AAMVA

American Association of
Motor Vehicle Administrators

Preventing, Detecting, and Investigating Cyber-Digital Fraud Whitepaper

December 2024

CYBER-DIGITAL FRAUD WORKING GROUP
LAW ENFORCEMENT STANDING COMMITTEE

Contents

Cover images: © iStockphoto.com

Executive Summary

Motor vehicle administrations (MVAs) across North America are adapting to the digital age, responding to citizen demands for convenient access to government services. This evolution toward providing more MVA services online necessitates robust identity authentication mechanisms to ensure security, reliability, and trust. This transition also brings forth significant challenges, particularly regarding the protection of personally identifiable information (PII) in the face of escalating cyber threats.

This white paper explores MVAs' evolution toward online services, the impact of fraudulent access to MVA and customer information, and the role of artificial intelligence (AI) in improving online identity authentication. Additionally, it discusses examples of AI implementation and considerations for successful deployment while addressing associated risks.

Verifying online identity poses a formidable challenge for MVAs. In the absence of physical documents, ensuring the legitimacy of user identities becomes paramount to prevent fraudulent activities. Furthermore, the omnipresent threat of data breaches underscores the importance of implementing stringent data security measures to protect citizens' PII.

This white paper explores the following general areas:

- Fraud and other criminal activity related to attacks on online MVA products and services
- Available solutions (immediate response of the MVA and technologies available)
- Enhancing online security for MVAs through AI
- Case studies from Colorado, Ohio, and Wisconsin

In the ever-evolving landscape of digital and cyber fraud, it's a common misperception among various jurisdictions that their environments are secure and unaffected by such threats.

Key Takeaways:

- Fraud is expensive! The Federal Trade Commission (FTC) estimates the public lost $10 billion in 2023.
- Cyberfraud at the MVA can be devastating to your customers but also poses a significant threat to the legitimacy of MVAs and to national security.
- There are solutions! Numerous AAMVA associate members have solutions designed to assist MVAs in combatting cyber digital fraud and customer identity verification.
- AI, when used properly, can be a valuable asset to MVAs in preventing and investigating fraud related to online transactions.

Chapter 1 Introduction

MVAs provide a valuable service for the public by issuing driver's licenses and identification cards, largely accepted as the primary form of identification in North America. These documents not only provide evidence of authorization to operate a vehicle on public roadways but are also used as a mechanism to identify an individual. These documents allow access to various services, products, and benefits, and they support efforts for homeland security protection. MVAs also manage vehicle ownership records and lien information, along with providing the means to grant permission for a vehicle to be legally operated on the roadway. These responsibilities require MVAs to obtain and maintain many important elements of an individual and organization's PII.

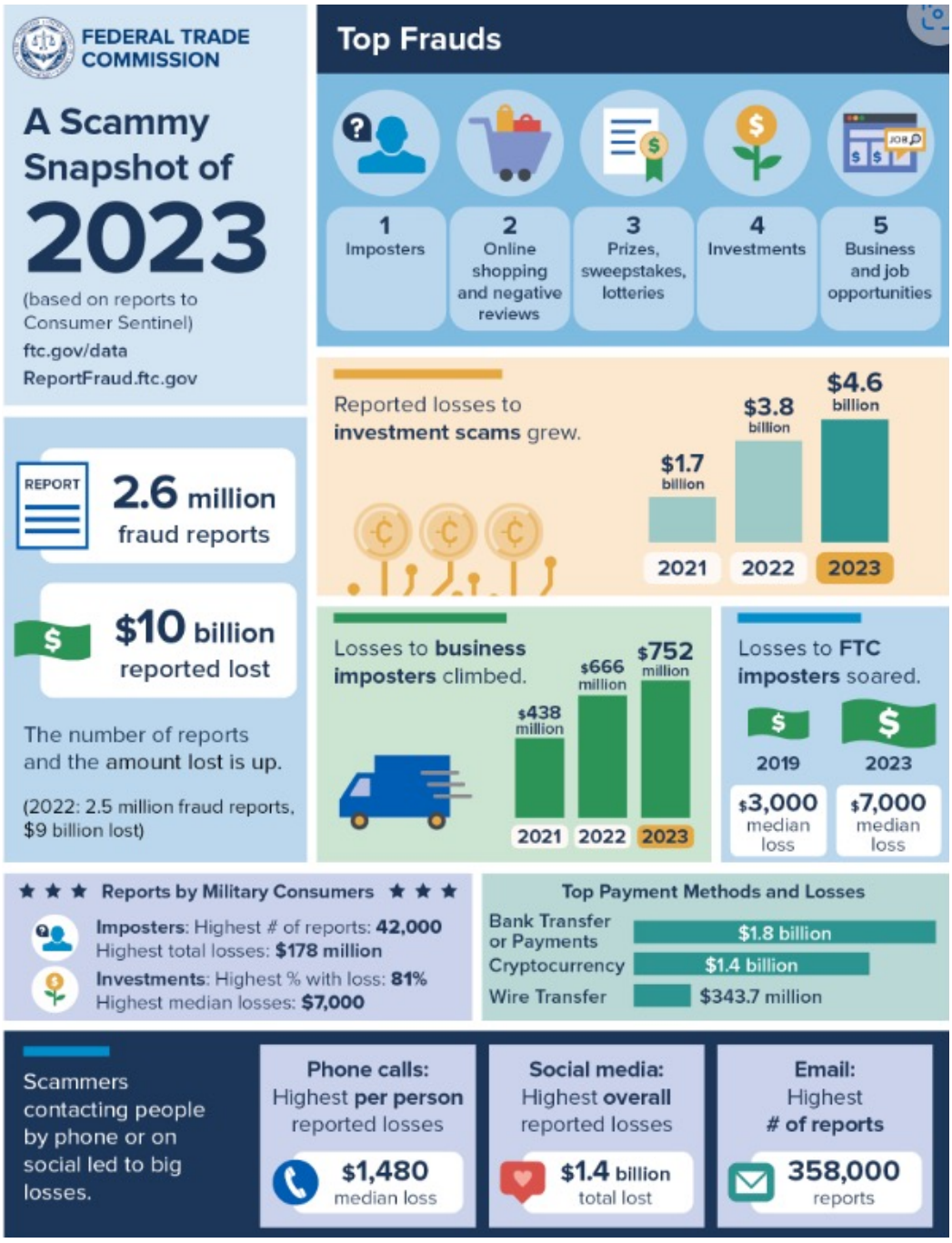
In today's increasingly digital world, the provision of online services has transitioned from a convenient option to an indispensable core function for MVAs. This evolution is driven not merely by a desire to offer additional value but also by the critical necessity to meet the diverse and expanding needs of the customer base. The physical limitations of in-person interactions, compounded by the global reach and 24/7 demands of modern consumers, underscore the imperative for robust online platforms. These platforms ensure that MVAs can provide uninterrupted, comprehensive service offerings that are accessible to all customers regardless of their geographical location or time of day. Consequently, integrating online services as a fundamental component of the operational framework is not a luxury but a strategic imperative to ensure inclusivity, scalability, and the sustained satisfaction of customer needs in a digitally connected era.

The repercussions of large-scale financial data breaches extend far beyond compromised financial information. Such breaches have unleashed a torrent of PII such as names, addresses, Social Security numbers, dates of birth, and driver's license numbers, into the hands of cybercriminals. With sensitive details now circulating in the cyber underworld, including data MVAs use to complete online transactions or establish an online account, urgent action of fortifying identity security measures is imperative to safeguard against fraudulent activities and protect the privacy of individuals whose information is now vulnerable to exploitation.

Cost of Cyber-security Protection

The cost of protecting MVA online services from fraud and cyber-attacks is a legitimate concern and one that needs to be addressed. A cost–benefit analysis will help show the value of implementing proper cyber-security measures to protect customers' data. The FTC estimates that the public lost $10 billion in fraud scams in 2023, with a total of 2.6 million fraud

The FTC estimates that the public lost $10 billion in fraud scams in 2023, with a total of 2.6 million fraud reports. This is $1 billion more than reported in 2022.



Credit: United States Federal Trade Commission

reports. This is $1 billion more than reported in 2022.[1] Potential losses to MVA customers from cyber-attacks is significant and needs to be taken seriously.

MVAs are encouraged to work with other government agencies offering online services in their jurisdiction to identify the best anti cyber-fraud solutions and products. By working together with other agencies, the costs and benefits can be spread among the agencies, which may reduce the overall costs of cyber fraud protection.

1 https://www.ftc.gov/business-guidance/blog/2024/02/facts-about-fraud-ftc-what-it-means-your-business

Chapter 2 Acronyms and Definitions

Acronyms and definitions as used in this document:

AAMVA	American Association of Motor Vehicle Administrators
Active liveness	The practice of having a person perform a specified facial movement during facial recognition.
Anti-money laundering (AML)	A set of policies and practices to ensure that financial institutions and other regulated entities prevent, detect, and report financial crime, especially money laundering activities.
Artificial intelligence (AI)	The theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision making, and translation between languages.
Automated bots	An automated software application that performs repetitive tasks over a network. It follows specific instructions to imitate human behavior but is faster and more accurate. A bot can also run independently without human intervention.
Cybersecurity	The practice of protecting systems, networks, devices, programs, and data from digital attacks, unauthorized access, and criminal use. It encompasses a range of technologies, processes, and measures designed to safeguard the confidentiality, integrity, and availability of information in the digital realm.
Facial recognition	The use of a person's image to compare with a known image of that person for identity verification. Sometimes referred to as facial verification.
Federal Trade Commission (FTC)	Federal government agency of the United States that, among other activities, provides information to assist consumers who have been the victim of identity theft.

Fraud Detection and Remediation (FDR) Training Program	AAMVA's comprehensive antifraud toolbox for anyone handling secure documents or sensitive transactions, including all agency staff.
Identity Theft Resource Center (ITRC)	Organization whose mission is to minimize risk and mitigate the impact of identity compromise and crime (ITRC).
Interception attack	A situation in which a hacker secretly intercepts and changes communication between two parties without their knowledge.
IP verification	Identity verification through analysis of an individual's Internet Protocol (IP) address compared with their history of online transactions from a unique device.
Know Your Customer (KYC)	Standards designed to protect financial institutions against fraud, corruption, money laundering, and terrorist financing.
Mobile driver's license (mDL)	A driver's license that is provisioned to a mobile device with the capability to be updated in real time. It is composed of the same data elements that are used to produce a physical driver's license; however, the data are transmitted electronically to a relying party's reader device and authenticated.
Motor vehicle agency (MVA)	An agency tasked with administering motor vehicle registration and driver licensing. These may include vehicle registration and issuing driver's licenses and ID cards, driving records, title transfers, and so on.
Multifactor authentication (MFA)	An electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism.
National Institute for Standards and Technology (NIST)	An agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness.
Passive liveness	The process of conducting facial recognition without the person doing anything other than capturing an image. The method of image capture ensures the subject is a person and not a still photograph or artificial intelligence–generated image.

Personally identifiable information (PII)	Information about a person, such as name, date of birth, Social Security number, and other information as defined by a jurisdiction.
Phishing	The fraudulent practice of sending emails or other messages purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers.
Quick-response (QR) code	A machine-readable code consisting of an array of black and white squares, typically used for storing URLs or other information for reading by the camera on a smartphone.
Romance scams	When a criminal adopts a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate or steal from the victim.
Subscriber identity module (SIM) swap attacks	An attack that occurs when the device tied to a customer's phone number is fraudulently manipulated. Fraudsters usually use SIM swapping to receive one-time security codes from banks, cryptocurrency exchanges, and other financial institutions.
Smishing	A social engineering attack that uses fake mobile text messages to trick people into downloading malware, sharing sensitive information or sending money to cybercriminals. The term "smishing" is a combination of "SMS"—or "short message service," the technology behind text messages—and "phishing."
Software as a Service (Saas)	Cloud-based method of providing software to users.
Spear phishing	A type of phishing attack that targets a specific individual, group, or organization. These personalized scams trick victims into divulging sensitive data, downloading malware, or sending money to an attacker.

Chapter 3 Fraud and Other Criminal Activity Related to Attacks on Online Motor Vehicle Administration Products and Services

How Are Online Services Attacked?

MVAs offer the convenience of online services to customers to perform a variety of transactions. These services allow for more efficient customer access and provide opportunity for less staff resources to conduct and process the transaction. Although the requirements to create and access these online services may vary, the customer is normally required to provide PII to establish an account. This PII consists of specific information about the person but may also be available to fraudsters who have obtained it through data breaches, social engineering, malware, phishing scams, hacking databases, and the dark web. These methods exploit vulnerabilities in security systems to obtain PII or trick individuals into revealing their PII.

A recent trend identified by the Identity Theft Resource Center (ITRC) is third-party vendor attacks, known as supply chain attacks. Rather than targeting a large organization with established security protections, these attacks target the information of the business customers, clients, or other vendors in a supply chain and steal information stored in their databases. Vendors who have access to MVA data could provide opportunities for fraudsters to access customers PII. Examples include bulk records purchasers, electronic court reporting, vital records, driver training schools, and third parties providing services on behalf of the MVA.

Fraudsters use this PII to appear to be the legitimate customer and may use automated bots to make multiple attempts to gain access to these online services, either through automated scripts or manual entry.

Technology allows for multiple methods fraudsters may use to commit online attacks such as synthetic content to hijack actual customer images or AI generative chat when interacting with MVA customer service representatives. MVAs need to be aware of the ever-evolving use of technology by fraudsters and implement a multilayered approach to prevent such activity.

According to the ITRC, the most common type of breaches in 2023 involved sensitive personal information.[2] The ITRC recognized that verifying data could not be trusted as the sole source of verifying a person's identity and concluded that the expanded use of facial verification and digital credentials is crucial to reducing the number of identity crimes involving the use of stolen personal information.

What Do Fraudsters Do After They Have Created or Accessed an Account?

When a fraudster accesses MVA services online, they may have the ability to change account information, including email address, mailing and residential address, telephone number, and preferred method of contact. They also have the option of changing demographic information such as height, weight, eye color, hair color, and so on. These changes are often made by the fraudster to more closely match their own demographics. In addition to changing account and demographic information, depending on the services offered by jurisdictions, they may request services such as renewal or replacement of a credential or a change of veteran or voter designation. For services requiring payment, they may provide fraudulent payment information such as a stolen or counterfeit credit card, stolen or closed bank account information,

2 https://www.hipaajournal.com/itrc-data-compromises-record-2023/#:~:text=Cyberattacks%20topped%20the%20list%20of,companies%20suggest%20that%20ransomware%20attacks

stolen or counterfeit gift cards, or compromised mobile payment technologies. Attempted use of these payment technologies or resources may result in a stopped payment, but the service may have already been provided. Free online services offered by MVAs are even more attractive for fraudsters because they do not need to secure payment information to complete the transaction. All of these activities alone or in combination may occur unbeknownst to the true account holder, only to be discovered at a later date.

The victim, however, is the most impacted. Victims may incur fines, citations, arrests, license sanctions, credit damage, loan victimization, fraudulent vehicle purchases or transfers, impersonation of professional licensing, undue stress, and lifelong challenges with clearing their identity and protecting it from future misuse.

After a fraudster gains account access to an account and changes account information, they can conduct transactions as if they are being completed by the true account holder. Unless the activity attracts the attention of the MVA, the transaction will move to completion. Fraudsters may only be looking for certain elements of data contained in the account and not the entire account information. MVAs need to be aware that any unauthorized access to account information may compromise the entire account.

Fraudsters who have the knowledge and sophistication to gain unauthorized access to MVA systems are often equipped with extensive experience and the ability to further their criminal endeavor. Criminal organizations engaged in these activities may be involved in multiple layers of fraud. These are the groups that perpetrate fraud schemes such as romance scams, business email compromises, website spoofing, investment scams, and hundreds of other schemes designed to generate fraudulent revenue. Often, these cyber fraudsters are quite savvy at operating in the virtual environment and find MVAs valuable targets for attack because of the PII and credentials maintained. The organized cyber fraud structures give these organizations a tremendous advantage at exploiting the services provided because they can simultaneously conduct a variety of attacks at numerous locations within and across jurisdictions.

Who Is Impacted by These Criminal Activities?

The fraudster's behavior upon accessing online MVA-provided accounts to obtain PII and credentials impacts the entire MVA community, other public agencies, the private sector, and the victim. Within the MVA community, there is potential for loss of public trust in the services and products MVAs provide, as well as an impact to MVA resources in researching and investigating fraudulent activities and providing victim assistance. MVAs may also endure a financial impact from stop payments and the replacement of credentials.

The private and public sectors are potentially impacted by accepting false credentials obtained by fraudsters. Fraudsters may use the fraudulent credential to sell, rent, or lease vehicles and other property; apply for loans; or be granted access to secure information and facilities. Governmental agencies that provide assistance such as unemployment, social security, welfare, and student loans are vulnerable to benefit fraud. This type of fraud negatively impacts taxpayers and reduces the funds available for the most vulnerable in our communities. The credibility of the MVA may also be negatively impacted because the public may lose faith and trust in MVA's products or services.

What is the Impact Related to the Victim's Identity?

MVAs need to be aware of the trends in fraud, have procedures in place to detect fraud, and be prepared to investigate fraud upon its discovery. This includes being aware of what customer information is

vulnerable to fraud attempts, which may include any elements of personal identification and driver's license records. These elements can be used to validate an identity, which the fraudster may find valuable later if faced with questions about the identity.

Although not all identity-related fraud is within the responsibility of the MVA to investigate, being aware of how MVA data may be compromised and the potential adverse impact on the customer is important to understand. The following are examples of how the customer could be affected if MVA driver's license and identification data are compromised.

1. A customer operating a vehicle on the public roadways may be unaware their driver's license is invalid because of fraud. This may be due to the fraudster's obtaining a replacement credential in their name and surrendering it to another jurisdiction, therefore invalidating the victim's credential.

2. A customer may be operating a vehicle with invalid driving privileges if a fraudster obtained a replacement credential and incurred driving violations in their identity. This may include serious driving violations such as operating while intoxicated, leading to arrest and court proceedings, and subsequent driving sanctions such as an ignition interlock requirement. This is perpetuated if the customer's mailing address has been changed by the fraudster so notifications from the motor vehicle agency or other government agencies are not received by the customer. A customer's license may also be invalidated if the license was obtained using a fraudulent payment method.

3. Not only are customers' driving records tampered with, but their identity may also have been compromised in many other ways, placing a burden on them to correct these records. This includes the customer's having to contact credit reporting agencies, lending institutions, insurance companies, and other government agencies where false claims for loans, medical procedures, or government benefits may have been submitted. The customer may also be impacted because of these claims in paying higher insurance premiums or having credit denied because of a poor credit rating. This activity includes fraudsters building up credit accounts in the customer's name and in one day, "busting out" these accounts, obtaining substantial loans and property liens in the customer's identity. This could lead to frauds involving personal, false business entity creation (LLCs and sole proprietorships) as well as fraudulent lines of credit being established in the victim's name without their awareness. This may be occurring without the customer being aware.

4. The victim's identity could be added into real estate transactions, utility and phone accounts, bank accounts, and government benefit programs. This may also include false tax filing in the victim's identity.

5. A customer operating a vehicle on public roadways and attempting to cross the border using an enhanced document may be unaware their enhanced driver's license and RFID is invalid because of fraud. This may be because the fraudster has obtained a replacement enhanced driver's license in their name, therefore invalidating the prior credential.

What Is the Impact Related to Motor Vehicle Records?

Vehicles that have been fraudulently titled and registered into a victim's name without their awareness can lead to many problems. An example is a traffic crash and liability claim from a crash involving a vehicle in the victim's name. The following are

examples of how a customer could be affected if MVA motor vehicle data are compromised.

1. A victim could have a vehicle transferred into their name without their knowledge. The vehicle could incur traffic violations and be used for criminal activity. The victim would then be required to prove it is not their vehicle and that they are not responsible.
2. If a victim unknowingly has a vehicle registered to their name, any registration delinquency or insurance violation on the vehicle may prevent or cancel the registration of other vehicles the customer legitimately owns.
3. If a customer unknowingly has their contact information changed in the MVA system, they may not receive vehicle renewal notices and could face a registration delinquency.
4. Vehicles titled and registered in the customer's name may end up being abandoned by the fraudsters, which can lead to citations, towing, and storage expenses.
5. Motor vehicle fraud with the use of a victim's identity can coalesce in ways such as falsified transfers of ownership, lien fraud by disposal of vehicles being held in trust, and title fraud. A victim may have a vehicle sold under their name without ever owning the vehicle or knowing such transaction took place. This in turn creates additional victimization of both the buyer of the vehicle and the person who had their identity stolen.
6. Fraudsters could gain access to MVA records and vehicle crash reports that provide PII and other valuable information.

All complaints from customers need to be investigated as soon as possible to ensure that mitigation can occur to lessen any further impact.

Chapter 4 Available Solutions (Immediate Response of the Motor Vehicle Administration and Technologies Available)

What Can the Motor Vehicle Administration Do to Help the Victim?

If fraud has been detected, then reactive measures must be taken. After the MVA has taken immediate action to stop the fraud, the MVA must work to contact all known victims via a trusted resource to help them understand what has happened, what actions they should take, and how the MVA may assist them. The notification should have information that explains what occurred and inform the customer of pertinent details of what happened.

If the MVA has implemented a mobile driver's license (mDL) program, the mDL can be used to notify the customer of any online activity that occurs in their account. This will provide an avenue for the holder of the account to be notified prior to any updates, thereby providing a proactive defense against fraud. An mDL would provide a contact avenue whereby the jurisdiction can notify the victim through the mDL app or wallet.

One example of how a victim's account can be tampered with is by changing their physical address, ordering a new credential, and mailing it to the new address. The notification should explain what the MVA has already done and what it is doing to help remedy the situation. (See Chapter 6 for an example of a victim notification letter.) When a fraudster orders a new credential, they likely used a stolen or counterfeit credit card. At some point, this will be discovered, and there will likely be a "chargeback" and outstanding charge on the victim's record. The MVA should reverse this charge to avoid a "hold" or negative balance being placed on a victim's account.

The MVA may provide victims with resources such as:

- Identity theft protection resources
- Information for placing a security freeze on their credit reports
- Information on how to obtain credit monitoring services
- Other pertinent resources and websites designed to assist victims of identity crimes.

For more information and resources for identity theft victims, see the FTC's, Identitythetft.gov.

The MVA should consider using these resources to create an identity theft brochure. Using quick-response (QR) codes can simplify access to these resources. QR codes can also be placed on notification correspondence. The victim should be encouraged to file a report with their local law enforcement agency. Law enforcement may add relevant information to the National Crime Information Center (NCIC) Identity Theft file.

These are all ways to empower victims to protect themselves from being further victimized and may assist law enforcement to locate suspect leads. Depending on the number of fraudulent transactions, the MVA may consider creating a call center to answer victims' questions. The call center staff should be able to answer common questions and pass on more complex questions to staff assigned to investigate the matter. It is recommended that MVAs each have a dedicated unit or staff to address fraud occurring related to customer access and within these organizations. For more information on best practices for creating an investigative unit, please see the AAMVA MVA Investigative Unit Resources Guide, Edition 2.

The MVA should consider what activity the fraudster was able to manipulate and how they accessed the customer's account. MVAs should evaluate whether their online portal account requirements are stringent enough. For example, some jurisdictions may require only a few security questions for online access that may include personal information that is publicly available or available through the dark web.

The MVA should also consider checking with other law enforcement agencies and other jurisdiction MVAs to see if they have seen the same types of fraud occur. Also, other government agencies within or outside the jurisdiction may have seen the same or similar methods of operation by fraudsters. Information can be gathered from them, along with lessons learned to allow for an easier and more effective course of action. Certain law enforcement agencies that are helpful in these types of investigations are the United States Postal Inspection Services; the Federal Bureau of Investigations; and U.S. Homeland Security, which investigates interstate fraud and fraud occurring through electronic means or via mail.

It is recommended the MVA collaborate with and educate local, state, and federal law enforcement agencies on challenges associated with online access to genuine MVA credentials. Prior to genuine credentials being available online, many identity theft reports had counterfeit cards or theft of information at the source, making it less likely to involve a genuine MVA credential. In today's environment, an identity theft report to local law enforcement may be a valuable lead for the MVA to investigate, especially if a genuine fraudulently ordered MVA credential was used to perpetuate the fraud. A responding law enforcement officer that is aware of the MVA's online access to genuine credentials will be more apt to contact the MVA.

An example of this occurred in Ohio, where a victim reported identity theft with local law enforcement on fraudulent retail credit cards being opened in his name. The responding officer took an identity fraud report but also collaborated with the MVA investigation team; it was quickly determined that a genuine credential was fraudulently ordered online and was being used to perpetuate the fraud. The MVA was able to react quickly and identify additional fraudulent orders of genuine MVA credentials. Had that responding officer not collaborated with MVA, there would have been a significant lapse or complete lack of identification to the fraudulently obtained credentials.

The MVA should review its victim list and records to look for similarities or clues left behind by the fraudster. This may include the use of the same bank information or indicating the same new mailing address for sending the credentials. In a recent Colorado MVA investigation of online fraud, the victims' credentials were mailed to one of approximately 25 addresses, most out of state, and primarily in New York and New Jersey. In this example, the MVA initiated a stop on all online renewals that went to out-of-state addresses. Every scenario is different, but there likely will be a pattern that can help the investigation lead to the discovery of the suspects and stopping the fraud altogether.

Another option is to audit the victim's record, looking for common or repetitive searches. Several jurisdictions have indicated this has revealed common searches or fraud rings.

Another investigative tactic is to check with other jurisdiction government agencies directly related to your list of victims who were impacted. In Colorado, for example, whenever someone changes a credential such as an address, the Colorado Secretary of State receives an update for voter registration purposes. During the Colorado investigation, the MVA checked with the Secretary of State to see if the addresses matched the MVA's list. This proved helpful because the Secretary of State corrected their records, so the victims were still able to receive correspondence from their office.

One additional area for MVAs to consider is strengthening their online access by adding review

"gates" to their systems before credentials can be mailed. For example, an MVA could stop credentials from being mailed to an address flagged as potentially fraudulent or limit the number of credentials mailed to a new address requested by multiple customers. Another example is a stop could be put in place to not allow any credentials to be mailed if the mailing address and Internet Protocol (IP) address have been flagged as potentially fraudulent. AI could be used to detect suspicious activity and place the credential renewal into a review gate before releasing it.

AAMVA Fraud Detection and Remediation (FDR) training provides educational material for any employee who interacts with customers. The ability to identify potential fraudsters during in-person, online, or telephone interaction is critical.

As jurisdictions continue to evolve operational practices to meet the changing demands of their customers, the significance of fraud detection within in-person transactions has been a cornerstone of staff training programs, ensuring the integrity and security of customer interactions. However, the digital transformation of services necessitates an equivalent emphasis on fraud detection for remote customer transactions. The same level of rigor, vigilance, and expertise that staff apply to in-person transactions must be seamlessly extended to online platforms. This approach is critical to safeguarding the trust and security of customer interactions across all channels. Therefore, enhancing training and operational protocols to include advanced fraud detection techniques for remote transactions is imperative. This ensures a uniformly secure and trustworthy service environment, reinforcing our commitment to operational excellence and customer trust in an increasingly digital world.

With the amount of PII potentially available to fraudsters, MVAs should consider establishing protocols for online account creations that incorporate two-factor authentication, biometric authentication, and credential authentication. These protocols need to also be phishing resistant and not require human interaction to assist the customer with access given the amount and variety of attacks today. This includes secure account recovery using established verification methods and monitoring and detection of fraudulent activities.

Digital transformation of services necessitates an equivalent emphasis on fraud detection for remote customer transactions.

The security, verification, and validation of PII are paramount for MVAs offering online services. Using appropriate security measures will help ensure the confidentiality, integrity, and availability of user information within their systems. MVAs should be vigilant in monitoring who has access to these online services and that the access is consistent with the need to know the information. User experience and access to the portal will always be at odds with each other because the more secure the system is, the more effort that may be required of the user to access the system. This is often referred to as "friction" between the user experience and system access. The more friction involved in the user experience, potentially the more secure the system, but the effort required by the user to access the system may increase. With proper education and information, the user may gain a better understanding and acceptance of the enhanced security, knowing their information is secure. MVAs need to be mindful of this to allow for a positive user experience balanced with a secure online process.

Common Remote Customer Verification Mechanisms

The identity verification processes includes the collection of customer information by gathering layered verifiable PII details such as name, address, date of birth, and identification numbers. Document verification includes checking documents for

authenticity, security features, and signs of alteration. Identity and document verifications include database checks by cross-referencing information against secure databases held by the relevant MVA, other available state government datasets, or trusted aggregated antifraud datasets for authentication.

Establishing trust in digital MVA interactions and protecting against identity theft and fraud is foundational in a practical sense for a much broader ability to access official data and services.

Meeting legal requirements represents a secondary consideration for MVA identity verification given the foundational use of MVA products. This includes direct privacy protection mandates, anti–money laundering (AML), and know your customer (KYC) standards in financial transactions, healthcare patient information, and service access integrity.

General online digital identity verification methods may include:

a. *Two-Factor Authentication (2FA):* Requires customers to provide two forms of identification, typically something they know (password) and something they have (a mobile device shared code required to be returned by a user)

b. *One-Time Password (OTP) Authentication:* Generates a unique code sent to the customer's mobile device or email, which they must enter to verify their identity

c. *Knowledge-Based Authentication (KBA):* Asks personal questions that only the customer should be able to answer

d. *Online Document Verification:* Uses technology to scan and validate government-issued IDs and other documents

e. *Credit Bureau-Based Authentication:* Verifies customer identity through credit history checks

f. *Age, Date of Birth, Other Known PII Verification:* Confirms the customer's age, date of birth, or other known PII to authenticate the user identity

g. *Photo Verification:* Compares a live photo of the customer with an ID document to confirm identity

h. *Biometric Verification:* Uses fingerprints, facial recognition, or other biometric data for verification purposes

i. *Database Checks:* Cross-references personal information against trusted databases for authentication or fraud flagging

j. *Optical Character Recognition (OCR):* Scans ID documents to extract and verify information such as Social Security numbers, addresses, and driver's licenses

k. *Public Key Infrastructure Signature or Key Exchange:* Uses cryptographic Public and Private key exchange or trusted cryptographic signatures for verification of identity

l. *Behavioral Biometrics:* Analyzes patterns in user behavior (e.g., typing speed, mouse movements) for continuous authentication

m. *Passkey:* Provides the ability to log in to an app or website without using a username and password combination via a pair of cryptography keys

When considering the use of these methods, the MVA must balance the need for security with a smooth customer experience or latency related to transactional volume. The goal is to leverage appropriate technology to efficiently streamline the verification process while simultaneously and effectively reducing fraud risks. This starts with technology testing and validation for efficacy within the intended use context followed by monitoring of attempted fraud and the performance impacts noted.

Keeping up with advancements in digital verification methods may be relevant to the specific efficacy of existing biometric technologies such as facial

recognition or implementation of emerging technology such as the use of retina scanning. It is important to track and adapt to changes in laws and regulations affecting identity verification. This may provoke technology changes such as mDL implementation in jurisdictions where it currently does not exist or broader use of mobile identification sufficient for use in customer data collection processes.

Even if technology integration is possible and effective, there must also be assurance that cost is reasonable and that administrative overhead can be managed by MVA organizational workflow and staffing.

Downward Trends in Reliability

It is notable that the National Institute of Standards and Technology (NIST) provides a series of standards and guidelines with technical requirements for implementing digital identity services. Addressing online fraud effectively requires focusing on the integrity of identity enrollment and verification, particularly when that identity serves as the foundation for authentication and subsequent access to services. NIST lays out guidelines for identity proofing and technical considerations when determining identity assurance levels of applicant supplied data. The following NIST documents are potentially relevant when implementing MVA identity verification programs to include verification online:

1. NIST Special Publication 800-63 Digital Identity Guidelines. https://www.nist.gov/identity-access-management/nist-special-publication-800-63-digital-identity-guidelines.
2. NIST Special Publication 800-63A. https://pages.nist.gov/800-63-3/sp800-63a.html.
3. NIST Drafts Revised Guidelines for Digital Identification in Federal. https://www.nist.gov/news-events/news/2022/12/nist-drafts-revised-guidelines-digital-identification-federal-systems.
4. Digital Identity Guidelines: Enrollment and Identity Proofing. https://www.nist.gov/publications/digital-identity-guidelines-enrollment-and-identity-proofing-requirements-including.

Additionally, the Draft Fourth Revision of NIST SP 800-63 (https://www.nist.gov/special-publication-800-63) was available for review until April 14, 2023, indicating ongoing updates to these guidelines.

Overall, the reliability of traditional authentication methods (passwords, security questions, SMS or email verification) has been trending downwards because of advancements in phishing techniques, the availability of personal information online, and technology-based attacks (e.g., SIM swapping). In response to these vulnerabilities, there is a growing emphasis on multifactor authentication (MFA), combining something the user knows (password), something the user has (a mobile device), and something the user is (biometric verification).

Deterring and Detecting Fraud in Your Jurisdiction

In the ever-evolving landscape of digital and cyber fraud, it's a common misperception among various jurisdictions that their environments are secure and unaffected by such threats. This belief, however comforting, is often a reflection of undetected fraud activities or an indication of the inevitable arrival of these threats. The digital world's interconnected nature means no entity remains insulated from the global reach of cybercriminals. These adversaries constantly refine their techniques, exploiting technological advancements and regulatory loopholes to orchestrate sophisticated attacks.

The reality is stark—cyber and digital fraud are not confined by geographic boundaries or the scale of an organization. From phishing schemes targeting individuals to advanced persistent threats against national infrastructures, the spectrum of cyber fraud is broad and indiscriminate. The illusion of safety is shattered when considering the dynamic and adaptive nature of cyber threats, which are designed to bypass conventional security measures and exploit new vulnerabilities.

The necessity for continuous vigilance and proactive preparation cannot be overstated. Jurisdictions must acknowledge the latent or looming presence of cyber threats as a call to action. It is imperative to invest in comprehensive cybersecurity strategies that encompass not only technological solutions but also education, legal frameworks, and international cooperation. These strategies should be agile, capable of evolving with the threat landscape, and inclusive of public–private partnerships to leverage collective expertise.

Encouraging a culture of cybersecurity awareness and preparedness is essential. This includes regular training for individuals and organizations, sharing best practices, and fostering open communication channels for reporting and mitigating incidents of cyber fraud. Moreover, developing and implementing robust incident response plans will ensure readiness to efficiently address and recover from breaches when they occur. The sooner an MVA is aware of a potential cyber-attack incident, the quicker it can put a stop to the attack and triage the situation.

As threats continue to evolve with increasing sophistication, the need for preparation and resilience becomes more critical. Jurisdictions must embrace a forward-thinking approach to cybersecurity, recognizing the inevitability of these challenges and the importance of being well-equipped to confront and mitigate them. In the digital age, preparation and adaptability are the cornerstones of security and trust. The following are necessary measures to consider before fraud occurs (deter), how to determine when it has happened (detect), and how to repair damage when an intrusion occurs (remediate):

Deter or Prevent

- Secure online accounts; consider not allowing guest accounts.
- Consider online account creation occurring at time of first in person service.
- Use a layered authentication approach, with a combination of password, pass code, knowledge-based authentication questions.
- Limit online services to those with limited PII exposure.

Detect

- Monitor online service activity for failed log ins, repeated data errors, and other anomalies.
- Look at user behavior analytics for time in the system.
- Identify and audit repeated use of the same financial information (credit card and ACH account number), IP address, phone number, email addresses).

Remediate

- Add locks, holds, or indicators to victims' records to prevent further fraud.
- Allow customers to freeze their online accounts when they have had a document lost or stolen or if their identity was otherwise compromised.

Communication Between Agencies and Jurisdictions

Many times, cyber-attacks occur simultaneously or in a rapid sequence to multiple agencies within a jurisdiction and to agencies in other jurisdictions. These cyber-attacks may have many similarities in the method of attack and information obtained from the attack. It is important that cyber-attack information be shared as quickly as possible with other applicable agencies to limit the amount of damage incurred, detect potential cyber-attack sources, and deter future attacks.

This communication begins before any cyber-attack occurs by MVAs establishing partnerships with a variety of resources and agencies. This can be done both informally and formally through memorandums of understanding and data sharing agreements. These partnerships should include other government agencies providing online services, law enforcement, and information technology resources. Contacts should be established to develop a protocol to share information about cyber-attack preparedness and a plan for steps that will be taken if a cyber-attack event occurs. This will ensure communication occurs in a well-structured manner to provide for the most efficient and effective planning and response. For more information about MVAs establishing and supporting partnerships, see Chapter 4 of the AAMVA MVA Investigative Unit Resources Guide, Edition 2.

Not all customers in a jurisdiction may be affected by a cyber-attack, but the MVA may consider the benefit of broad communication to their customer base. In addition to pre-established contacts and resources developed with law enforcement and other jurisdictions, MVAs may consider developing a plan for jurisdiction-wide communication. This can help create public awareness of the importance of being vigilant in protecting their personal data and avoiding falling victim to social engineering scams. The MVA should include contact information for the public if they have questions or concerns. Administrators should work with their media relations staff to develop messaging needed to be conveyed to the public.

AAMVA also has a resource for sharing fraud alerts with all AAMVA MVA and law enforcement members. This is done through the AAMVA Document Updates and Fraud Activity Alerts SharePoint site. Members can share specific details about a cyber-attack, which can be disseminated to all members participating in this notification program. For more information on this resource, contact AAMVA at info@aamva.org.

Chapter 5 Enhancing Online Security for Motor Vehicle Administrations Through Artificial Intelligence

As outlined in the previous sections, in today's digital age, MVAs face a growing challenge: balancing the convenience of online services with the critical need for robust security. Traditional authentication methods don't always keep pace with increasingly sophisticated cyber threats. This section explores how AI can empower MVAs to address this challenge. AI offers a powerful toolkit for verifying user identities accurately and efficiently, enhancing online security without sacrificing user experience. By delving into AI's capabilities, potential applications, and associated considerations, this section outlines a path for MVAs to leverage AI and navigate the evolving online security landscape. The field of AI solutions is constantly evolving; some AI solutions may not be practical for use today but may be in the future. See Chapter 6 of this document for case study examples.

Understanding Artificial Intelligence

AI refers to the simulation of human intelligence processes by machines, primarily using algorithms and data. Unlike traditional computer programs that follow predefined instructions, AI systems can learn from data, adapt to new information, and make decisions or predictions autonomously. AI encompasses various subfields, including machine learning, deep learning, natural language processing, and computer vision, each of which contributes to its capabilities.

The Role of Artificial Intelligence in Securing Online Motor Vehicle Administrations

With the rising frequency of data breaches and identity theft incidents, traditional methods of authentication, such as passwords and security questions, are proving insufficient in safeguarding sensitive information. In response to these challenges, AI has emerged as a potent ally in fortifying the security of online MVAs. Leveraging advanced algorithms and machine learning techniques, AI can augment traditional security measures and mitigate the risks associated with online identity authentication, offering a more secure and seamless experience for users.

One of AI's advantages is its ability to adapt and learn from data to identify patterns and anomalies indicative of potential security threats. By continuously learning from new data and evolving threat landscapes, AI-based systems can anticipate potential cybercriminals and emerging threats, enabling quicker responses and enhanced preparedness.

In addition, AI-driven authentication solutions can leverage advanced techniques such as biometric authentication, behavioral analysis, and anomaly detection to verify users' identities more accurately and securely. AI-based behavioral analysis can assess users' interactions with online platforms to establish a baseline of normal behaviors. Any deviations from this baseline, such as unusual login times or access attempts from unfamiliar locations, can trigger alerts for further investigation, helping MVAs detect and mitigate potential security threats in real time.

Also, AI facilitates proactive threat detection and response by continuously monitoring network traffic, system logs, and user activities for signs of malicious behavior. By automatically correlating and analyzing disparate data sources, AI can identify potential security incidents more quickly and accurately, enabling MVAs to take timely action to mitigate the impact of cyber-attacks.

AI guardrails are essential for the responsible and ethical development and deployment of AI systems, balancing the need for innovation with the imperative to protect individuals and society. The necessity and value of using guardrails for AI are significant for several reasons:

a. *Ethical Use:* Guardrails ensure that AI systems operate within ethical boundaries.

b. *Safety:* Guardrails act as safety measures to prevent AI from causing unintended harm.

c. *Trust:* Effective guardrails help maintain public trust in AI technologies.

d. *Compliance:* Guardrails help ensure that AI systems comply with existing laws and regulations.

e. *Risk Mitigation:* By setting clear boundaries, guardrails mitigate risks associated with AI.

f. *Preventing Misuse:* They are designed to prevent the misuse of AI.

g. *Transparency and Accountability:* Guardrails promote transparency and accountability in AI systems.

h. *Innovation Balance:* Ensure that new developments in AI do not outrun the ability to manage them.

i. *Social Impact:* Guardrails ensure that technology does not give way to inequalities.

Using Artificial Intelligence for Account Authentication

Using AI for account creation and authentication offers several advantages, including:

- **Enhanced Security:** AI-powered authentication can analyze multiple factors simultaneously, such as biometric data, behavioral patterns, and device attributes, to verify users' identities with greater accuracy. This MFA approach reduces the risk of unauthorized access and strengthens overall security.

AI guardrails are essential for the responsible and ethical development and deployment of AI systems, balancing the need for innovation with the imperative to protect individuals and society.

- **Improved User Experience:** AI can streamline the authentication process by minimizing the need for complex passwords and security questions. By analyzing user behaviors and preferences, AI systems can personalize authentication experiences, offering a more convenient and user-friendly approach to access control.
- **Adaptability and Scalability:** AI algorithms can adapt and evolve over time, continuously learning from new data and user interactions to improve authentication accuracy and effectiveness. This adaptability enables organizations to stay ahead of emerging threats and scale their authentication systems to accommodate growing user bases.
- **Fraud Detection and Prevention:** AI can analyze vast amounts of data in real time to detect suspicious activities and anomalies indicative of fraudulent behavior. By leveraging machine learning techniques, AI-powered authentication systems can proactively identify and mitigate fraud risks, protecting both users and organizations from financial losses and reputational damage.

Examples of Artificial Intelligence in Action

Biometric Authentication

AI-driven biometric authentication uses unique biological traits, such as fingerprints, facial features, or voice patterns, to verify an individual's identity.

Example: Facial recognition technology analyzes facial features to authenticate users' identities. This could be used to recognize users' unique facial features, allowing secure access to their devices.

Behavioral Biometrics

AI can analyze and recognize patterns in user behavior, such as typing dynamics, mouse movements, or navigation patterns, to authenticate identities based on behavioral biometrics.

Example: Typing biometrics analyzes the rhythm, speed, and keystroke patterns of users to create unique behavioral profiles to authenticate users based on their typing patterns.

Anomaly Detection

AI-powered anomaly detection techniques identify deviations from normal behavior or access patterns, signaling potential security threats or unauthorized access attempts.

Example: An AI-based anomaly detection system monitors login activities and user behavior, flagging suspicious login attempts, such as unusual login times, locations, or device usage, to detect and prevent unauthorized access.

Multifactor Authentication

AI enhances MFA by intelligently combining multiple authentication factors, such as biometrics, passwords, tokens, or geolocation data, to verify users' identities.

Example: Facial recognition can be integrated as part of a MFA approach, in which it serves as one of several authentication factors alongside passwords, PINs, or biometric identifiers like fingerprints.

Chatbots and Virtual Assistants

AI-driven chatbots and virtual assistants are deployed to provide personalized assistance to MVA customers.

Example: AI chatbots can answer common inquiries, assist with form submissions, and guide users through the application process, improving customer satisfaction and reducing the burden on MVA staff.

Data Analysis and Reporting

AI algorithms are employed to analyze large volumes of data collected by MVAs, extracting valuable insights to inform decision-making and policy formulation.

Example: AI can analyze online transaction data to identify unusual patterns, enabling MVAs to implement safeguards against fraudulent activities.

Risks Associated with Artificial Intelligence

Although AI holds tremendous potential for enhancing online security, its implementation is not without risks. Among these concerns are issues of:

- **Bias:** AI algorithms are susceptible to biases inherent in the data used for training, potentially resulting in discriminatory outcomes or unfair treatment of certain user groups. Addressing these biases requires scrutiny of training data and the implementation of bias mitigation techniques.
- **Explainability:** Complex AI models can be challenging to interpret and explain, leading to opacity in decision-making processes. To foster trust and accountability, it is imperative to prioritize the development of explainable AI solutions that enable human oversight and understanding.
- **Security Vulnerabilities:** AI systems themselves can be vulnerable to exploitation by malicious actors, posing a significant risk to user data and system integrity. Robust cybersecurity measures, including regular vulnerability assessments and

threat monitoring, are essential to safeguarding AI systems against potential attacks. In addition, MVAs may consider restricting use of AI programs to only trained and authorized users.

- **Privacy Concerns:** AI systems often require access to large amounts of data, including personal information, to function effectively. There is a risk that sensitive data collected by AI-powered systems within MVAs could be misused or compromised, leading to privacy violations or breaches of confidentiality. Unaware MVA system users and employees may pass sensitive data in the questions or prompts to the generative AI bots, which could then inadvertently become part of a publicly available information pool, usable outside the MVA systems, without intentional guardrails in place to silo generative AI systems being used by the MVA.

Recommendations

To harness the full potential of AI while mitigating associated risks, MVAs should adopt a measured and responsible approach to implementation:

- **Focus on Explainable AI:** Prioritize the adoption of transparent AI models that facilitate human understanding and oversight.
- **Address Bias:** Proactively identify and mitigate biases in AI algorithms through rigorous testing and validation processes.
- **Prioritize Security:** Implement robust cybersecurity protocols to protect AI systems and safeguard citizen data against potential breaches.
- **Comply with Privacy Laws:** Develop a data governance framework to ensure your AI implementation complies with all relevant data privacy laws throughout the AI lifecycle. In addition, conduct regular security audits to identify and address any potential privacy vulnerabilities to the AI system.
- **Maintain Human Oversight:** Ensure that AI serves as a tool to augment human expertise rather than replace it entirely, fostering collaboration and accountability.
- **Build Technology Guardrails Against AI-Powered Attack Vectors:** Add detection and protection around the use of Generative AI tools as attack vectors in the use of MVA online and other digital channels. This may start with protecting against known Generative AI sources to curb amateur threat vectors and expanding to more sophisticated detection against AI bots using AI in the network and web application defense systems.
- **Build Technology Guardrails to Set AI System Boundaries:** To prevent the AI systems from inadvertently sharing any sensitive data outside the MVA system's boundaries, apply available architectural design patterns and cloud Software as a Service (SaaS) offerings that silo the data consumption and retention boundaries.

Conclusion

The transition toward online services presents both opportunities and challenges for MVAs and necessitates a reevaluation of identity authentication practices. By leveraging AI and advanced technologies, MVAs can enhance security, streamline operations, and deliver secure and accessible services while safeguarding citizens' sensitive information. However, successful implementation requires careful consideration of associated risks and proactive measures to mitigate potential pitfalls. As MVAs continue to navigate the digital landscape, investing in robust identity authentication mechanisms will be crucial to ensuring trust, security, and efficiency in online transactions.

Chapter 6 Case Studies

Colorado

In August of 2023, the accounting department that processes credit card purchases for the Colorado Department of Motor Vehicles (DMV) noticed several hundred instances when fraudsters somehow accessed Colorado customers' online DMV accounts and made several suspicious transactions. It was discovered that fraudsters:

- Accessed customer accounts
- Changed the customer's mailing address
- Ordered a new credential or multiple credentials
- Paid for the credential with a stolen or otherwise unknown or untraceable credit card that didn't belong to the victim
- In some instances, repeated the process and ordered several new credentials

The accounting department sent email notifications immediately to the Motor Vehicle Investigations Unit (MVIU), and an investigation was initiated. Almost immediately, it was discovered that the victims were not responsible for the transactions.

Upon review of the victims' accounts, it was noticed that almost all the victims had Asian surnames. The MVIU had seen a much smaller incident like this occur in Colorado a few months earlier, but in that incident, there were only 12 victims. However, the pattern was the same—fraudsters had ordered a new credential after changing the mailing address to an out-of-state address and paid for it with a stolen credit card.

Other commonalities were noted among the fraudulent transactions in this incident. The fraudsters had changed the addresses to approximately 12 addresses, many in New York or New Jersey. Many of the New York addresses were in the cities of Flushing and Bayside, along with cities in New Jersey or in Philadelphia, PA.

Research showed other states throughout the country had experienced similar instances of this same fraud, including Texas, New York, Florida, Georgia, and Maine. MVIU investigators made contact and began sharing information and leads, and they discovered many new addresses that credentials were mailed to fraudulently. Also contacted was the United States Postal Inspector Service (USPIS), who was helpful in attempting to intercept fraudulently mailed credentials. USPIS inspectors were able to intercept credentials mailed to some of the heavily used fraudulent addresses.

At the time, the Colorado DMV allowed access to its online services by its customers if they had the four following pieces of information:

1. Name
2. Date of birth
3. The last four numbers of the Social Security number
4. Customer Identification Number, also known as a driver's license number

Unfortunately, with the numerous data breaches around the world, most of these pieces of information were available to fraudsters on the dark web. As days passed, the number of victims continued to grow.

The Colorado DMV made decisions to contact each victim of the identity theft and online fraud activity and to help them recover. A letter was sent to all victims notifying them of the incident and offering to help them with the situation by:

- Providing instructions on how to get a free credential with a new driver's license number
- Reversing any charges that might be on their account (caused by the fraudulent credit card usage, which created an amount owed or a negative balance on their account)
- Voiding the fraudulent credential
- Placing a "fraud note" in their file, identifying them as an identity theft victim (which also stopped online activity)
- Waiving the normal requirement that asks for an affidavit of lost or stolen credential and a requirement for a police report
- Providing resources about identity theft, links to common helpful websites about identity theft, freezing or protecting your credit, credit monitoring, and other resources
- Setting up a special website for victims to access answers the most common questions about this incident

The Colorado DMV also set up a "Fraud Call Center" and trained call takers to be able to answer the most common questions asked. These Fraud Center call takers were empowered to forward calls to MVIU investigators if there were questions they couldn't answer or if they received information that might be helpful to the investigation. The letters had information about what the DMV had already done and had "next steps" for the victims.

As the Colorado DMV was working to help the victims, other groups were working on strengthening the online access process. Because it was recognized that almost all the fraudulent address changes were sending the new credentials to out-of-state addresses, the ability to order credentials *online* was stopped. The DMV would still take care of customers who needed to order credentials and have them mailed out of state, such as college students or military personnel stationed out of Colorado. But the ability to conduct online ordering of out-of-state credentials was discontinued. This was completed within a few days of the fraud's discovery. The MVIU then started to look into three Colorado addresses that credentials were being mailed to. These addresses were monitored by both the MVIU and the USPIS, which was asked to intercept credentials being mailed to these addresses.

The Colorado DMV also was able to strengthen its online access by adding a fifth question or requirement by asking for the issuance date of the most recent credential. It was thought that the fraudsters did not have a credential in their possession, and this information would most likely only be known by someone who possessed the credential when making an online transaction. This was something learned by the state of Texas, which had added a fifth question and had success. If a customer didn't know their issue date of the most recent credential, they were advised that an online transaction could not take place, and they needed to contact the fraud call center during business hours.

The DMV also began to set up a process in which they asked their vendor to set up a "review gate" that stops certain requests before a credential is made and mailed out. Certain known fraud addresses (or known out-of-state fraud cities) were added to this "review gate" process. It was also decided to have certain situations pass through a review gate, such as:

- More than three credentials ordered from the same address within 30 days
- More than three credentials ordered from the same IP address
- Known fraudulent credit cards used previously

The Colorado DMV also partnered with other state agencies. The DMV worked with the Secretary of State to compare lists of victims to ensure that none of the fraud affected their status as a voter. In Colorado, when someone receives a credential or changes their address, the new address is provided to the Secretary of State for voting purposes. Lists were compared to ensure that identity theft victims did not have their addresses changed against their wishes to avoid the appearance of voter fraud.

Colorado was able to stop this fraudulent activity but believes that fraudsters will come up with new ways to attempt similar fraud schemes. Colorado has started a procurement process to further strengthen the system.

Here is a summary of a victim notification letter that the Colorado DMV recently sent:

1. The Colorado DMV has opened an investigation into the described fraudulent activity.
2. The Colorado DMV has canceled and voided the newly ordered (fraudulent) credential and created a "block" to the motor vehicle record that will prevent any *additional* online activity from occurring.
3. The Colorado DMV has added a note to your record that indicates a police report has been opened (example, case number 23-1234) that identifies you as a victim of this crime.
4. The Colorado DMV has established a website for victims to obtain answers to additional questions, receive updates, and other information about the investigation. This website will be updated as new information becomes available.

In addition, Colorado provided the following "next steps" for the victims:

1. If the driver's license or identification card number is compromised, the Colorado DMV strongly encouraged the victim to get a new driver's license or identification card with a new number to provide a level of protection if a fraudster attempts to use the current credential.
2. To obtain a new driver's license or identification card, bring this notification to your local MVA office. You are encouraged to make an appointment before visiting the office. (Information may be omitted if the MVA does not offer appointments.) You will be issued a free replacement credential.
3. If you discover that someone has used your identity or credential to commit a crime such as opening a credit card or bank account in your name, please contact law enforcement to file a police report. Please mention this notification and case number.

Wisconsin

Wisconsin was presented with three different solutions to reduce improper access of our customer records using online applications. The most important criteria were ease of use and customer impact, effectiveness, and cost. Wisconsin does approximately 300,000 online transactions a year, and there was concern for that number dipping. A decision was made to only use the solution when information or products were being shared: a driver's own record, a duplicate driver's license or identification, and online renewal of a driver's license or identification. Other applications were reviewed, and PII was removed where possible.

Proposed Solutions

- A document verification and account-based solution: Customers would provide a photo of themselves as well as photos of identity documents to create a profile. It was decided this was too large a burden on customers, and many of these documents have already been presented to Wisconsin DMV to obtain their original products, creating a sense of redundancy.
- A user and information- or history-based solution: Patterns in the customer's device

use would be compared with the current sign in and would escalate to knowledge-based questions when needed. Wisconsin decided against this because of the availability of so much information on the web and dark web. This did not seem user friendly and could potentially create a feeling of "big brother" if the DMV application is asking non-DMV types of questions.

- A facial recognition–based solution: This solution was chosen because of the cost, the low impact on customers (not having to provide new documentation), and the security that comes from comparing against an already existing record.

Cost and Implementation

Billing is based on a per-use cost structure. Implementation has been completed in approximately four months by a team compromising the vendor, DMV information technology resources, and program representatives.

Security and Customer Considerations

One of the most secure and difficult to replicate identity features is the human face, and the Wisconsin DMV wanted to take advantage of the fact that this piece of information was already available. The facial recognition–based solution compares the person using the application with the photo that exists in the database. The solution can be used via laptop or smartphone and will coach the user through the process. The selfie is then run through a one-to-one verification while also checking for liveness.

Another part of this choice was for management to acknowledge that this may reduce the use of our applications. Although a decrease in online applications has been noticed, it has not been felt in the offices or call centers. More information is still needed to understand the impact.

Ohio

Ohio has an "OHID" account that is offered at the statewide level and is labeled as "Ohio's Digital Identity Standard." After being established, the OHID can be used in several different state programs; among these state programs is the Ohio Bureau of Motor Vehicles (BMV). An OHID is required to submit an online order for a reprinted or renewed Ohio driver's license or identification card. The Ohio BMV service provider is a statewide vendor.

The Ohio BMV Service Provider

The Ohio BMV Service provider has thousands of customers across several different industry types, including government and financial institutions.

The Ohio BMV Service Provider is multifaceted and aims to use every element of identity within its data analysis. The Ohio BMV provider's website contains a complete portfolio overview; however, the focus of this case study highlights the components mainly used by this business unit (the Ohio BMV Investigations Section).

- **Address Risk:** The Ohio BMV service provider provides an assessment of risk associated with the customer's address. The Ohio BMV service provider aims to assess whether the address itself is associated with fraud and the correlation that exists between the identity and the presented address.
- **Email Risk:** Much like the address risk assessment, the Ohio BMV service provider aims to weigh the risk with the provided email address. The email feature aims to assess how likely the email is associated with fraud, assess the correlation between the email address, and the user and assess whether the email address is fake.
- **Phone Risk:** The Ohio BMV service provider assesses a phone risk similar to the fundamentals of the address and email risk assessment.

Similar to the address and email assessment, the provider aims to assess the likelihood of the phone number's being associated with fraud, the assessment of whether the phone number is fictitious or a nonfixed VOIP (Voice over Internet Protocol) number, and assess the correlation between the phone number and the input identity.

- **Overall Assessment:** In addition to the address, email, and phone assessment, the Ohio BMV service provider provides an analysis of many different facets of the consumer's identity and the correlation that exists with that identity. This assessment includes but is not limited to name, email, phone, address, date of birth, Social Security number, IP address, and device used.
- **Advanced Authentication:** The Ohio BMV service provider also offers some advanced-level authentication processes in which an applicant needs to provide proof of a document (take picture of front and back of credential) and pass a liveness test to proceed with an assessment. The Ohio service provider posts a high rate of accuracy in the detection methods and overall assessment of the uploaded documents.
- **Decision Point:** The Ohio BMV service provider enables the client to tweak policies and risk scores in minutes to adapt on the fly to adjust thresholds to ensure the system is appropriating applications to the desired decision point.

Ohio BMV Application

The Ohio BMV Investigations Section uses the data and assessment supplied from the Ohio BMV service to help formulate decisions based around online activity in connection with Ohio BMV online services. The Ohio BMV service provider supplies a dashboard for users to review the assessments of various data points. In the example of an online application for an Ohio driver's license, the online account can be reviewed to see risk and assessments connected to the input data points of the following as well as how they correlate to the identity and other elements:

- Address
- Email
- Phone
- Geolocation

The Ohio BMV Investigation uses the solution's provided data to make assessments of BMV-specific applications and identify anomalies and fraud that need further analysis.

Appendix Cyber-Digital Fraud Working Group Roster

JURISDICTION MEMBERS

Owen McShane, Chair
Deputy Commissioner, Investigations and Law Enforcement
New York State DMV

Negash Assefa
Director of IT
Maryland Motor Vehicle Administration

Todd Ballinger
Administrator
Ohio BMV Investigations Section

Karen Brooks
Investigator 3
Georgia Department of Driver Services

Dana Chavez
Chief Investigator
Colorado DOR

Adam Guess
Compliance, Audit and Fraud Unit Supervisor
Wisconsin DMV

Beau Hurley
CISO & Agency Risk Manager
Virginia DMV

Chris Leeman
Investigator
Iowa DOT

Michael Ross
Detective
Maine Bureau of Motor Vehicles

Joanna Shanafelt
Assistant Administrator
Washington State DOL

TECHNICAL ADVISORS

Jim Emerson
Vice President
National White Collar Crime Center (NW3C)

Steve Hunter
Special Agent, Senior Liaison Officer
Homeland Security Investigations

Dr. C. Ariel Pinto
Professor, Department of Cybersecurity
University of Albany

Steve Sebestyen
Principal, Apex Consulting
AAMVA FDR Program Manager

AAMVA STAFF

Tom Foster, Project Manager
AAMVA Law Enforcement Program Manager

Patrice Aasmo
AAMVA Director, Member Services Regions 1 & 2

PY Boyer
AAMVA CISO and Senior Director of Enterprise Architecture

Patrick Fernan
AAMVA Vice President, Driver Programs and Services

Julie Knittle
AAMVA Director, Member Services Regions 3 & 4

Mike McCaskill
AAMVA Vice President, Identity Management Programs and Services

Paul Steier
AAMVA Director, Vehicle Programs

Brian Ursino
AAMVA Vice President, Law Enforcement Programs and Services

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**