ISO).

The CDS provides for the design of driver licenses and identification cards, and its intent is to improve the security of the DL/ID cards and the level of interoperability among cards issued by all North American jurisdictions.
2014 DL/ID Card Design Standard

- Overseen by Committee
  - Jurisdictional members/DHS/Fellows/AAMVA
- Continuous maintenance
- Supersedes AAMVA DL/ID-2012 v1.0
- Functional requirements
- Three key concepts
  - Interoperability
  - Commonality/Uniformity
  - Security
- Compatibility with ISO 18013 standard for International Driving License
- Accommodation of REAL ID/WHTI (EDL) requirements
2014 DL/ID Card Design Standard

- Card Design
- Physical Security (inc. Security Levels & Threat Types)
- DL/ID Threat Index
- PDF - 417 Bar Code
- Test Methods
- Magnetic Stripe
- Optical Memory
- Enhanced DLs
- Compact Encoding
- Integrated Circuit
Secure Card Design Principles

- Companion to DL/ID standard
- Addresses “art & science” of design
- Understanding stakeholders
- Manufacturing
- Performance monitoring
Comparing to the Standard

How does your current or proposed DL credential compare to the CDS? There is an easy way to find out!

AAMVA offers its free Courtesy Verification Program (CVP) through an arrangement with Intellicheck Mobilisa. The CVP provides an effective way for AAMVA members to determine if their driver’s licenses, IDs, and other motor vehicle administration documents conform to the applicable AAMVA standards and specifications. Just as compliance with these standards and specifications is voluntary, participation in the CVP is also voluntary.

AAMVA strongly encourages its member jurisdictions to regularly take advantage of the CVP. A primary objective of the CVP is to improve the consistency of implementation across all jurisdictions choosing to follow the AAMVA standard and specifications.

AAMVA recommends that its members consider submitting documents on three occasions. Probably the most important of these occasions is the introduction of a new configuration or design for the document. Many problems can be avoided if they are discovered before the actual issuance of documents begins. Similarly, the jurisdiction may choose to have documents tested as part of its selection process when choosing a contractor. Finally, AAMVA strongly recommends regular, periodic retesting of documents at least annually.

The process for submitting documents is fairly simple. The necessary forms and instructions are contained in the CVP Application Form.
Product Performance Analysis

Once the information about how your product compares to existing standards is known, there are innumerable decisions to be made.

To aid in this process, the North American Security Products Organization (NASPO) and the Document Security Alliance (DSA) have crafted a comprehensive Guidance Document to help agencies assess their product security needs, evaluate available solutions, and provide cost/benefit analysis tools.

The information and decision trees can be applied to documents, security features, and a host of other DMV product offerings.

More information about NASPO and DSA is included later in this course.
Other Standards and Tools

As mentioned, standards and anti-fraud tools are available for a wide range of DMV initiatives. Vehicle (as well as many other program) products, processes and systems can benefit from a number of existing documentation sources such as:

- The License Plate Configuration Design Booklet
- Branding Best Practices
- NMVTIS
- e-Titling
Much like the product itself, the driver's license issuance process rightly garners significant attention because of its high level of exposure to fraud. The unfortunate fact remains that ALL processes within DMV operations are at risk to fraudulent activity.

Even lower-profile programs present opportunities for both internal and external parties to manipulate processes for personal gain and put the agency at risk.

Consider the opportunities for bribery, extortion, and other nefarious activities that may exist in programs dealing with products or services of value. It quickly becomes clear that functions within driver, vehicle, adjudication, IRP, tags, dealer services, emissions & safety inspection licensure all are vulnerable to attack...with some providing opportunities for surprisingly high financial and public safety risks.

*Click the arrows in the upper right to learn more.*
Engineering Processes

Fraud Best Practices

A number of AAMVA Working Groups have created outstanding guidance documents to help agencies identify and remediate process risks. One such document is the Internal Fraud Deterrence Best Practices Guide. The document and tools contained within are critical to managers as they create or improve any business process, and minimize exposure to attack.

A summary of the information contained:
- Real World Examples of Internal Fraud
- Fraud, the Economy and Event Driven Occasions
- Fraud Deterrence
- Breaking the Fraud Triangle
- Internal Controls
- Five Framework Components
- Vulnerabilities and Recommendations Checklist

Administrators are urged to review the extensive Vulnerabilities and Recommendations Checklist. The highly-detailed document provides an outstanding roadmap to evaluate ALL DMV operations (including primary, support, and administrative functions) while recognizing program-specific challenges, and providing general, procedural, and IT support recommendations.

1. Welcome
2. Introduction
3. Administrator’s FIFTEEN
4. Engineering
5. Engineering Products
6. Engineering Processes
7. Engineering Processes - Advanced Strategies
8. Engineering Procurements
9. Education
10. From FDR’s Internal Fraud for Staff - ICE
11. Education (cont.)
12. Networking
13. ICE Partnerships Fighting ID Theft
14. Networking - Other Resources
15. Conclusion
Much of the material contained within the Working Group's document is also available in the FDR e-Learning Course "Internal Fraud for Managers".

Utilizing the courseware provides managers with a comprehensive, trackable, and interactive fraud-fighting experience, detailing the use of a number of process-development and management tools, including:

- Leadership and support checklists
- Behavioral flags
- Reporting channels
- Internal controls
- Code of ethics
- Policies and procedures
- Auditing
- Investigations
- Partnerships

The next slide set is an excerpt from the course, provided so that you may assess how your management staff may benefit from the FDR module.
Successful managers continually look for new and better ways of doing business. New technologies and constantly evolving schemes - for both staff and criminals - require proactive efforts to detect and deter internal fraud.

Managers must look for gaps that would allow employees to defraud, and take steps to remedy them. Because more fraud tends to take place during recessions, increased focus during tough economic times is prudent.

Most importantly, be mindful that making single adjustments will not fix the identified problems indefinitely. Managers must continue to police processes and procedures. As operations are improved and oversight is strengthened, those who wish to defraud will continue to hone their approaches.

*Click the arrow in the upper right to learn more.*
Internal controls can be defined as mechanisms that provide reasonable assurance that basic business objectives are targeted:

- Effective and efficient operations
- Reliability of reporting
- Compliance with laws and regulations
- Safe and uniform application of policies
- Safeguarding of assets

There are three types of internal controls:

- **Preventative/Deterrent Controls** discourage irregularities. For instance, the requiring of sign-off on any exception process.
- **Detective Controls** identify irregularities after the fact. For example, checking electronic transaction logs against hardcopy documents.
- **Corrective Controls** correct irregularities and close loopholes that have been detected.

Without the perception of active fraud detection, the risk of fraudulent activity increases.
Code of Ethics

Fraud deterrence can be built directly into an organization's code of ethics. Although many codes include statements covering conflicts of interest, compliance with laws and policies, etc., a code of ethics can be written specifically to address fraud and abuse.

- The code should be clearly communicated to every employee, with each acknowledging receipt and understanding.

- Management must remain active in administering the code through training and updated postings.

- Finally, management must enforce the code by taking swift corrective action when violations are discovered.
Clear Policies and Procedures

Ethics policies should clearly detail what is considered illegal, improper, and fraudulent behavior. The best policies and procedures won't work, however, if they are not communicated or enforced.

It is critical to continually update and educate new and existing staff about the use of such policies and the penalties for defying them.

Deterring specific frauds often require specific policies and procedures. For example, deter credit card fraud by limiting employee access to customers' credit card numbers. Recent technological advances can prevent some Internet credit card fraud. For example, the address verification system (AVS) protects against random credit card generation and bogus billing addresses.

Deter procurement fraud by creating an approved vendor list that ensures you pay only vendors that pass background checks.
Engineering Processes - Advanced Strategies

4 Establish Hotlines

Because whistle-blowers expose a large percentage of frauds, hotlines encourage employees to report potential offenses that security professionals can investigate. Hotlines allow employees to report suspicious activity in an anonymous and secure reporting environment, and can range from a voice mail box accessed by management, to a fully outsourced, fully staffed, 24-hour service.

Promote the confidentiality and anonymity aspects of your fraud-prevention hotlines. Keeping employees informed about the reporting mechanisms demonstrates your intolerance for fraud and your sensitivity to privacy concerns of the reporting parties.

When instituting a hotline program, consider providing hotline access to customers, vendors, and any others with whom the agency deals. This will help ensure that suspicious activity witnessed by anyone inside or outside the agency is reported.
Background Checks

Conducting background and credit checks (to the extent allowed by your agency) on employees who may have access to credit card and other financial data is a prudent step. Credit histories can turn up financial problems, such as gambling habits, which can drive employees to crime. Workers with these types of problems might be considered for positions with no financially-related responsibilities or in positions not susceptible to bribery in exchange for agency assets.

Determining a criminal history of a potential employee can be burdensome. However, due diligence in background research can provide key insight into employment patterns, debt history, standing pressures, and other key components of the Fraud Triangle. These factors must be carefully considered when hiring or promoting into sensitive positions.
6 Separate Duties

It is critical to separate financial tasks among several employees. The person who signs checks, for example, should not make bank deposits. Budgetary cutbacks and downsizing, however, often result in the same person handling multiple procedures such as taking payment and documenting transactions.

Further compounding such an invitation to fraud is when those same employees - fearing that other employees might discover their nefarious deeds - work unusually late and on weekends. Employees who are never sick, take no time off, arrive early, and stay late may be hiding criminal activity. Requiring all employees to take vacations often uncovers fraud that "model employees" perpetrate. It is difficult to keep a fraud hidden when a mandatory holiday requires that another employee performs the vacationing worker's tasks.
Institute Job Rotations

According to the Association of Certified Fraud Examiners, job rotation and mandatory vacations resulted in the second highest reduction (61%) in losses from fraudulent activity.

Many occupational frauds require that the perpetrator actively conceal his/her scheme through false records. Required job rotation provides an opportunity for these actions to come to the attention of management and others.

It is when employees are secure in their comfort zone that temptation becomes hard to resist. It is easier to successfully commit fraud or theft when the person is always in the same job, at the same place, every day.
Audit

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

Internal audit often plays a significant monitoring role. In order to preserve its independence of judgment, internal audit should not take any direct responsibility in designing, establishing, or maintaining the controls they are evaluating. Audit staff should only advise on potential improvements to be made.

All sensitive transactions should be audited on a random basis. And do not forget to audit the auditors, supervisors, managers and others in positions of authority.

When deficiencies are identified, take immediate and appropriate action, which may include retraining, progressive discipline, or legal action. Continual vigilance to the possibilities of internal fraud, as well as external fraud, will help ensure fraud of any type is minimized.
Investigate: Take the steps necessary to resolve allegations of fraud - interviewing witnesses, assembling evidence, writing reports, and dealing with prosecutors and the courts. File criminal charges when warranted.

Blow the Whistle: Whether you choose to publicize fraud in your organization or not, make it clear that you will find and fire perpetrators. If necessary, let your employees know that criminals will be prosecuted to fullest extent of the law. Create an environment where fraud cannot thrive.

Form an Internal Fraud Working Group: The group should consist of subject matter experts who hold positions that allow them to observe and report on fraud. Some areas to be represented include audits, investigations, operations, driver services, vehicle services, information technology, and accounting. Consider including representatives from other agencies, such as state police or third-party partners as ad hoc members. The work group should meet regularly to develop new policies, procedures, and technology recommendations using a multi-disciplinary approach.

Search the Web: The World Wide Web is a resource not to be overlooked. There are numerous materials on the Internet that can help define and improve your internal controls. In addition to recommendations, you can also find studies about what particular approaches are most successful.
Obviously, the procurement process is heavily regulated by local policies. By incorporating the previous engineering concepts, however, your staff should have an excellent roadmap by which to create effective RFPs, RFIs and other procurement documents that will help ensure that the items sought will be resistant to misuse and complement your fraud prevention efforts.

A number of jurisdictions have shared their procurement documents for a variety of products and services. These can be found in AAMVA's website repository.

Whether procuring secure products themselves, or operational support items and services that could be manipulated by a criminal element, a review of these documents can provide your staff with background information that will help them author solid requirements and standards for the items to be procured.

*Click the arrows in the upper right to learn more.*
Procurement of Security Features

Selecting appropriate and effective security features for DMV products is challenging, particularly with today's technological advancements and budgetary constraints.

When developing the most effective procurements for security features, it is important to understand a particular condition within the document security community.

Lessons learned from a number of jurisdictions indicate that it is quite easy to incorrectly use the names of trademarked or proprietary technologies within procurement requirements when, in fact, a generic identifier was intended.

To illustrate, the term "crystagram" is commonly used within the DMV community to refer generically to a security feature with certain optical characteristics. A Crystagram®, however, is a specific trademarked technology.

By incorrectly using the term within a procurement document, the agency may inadvertently disallow other types of security features offering similar performance, limit responses to those entities with access to the trademarked item, or face unexpected vendor disputes.
Administrator’s Fifteen

Education

Staff

Educating staff is paramount in the fight against fraud. This education should take place on a host of topics, from the evaluation of documents and presenters, to the consequences of engaging in any type of fraud.

Staff will also benefit greatly by being aware of how to evaluate their surroundings to detect and report potential fraud, and by understanding the agency’s anti-fraud policies.

AAMVA’s Fraud Detection and Remediation Program @ brings these topics (and many more) to staff and managers of all levels and programs. Not only are essential skills in fraud detection developed, but the foundations for effective management using the Fraud Detection Model are presented in an interactive and dynamic format that bolsters retention and on-the-job application.

The next slide is taken from FDR’s Internal Fraud for Staff module which is an excellent resource for both new employees and as refresher training, outlining the perils of engaging in fraud while encouraging environmental awareness. The video showcased is provided by US Immigration and Customs Enforcement (ICE) which provides other anti-fraud resources that are detailed later in the course.
From FDR's Internal Fraud for Staff - ICE Investigations

Please allow the video a few moments to load

Video courtesy of ICE

1-886-DHS-2-ICE
Education (cont.)

Tools for Staff

One of the most noteworthy tools that has become available to AAMVA members is FREE access to Genuine Document Databases®. AAMVA has partnered with 2 vendors to provide our jurisdiction members with another valued resource that can be used in conjunction with FDR.

ID Scientific is providing our jurisdiction members free access to its Electronic Genuine Document Reference (GDR) database containing information and images of U.S. and Canadian DLs and IDs, while Keesing Technologies is providing free access to its Documentchecker database containing images of ID documents from over 200 countries.

The databases can be accessed by your staff directly from the AAMVA website using existing AAMVA credentials, or they can create credentials themselves using their agency-assigned email address.

Click the arrows in the upper right to continue.
Education (cont.)

2. Partners - Law Enforcement

Educating partners about your products and anti-fraud programs can bring great improvements to daily working relationships. The most prevalent DMV partnership is often identified as that with Law Enforcement.

The FDR Program provides a very useful tool to help educate Law Enforcement about general DMV products. Particularly helpful to roadside officers that deal with DMV documents regularly, the FDR for Law Enforcement Supplement examines how the DMV mission impacts many of the daily law enforcement experiences.

Most importantly, the Supplement provides tools for officers, such as the Foreign National Driving Credential Resource Card, that address specific issues and relay guidance as to how to obtain even further-detailed resources.
Education - Customers and Other Users

Educating users about DMV products is routinely done by a number of jurisdictions. Most commonly, these jurisdictions prepare materials that help users understand documents and the security features that can be used for authentication. This has proven to be a valuable to many agencies when appropriate levels of information are communicated.

By carefully choosing security features that perform to anti-fraud requirements, and choosing information appropriate to target audiences, issuers can preserve the integrity of the credential while arming those who rely upon the document with the information they need to spot fraudulent use. An example of such a communication is pictured here. Many issuers have found that this user-education practice also diminishes time-consuming authentication requests.

Education need not stop there. In fact, when applied to fraud-fighting, some agencies have reported that educating customers and partners simply that new fraud training and detection strategies were in place had a profound impact on the number of fraudulent activities attempted!
Unquestionably, participation within the AAMVA community provides a number of opportunities to network with peers as we all address fraud issues. Not only can Administrators benefit from communicating within these circles, but other levels of staff can engage in order to sharpen their fraud-fighting focus with information that is appropriate for their job requirements.

Committees and Working Groups, both at the Regional and International levels, are a great starting point for networking. Just a few of the groups to consider are:

- Internal & External Fraud Working Groups
- FDR Maintenance Committee
- e-Titling Working Group
- NMTIS Law Enforcement Working Group
- Card Design Standard Working Group
- eID Working Group

And when it comes to fighting fraud, there are many more networking and partnership opportunities.

*Click the arrows in the upper right to learn more.*
Law Enforcement

Most agencies do not have the resources to place law enforcement officers inside their field locations. There are however, circumstances when coordinating with enforcement entities is desired.

There are several approaches agencies can take to get this enforcement assistance. Some of the entities that agencies can look to for the formation of fraud-fighting partnerships include:

- US Federal Bureau of Investigation (FBI)
- US Dept. of Justice Office for Victims of Crime
- US Department of State
- US Secret Service
- US Postal Inspection Service
- Royal Canadian Mounted Police Anti-Counterfeiting Bureau
- Law Enforcement Fusion Centers
- Local, municipal, county, state, and provincial law enforcement agencies
Immigration and Customs Enforcement (ICE) has dedicated significant and specific resources to partner with DMVs through their Document and Benefit Fraud Task Force and the Homeland Security Investigations Forensic Lab. The agency has produced an excellent package of DMV-specific fraud-fighting materials that is available to at no cost.

By partnering with federal, state, and local counterparts, the Document and Benefit Fraud Task Force has created a series of multi-agency teams developed to target criminal organizations and beneficiaries behind fraudulent schemes.

These task forces maximize resources, eliminate the duplication of efforts and produce a strong law enforcement presence. They combine DHS's unique criminal and administrative authorities with a variety of tools from other law enforcement agencies to achieve focused, high-impact criminal prosecutions and financial seizures. The next slide showcases a video provided by ICE that focuses on their DMV partnerships to fight identity theft.
Associations and other entities

There are many associations and entities that focus on fraud. Some are attuned to the global problems created by fraud, while others concentrate on specific fraud issues or the development of standards to prevent/combat fraudulent activity.

A number of DMVs have found that being "in tune" with the work of these entities has eliminated the need for duplicative independent research, and provided timely insight into the latest fraud trends and prevention strategies. Expert opinions, case studies, and training/analytical tools can also be found within the offerings of many of these organizations.

NOTE: Links to all of the organizations mentioned next can be found in the Attachment document.

Click the arrows in the upper right to learn more.
Networking - Other Resources

1. **DSA**

The Document Security Alliance (DSA) was created by government agencies, private industry and academia. DSA's goal is to identify methods of improving security documents and related procedures to help combat the growing acts of fraud, terrorism, illegal immigration, identity theft, and other criminal acts.
NASPO

The mission of the North American Security Products Organization (NASPO) is to develop national and international fraud countermeasures and control standards, and to support those standards through education, auditing, certification and accreditation of certification bodies.

NASPO is an ANSI-accredited standards development organization based in Washington, D.C. Its members include Fortune 500 companies, commercial, industrial, government and non-governmental organizations (NGOs).
Networking - Other Resources

3 NW3C

The National White Collar Crime Center (NW3C) provides a nationwide support system for law enforcement and regulatory agencies involved in the prevention, investigation and prosecution of economic and high-tech crime.

NW3C:
- Delivers training in computer forensics, cyber and financial crime investigations and intelligence analysis
- Offers investigative support to agencies investigating white collar and related crimes
- Conducts original research on all facets of white collar crime
- Partners with the Internet Crime Complaint Center (IC3®), which allows victims of cyber crime to report incidents to law enforcement
The Federal Trade Commission (FTC) operates the Identity Theft Data Clearinghouse, which houses the federal government’s centralized repository for consumer identity theft complaints.

The FTC analyzes identity theft trends, promotes the development and efficacy of identity fraud prevention strategies, and identifies targets for referral to criminal law enforcement.

The FTC operates a call center for ID theft victims where counselors tell consumers how to protect themselves from identity theft and what to do if their identity has been stolen.
The purpose of the National Odometer and Title Fraud Enforcement Association (NOTFEA) is to deter odometer, rebuilt/salvage, and other title fraud by promoting and encouraging cooperation among law enforcement and consumer protection agencies, licensing and motor vehicle departments, the automotive industry, and individuals interested in deterring such fraud.

NOTFEA’s programs include:

- Training NOTFEA members and the public in the detection of altered and counterfeit titles
- Developing and sharing investigative information and techniques, prosecutorial documents and techniques, and other educational materials among appropriate members
- Monitoring legislation as well as industry and government policies that have an effect on such fraud
- Promoting public awareness of odometer and rebuilt/salvage fraud and its economic impact
An educational, non-profit organization, the Association of Certified Fraud Specialists (ACFS) provides low-cost learning and networking opportunities to law enforcement, attorneys, public and private sector investigators, auditors, and other risk management professionals.

The organization also administers the Certified Fraud Specialist (CFS) designation, helping members who work in the anti-fraud profession achieve leadership status, attain higher levels of recognition, authenticate skills, and transform knowledge into a meaningful career.
Many agencies have found that vendors within the DMV community offer a wide range of insight to a host of fraud topics that range far beyond security features and document production.

A number of AAMVA Associate Members offer whitepapers, opinions, and training resulting from their experiences within DMVs, non-DMV markets, and worldwide ventures.
Conclusion

This course has attempted to raise awareness of the multitude of fraud-fighting tools available to Administrators and staff, and reflects FDR's member-driven evolution to become an expansive tool for global Fraud Detection and Remediation.

As emerging trends and new tools become available, FDR will release "Administrator's FIFTEEN Focus Modules" that will address specific topics and provide the appropriate level of instruction and detail so that you will be armed with the most current information available.

Please be certain to access the content contained within the Attachments tab for links and documentation that you can share with appropriate staff.

This information will help you to assess vulnerabilities and implement prevention, detection, and remediation tools across all DMV products and areas of operation.

Close this window to exit.
Future of FDR for ALL Levels of Staff

- Focused Supplements
- Trends
- New Resources
- Optimize Delivery
Access to the FDR Toolbox & the Administrator’s FIFTEEN

AAMVA website

Use/create AAMVA credentials

Choose the implementation package

Download

Distribute
Thank You!

• FDR Training
  • Steven Sebestyen
  • ssebestyen@aamva.org
  • 262-527-9983

• DL/ID Standards
  • Geoff Slagle
  • gslagle@aamva.org
  • 703-342-7459
Summary / Q&A

15 minutes
The Keys to Fighting Fraud: Deterrence, Detection, and Remediation
Up Next:

3:15 pm – 4:45 pm

GENERAL SESSION

A Glass Act: How Google Glass Is Changing the Face of Traffic Safety

Ballroom A