December 26, 2012 **# 12-13**

LAW ENFORCEMENT BULLETIN

FACIAL RECOGNITION SOFTWARE

The Department of Motor Vehicles has just begun utilizing Facial Recognition (FR) software in our driver license database to identify situations of fraud and/or identity theft. The FR program views an image of a person and compares it to one that is in the database. It does this by comparing structure, shape and proportions of the face; distance between the eyes, nose, mouth and jaw; upper outlines of the eye sockets; the sides of the mouth; location of the nose and eyes; and the area surrounding the check bones.

There may be situations in which FR may be of assistance to you during a criminal investigation. If you feel this tool may be of use to you; please contact staff in the DMV Enforcement and Safety Division at 828-2067.

Thank you.

Glendon W. Button
Director of Enforcement and Safety

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION

AND

THE VERMONT DEPARTMENT OF MOTOR VEHICLES

CONCERNING THE SEARCH OF PROBE PHOTOS AGAINST THE VERMONT DEPARTMENT OF MOTOR VEHICLES PHOTO REPOSITORY

I. PURPOSE

The purpose of this Memorandum of Understanding (MOU) is to document the agreed responsibilities and functions of the Parties with respect to conducting searches of the Vermont Department of Motor Vehicles (DMV) facial recognition (FR) photo repository, which contains license (DL) photos. These searches will be performed for the purpose of comparing FBI Facial Analysis, Comparison, and Evaluation (FACE) Services Unit probe photos against photos housed in the Vermont DMV's FR photo repository and obtaining information that will advance active FBI investigations, apprehend wanted fugitives or known or suspected terrorists, and locate missing persons nationwide. A probe photo refers to the photo of the subject of an active FBI investigation that is submitted for search against a photo repository. The anticipated result of that search will be a photo gallery of potential matches (candidates). These potential matches will be forwarded to the FBI, along with any associated information stored with the photo in the Vermont DMV FR system. The FBI FACE Services Unit will then perform comparisons of the candidate photo(s) against the probe photo(s) to determine their value as investigative leads.

II. PARTIES

A. The FBI, Criminal Justice Information Services (CJIS) Division, Biometric Services Section (BSS), FACE Services Unit provides investigative support to FBI field offices and headquarters divisions. The CJIS Division, through its Assistant Director, is the FBI's point of contact (POC) for this MOU. For certain day-to-day operations of the activities described by this MOU, the FBI's POC with the Vermont DMV will be the FACE Services Unit's Management and its Management and Program Analysts.

B. The Vermont DMV provides a variety of public safety services such as law enforcement, communications, criminal identification, regulatory licensing, criminal and arson investigation, forensic analysis, training, safety education

and emergency management. For the purposes of this MOU, the Vermont DMV POC is the DMV FR Program Manager, Michael Charter. For certain day-to-day operations of the activities described by this MOU, the FACE Services Unit will contact the Vermont DMV POC Director of Enforcement, Glen Button.

III. AUTHORITIES

A. The FBI enters into this MOU pursuant to Title 28, United States Code (U.S.C.) Sections 533 and 534; Title 28, Code of Federal Regulations Section 0.85; Title 42, U.S.C. Section 3771; and Title 18, U.S.C. Chapter 123.

B. The State of Vermont is authorized to share DL information with the FBI for authorized law enforcement purposes pursuant to Title 18, U.S.C. Section 2721 (b)(1).

C. The Vermont DMV enters into this MOU pursuant to Title 23, Vermont Statutes Annotated, Chapter 3, § 104 (d).

IV. BACKGROUND INFORMATION

A. The FACE Services Unit provides a facial recognition service in which FBI Special Agents, or other authorized FBI personnel, submit to the FBI CJIS Division a photo of the subject of an active FBI investigation. These probe photos are compared to photographs in databases authorized for use by the FBI (i.e., FR databases maintained by state motor vehicle departments/agencies, law enforcement, or other government agencies). In this case, a probe photo is sent to the Vermont DMV. The Vermont DMV compares the probe photo to its database, and candidates produced as a result of the search are sent by the Vermont DMV to the FACE Services Unit. The FACE Services Unit compares Vermont DMV candidate photos against the submitted probe in an effort to narrow down to the one or two most-likely candidates. These candidates are then provided to the requesting FBI contributor for use as an investigative lead. The number of candidates produced and provided to the FACE Services Unit as a result of these searches is dependent upon the searching threshold set by the individual agency.

B. The intent of this service is not to provide a positive identification, but to provide the FBI Special Agent with an investigative lead and analysis to support that lead. The FBI will utilize the Vermont DMV FR photo repository to supplement information provided by existing FBI database searches.

V. SPECIFIC RESPONSIBILITIES

A. The FBI will:

1. Submit probe photos, via Law Enforcement Online (LEO)-to-LEO e-mail, to the Vermont DMV for the purposes of comparing the probe photos with photos in the Vermont DMV FR photo repository. The LEO is accredited and approved by the FBI for Sensitive-but-Unclassified law enforcement information.

2. Manually analyze, compare, and evaluate the returned candidate photo gallery against the probe photo to determine the most-likely candidate.

3. If necessary, request additional biographical information associated with each photo determined to be a most-likely candidate via a secure email communication.

4. Submit the photo(s) of the most-likely candidate(s) to be searched against the FBI's Next Generation Identification Interstate Photo System in order to:

    a. Locate any additional photos and associated information relating to the "most likely" candidate(s).

    b. Identify additional potential candidates and associated information.

    The results of this search will be compared and analyzed against the original probe photo(s). Once the analysis is complete, the one or two most-likely candidate photos, along with their associated information, will be provided to the requesting FBI Special Agent as an investigative lead.

5. Store photo images and text associated with the DL of the most-likely candidate(s) to the probe in the FBI case management system for record keeping purposes.

6. Immediately destroy all other gallery photos and associated information.

B. The Vermont DMV will:

1. Apply for a LEO e-mail account through the LEO Operations Unit.

2. Compare the FACE Services Unit-submitted probe photo against the Vermont DMV FR photo repository.

3. Return electronic photos of all possible candidates to the FACE Services Unit via LEO e-mail.

4. Upon request, return additional biographical information associated with each photo determined to be a most-likely candidate.

5. Ensure that only authorized Vermont DMV personnel will handle requests submitted by the FBI CJIS Division. Authorized Vermont DMV personnel refers to the personnel who are currently trained to perform FR queries against the Vermont DMV FR photo repository for law enforcement purposes. Names of these predetermined Vermont DMV personnel will be submitted to the FBI CJIS Division for the purpose of the FACE Services Unit establishing and maintaining communications contact with those Vermont DMV personnel who will be providing services to the FACE Services Unit.

6. Destroy all probe photo images, and any associated data submitted from the FACE Services Unit, once the search has been completed and the response has been sent to the FACE Services Unit via LEO.

7. Ensure that photos received from the FACE Services Unit will not be electronically transmitted by any internal or external Vermont DMV systems except as necessary to effectuate this agreement.

8. Prohibit the sharing and/or dissemination of any information associated with FBI FACE Services Unit's requests beyond the authorized Vermont DMV personnel unless required by Vermont state law. If sharing or dissemination is required, the Vermont DMV will notify FBI FACE Services Unit as soon as possible and before the release of the information.

VI. PRIVACY AND SECURITY

A. The information involved in this MOU may identify U.S. persons, whose information is protected by the Privacy Act of 1974. The FBI will ensure that all such information will be handled lawfully pursuant to the provisions

thereof. Conversely, the Vermont DMV will comply with its own state's privacy laws.

B. For purposes of this MOU, Personally Identifiable Information (PII) is defined as information which can be used to distinguish or trace an individual's identity, including any personal information which is linked or linkable to a specific individual. Examples of PII are name, social security number, date of birth, place of birth, citizenship, mother's maiden name, and photographs, fingerprints, and other biometrics.

C. Each party that discloses PII is responsible for making reasonable efforts to ensure that the information disclosed is accurate, complete, timely, and relevant.

D. Each party will immediately report to the other party each instance in which information received from the other party is used, disclosed, or accessed in an unauthorized manner (including any information losses or breaches).

E. All transmissions of probes submitted by the FACE Services Unit to the Vermont DMV and responses returned to the FACE Services Unit will be made through a LEO-to-LEO e-mail connection.

F. The Vermont DMV will ensure user accounts and authorities granted to its personnel are maintained in a current and secure "need-to-know" status.

G. Both FBI requests and Vermont DMV responses will contain PII, and LEO e-mail is approved and authorized to ensure security of information contained in these transmissions.

H. All hardcopy facial images determined by the FACE Services Unit not to be a most-likely candidate, along with all associated textual information, will be disposed via confidential trash. All electronic facial images, including those saved on thumb drives, determined by the FACE Services Unit not to be a most-likely candidate, along with all associated textual information, will be deleted.

I. Photo images of the most-likely candidate will be retained by the FACE Services Unit in the FBI's case management system. All others will be destroyed by the FACE Services Unit.

J. The information and/or documents provided by Vermont DMV to the FACE Services Unit will contain PII about persons retained in the Vermont DMV FR system. The FACE Services Unit will use this information for lawful/authorized purposes only.

K. Each party shall be responsible for the safeguarding of any equipment used by it to access records and shall limit access to authorized users with a need to know the information and who have been properly instructed as to their duties and responsibilities under this MOU.

L. Each party shall implement procedures to ensure that such equipment is located in a secure area and to prevent information, including any printed copies of records, from being viewed by individuals not authorized to use the equipment and from being viewed by individuals not authorized to see or have access to this information.

VII. EFFECT OF THIS AGREEMENT

A. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable by law or otherwise against any of the parties, their parent agencies, the U.S., or the officers, employees, agents, or other associated personnel thereof. The parties will seek to resolve any disputes regarding this MOU by mutual consultation.

B. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of the understanding between the parties of the matters described herein. Unless otherwise agreed in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the language in this MOU in no way implies that funds will be made available for such expenditures.

C. This MOU does not constitute an agreement for any party to assume or waive any liability or claim under any applicable law.

D. Each party is responsible for ensuring that information it discloses was not knowingly obtained or maintained in violation of any law or policy applicable to the disclosing party, and that information is only made available to the receiving party as may be permitted by laws, regulations, policies, or procedures applicable to the disclosing party.

E. Each party will provide appropriate training regarding the responsibilities under this MOU to individuals whose information-sharing activities are covered by the provisions of this MOU.

VIII. EFFECTIVE DATE, MODIFICATION, AND TERMINATION

A. This agreement shall be effective when executed by all of the parties and will continue in effect until terminated. This agreement may be modified at any time by written consent of all parties.

B. This MOU may be terminated, with respect to any party, at any time upon written notice of withdrawal to all other parties. Any party desiring to withdraw from this MOU will endeavor to provide such written notification to all parties at least thirty (30) days prior to withdrawal. This MOU will be reviewed annually to ensure that the terms remain current, complete, and relevant.

C. This MOU, in eight distinct sections, is the exclusive statement of the parties with respect to its subject matter and supersedes any and all prior agreement, negotiations, representations, and/or proposals, written or verbal, relating to its subject matter.

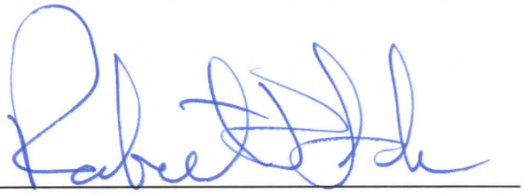
FOR THE FEDERAL BUREAU OF INVESTIGATION

4/30/13

David Cuthbertson
Assistant Director
Criminal Justice Information
Services Division

Date

FOR THE VERMONT DEPARTMENT OF MOTOR VEHICLES



5/8/13

Robert D. Ide
Commissioner
Vermont Department of Motor Vehicles

Date

Grant Progress Report

Progress Report # Final

Reporting Period: 01/01/2013 to 06/30/2013

Submittal Date 10/28/2013

Grant Agreement No: 2009-ID-MX-0024

Project Name: FY 2009 Driver's License Security Grant Program

Grantee: Vermont Department of Motor Vehicles

I certify under penalty of law that this document and any attachment was prepared by me or under my direction in accordance with the terms and conditions of each Grant Agreement Exhibit. Based on my inquiry of the persons or persons who manage the project or those directly responsible for gathering the information, the information submitted is, to the best of my knowledge and belief, true, accurate, and complete. All information submitted in this document and all attachments conform to and is in accordance with the state and federal laws and I so here certify with my signature. I am aware that there are significant penalties for submitting false or misleading information.

Project Director: Michael Charter (Printed Name) _____ (Signature)

Summary of Work Completed in Reporting Period

1. Completed the installation and implementation of Facial Recognition.

Progress Report Narrative

Introduction

Primary work in this reporting period was related to Facial Recognition. We also worked on improvements to card design to meet newest available AAMVA standards and on upgrades to our license process to improve our ability to monitor and audit individual license transactions.

Summary of Activities

1. With the death of VTDrives (a failed modernization project) Vermont DMV elected to focus on benchmark 6; 37.13(a), *Make reasonable efforts to ensure that the applicant does not have more than one DL or ID already issued by that State under a different identity*. Vermont DMV Enforcement had long wanted a tool like Facial Recognition Software (FR) and we realized this would also help satisfy this benchmark in particular. Vermont DMV completed installation of Facial Recognition (FR).

   The DMV Enforcement unit completed a full scrub of all existing records. The scrub has already led to a number of investigations and uncovered a number of data entry errors. The cleansing of records continues to this date; initially only records within the state statute of limitations are being investigated along with all newly enrolled customers. As time allows all older records are being reviewed.

   Our FRS provides both one-to-one (1:1) and one-to-many (1:N) comparisons of applicant images. Using large, side-by-side images, 1:1 comparisons are performed as part of the enrollment process and may also be performed later, during investigations, allowing the comparison of the recently captured image of the applicant against a previously stored image of that applicant. Automatic 1:N batch comparisons of each day's applicants enable comparison all applicant images captured on a

given day against millions of stored images to quickly identify attempts at multiple identity fraud before IDs are issued.

Facial Recognition Software			
Installation/Setup	$900,000.00	1	$900,000.00
	TOTAL		**$900,000.00**
FY 2008 Real ID Demonstration Grant Program			**$150,880.97**
FY 2009 Driver's License Security Grant Program			**$661,690.00**
Total State Funds (installation & Setup)		**$87,429.03**	
Total Grant Funds (installation & Setup)			**$812,570.97**
Annual ongoing cost ($0.511 per card produced)			**$88,000.00**

Material Compliance Checklist (as submitted with compliance package)

#	Section	Does The State:	Yes/No	Comments
1	§ 37.11(a)	Subject each applicant to a mandatory facial image capture and retain such image even if a driver license (DL) or identification card (ID) is not issued.	Yes	All customers obtaining a license or ID are subject to a mandatory image. All images are stored and all images are processed through Facial Recognition. Current policies and procedures for license and ID applicants have the photographs being taken as the final step in the process.
2	§ 37.11(b)	Have each applicant sign a declaration under penalty of perjury that the information presented is true and correct, and retain this declaration pursuant to § 37.31.	Yes	Vermont has long required all applicants to sign a declaration under penalty of perjury that the information presented is true and correct. All applications are imaged and stored indefinitely.
3	§ 37.11(c)(1)	Require an individual to present at least one of the source documents listed in subsections (i) through (x) when establishing identity	Yes	Vermont will require applicants applying for a REAL ID compliant license to submit the documentation required by §37.11 (c)(1) to establish their identity.

#	Section	Does The State:	Yes/No	Comments
4	§ 37.11(d)-(g)	Require documentation of: • Date of birth • Social Security Number • Address of principal residence • Evidence of lawful status	Yes	Vermont required documentation of DOB, SSN, proof of address and evidence of lawful status long before the beginning of the Real ID process
5	§ 37.11(h)	Have a documented exceptions process that meets the requirements established in 37.11(h)(1)-(3) (if States choose to have such a process)	Yes	Vermont has created an exceptions process to meet the requirements established in 37.11(h)(1)-(3)
6	§ 37.13(a)	Make reasonable efforts to ensure that the applicant does not have more than one DL or ID already issued by that State under a different identity	Yes	Vermont has procedures in place to prevent issuance of multiple ID's to include the use of facial recognition technology.
7	§ 37.13(b)(1)	Verify lawful status through SAVE or another method approved by DHS	Yes	Vermont utilizes SAVE
8	§ 37.13(b)(2)	Verify Social Security account numbers with the Social Security Administration or another method approved by DHS	Yes	Vermont utilizes PDPS/SSOLV
9	§ 37.15(b)	Issue DL and IDs that contain Level 1, 2 and 3 integrated security features	Yes	Current Vermont EDL and OTC contain Level 1, 2 and 3 integrated security features. Additionally the OTC is scheduled for a refresh in the second quarter of 2013 which will further enhance the card.

#	Section	Does The State:	Yes/No	Comments
10	§ 37.17(a)-(l)	Surface (front and back) of cards include the following printed information in Latin alpha-numeric characters: • Full legal name • Date of birth • Gender • Unique DL/ID number • Full facial digital photograph • Address of principal residence [with exceptions] • Signature [with exceptions] • Date of transaction • Expiration date • State or territory of issuance	Yes	
11	§ 37.17 (n)	Commit to mark materially compliant DL and IDs with a DHS-approved security marking	Yes	Vermont is prepared to add the DHS-approved security marking as soon as approval from DHS has been received. We have already made necessary changes to our card design and worked with our license vendor to add the marking.
12	§ 37.21	Issue temporary or limited-term licenses to all individuals with temporary lawful status and tie license validity to the end of lawful status	Yes	Vermont has been doing this for years

#	Section	Does The State:	Yes/No	Comments
13	§ 37.41	Have a documented security plan for DMV operations in accordance with the requirements set forth in § 37.41	Yes	Documented security plan is currently in development. The Department of Buildings and General Services, Security Division, provides access control, intrusion, and CCTV solutions for all State Agencies in all state buildings. All DMV offices have controlled access using proximity cards. Access within buildings is further restricted using either access cards or combination locks on doors. Draft security plan has been submitted as part of this package and will be re-submitted once finalized.
14	§ 37.41(b)(2)	Have protections in place to ensure the security of personally identifiable information	Yes	
15	§ 37.41(b)(5)(i)-(ii)	Require all employees handling source documents or issuing DLs or IDs to attend and complete the AAMVA approved (or equivalent) fraudulent document recognition training and security awareness training	Yes	
16	§ 37.45	Conduct name-based and fingerprint-based criminal history and employment eligibility checks on all employees in covered positions or an alternative procedure approved by DHS	Yes	The state of Vermont will meet the requirements of §37.45. We have added the requirement as a prerequisite to all new hires of the Department. We are in discussions with our Department of Human Resources - Labor Relations Division to begin impact bargaining with the Vermont State Employees Association (the Union) for existing Department employees.
17	§ 37.51 (b)(1)	Commit to be in material compliance with Subparts A through D no later than January 1, 2010 or within 90 days of submission of this document, whichever date is earlier		

#	Section	Does The State:	Yes/No	Comments
18	§ 37.71 (b)(1)	Clearly state on the face of non-compliant DLs or IDs that the card is not acceptable for official purposes, except for licenses renewed or reissued under § 37.27	Yes	

Smith, Michael

From:	Charter, Michael
Sent:	Wednesday, June 26, 2013 4:11 PM
To:	Bloom, Drew; Codling, Kathy
Cc:	Broe, Jennifer; Mullins, Jeri; Smith, Michael; Button, Glen; Charter, Michael
Subject:	Facial Recognition
Attachments:	FR Process 06_2013.pdf; FR FAQ.pdf; FR MOU.pdf

I have several documents I would like you to take a look at please.

FR Process – a procedure of how we use FR. In part we need this should there be any further press inquiries. Please let me know what needs correcting or modifying. I have a couple of items marked in red that I'm not certain about.

FR FAQ – intended for publication on website. As above, let me know what needs correcting or modifying.

FR MOU – I created this heavily leveraging the MOU between us and the FBI. This was not requested however it occurred to me that perhaps we should require police departments to have a signed MOU on file before they can submit images to us. The MOU dictates how images can be used and could cover us should any overzealous officer step out of bounds. If agreed, it will obvious need vetting from Mr McCormick.

Michael

Michael Charter | DMV Project Specialist | Vermont Department of Motor Vehicles
120 State St | Montpelier VT 05603 | 802.828.0496

The Vermont Department of Motor Vehicles (DMV) Enforcement and Safety Division is comprised of a contingent of sworn law enforcement officers and non-sworn civilian staff. The Division has three sections, the Commercial Vehicle Enforcement Section, the Investigative Section and the Administrative Support Section. Below is an overview of the function of each of the respective sections.

The DMV Investigative Section uses Facial Recognition (FR) software to identify possible duplicate identities. The FR software creates "Leads" on a nightly basis. FR leads are triggered by a single image appearing in more than one DMV issued credential file. DMV Investigative staff review the leads generated by the FR software by visual review and analysis of any associated DMV (historical license) records. All leads are scanned for particular facts that would indicate one of two actions.

- **"No Action"** - The file will have a correction performed, by direction of the Chief Inspector, which will correct the problem and cross-reference the files to a valid credential.

- **"Refer for Investigation"** - The file will indicate possible fraudulent activity. Chief Inspector will assign to an investigator for further action. Any individual revoked will have an opportunity to request a formal DMV hearing to contest the action.

"No Action"

Many of the leads will be the result of duplicate credential records. Most of these are records where fraud has not occurred and there is an error due to:

- The individual had a Non-Driver ID (NDR) and then obtained a Driver's License (DL) and the DMV staff did not utilize the Personal Identification (PID) number from the NDR when the new credential was issued.

- There was a change of name that did not get recorded on the old credential and a new credential was issued with a different number at a later date.

- The first and last names were transposed when the data was entered on the first credential; this was not corrected and resulted in a new credential with a different number being issued at a later date.

- There was an error in the data entry for the date of birth; this can cause a new credential to be issued as the data will indicate this a different individual.

- DMV issued a new credential number due to fraud and cancelled or revoked the old credential without any cross reference or comment.

- There may be other fact patterns; this procedure lists some of the more common possibilities.

Review of the files consists of an examination and comparison of the credentials in the fields containing;

- Name
- Date of Birth
- Social Security Number
- Address history
- Signature

- Image
- Expiration date of credential
- Review of the DMV historical file for credential modifications that were processed by DMV
- Check of the suspension files
- Any other relevant data

If a determination is made that there was no fraud in the reviewed files the following procedure should be followed.

1. The record can be corrected by cancellation of the questionable credential and a cross reference made to the appropriate valid credential.

2. The paperwork will be brought to the Chief of Information & Processing for assignment and correction.

    a. Staff will cancel and cross reference the no longer valid credential and will place a note on the valid credential regarding the cancelled file for reference. A printout of both modifications should be attached to the record. The case file may now be closed.

"Refer for Investigation"

If a file has an image in it and that same image also appears in other files utilizing different demographics, those files are submitted for document and image review by the Chief Inspector. These are cases where it appears an individual has obtained different credentials for the purpose of fraud. During review of these cases there are common indicators in the demographics that indicate likely fraud. They are;

- The names are usually completely different
- There are multiple SSNs, many of them may verify with the SSOLV
- Multiple dates of birth, generally within a two or three year time frame
- Different street addresses, but usually located around a specific town or area
- Multiple non-matching images in the same credential file indicate a "group sharing"' of a fraudulent credential
- Signature has misspelled name or non-matching name
- Some credentials may continue to be renewed and kept current but most are a "one- shot" and only used for one cycle

Once defined as fraudulent the credential is revoked, the file is marked on the comment sheet the associated files are all noted on the report, the appropriate boxes checked and the associated files are placed together and forwarded to who?.

There are circumstances which will create variations of these procedures. There may be an image in a legitimate file; this could be a case where an individual obtained a credential using someone else's DL record. Care must be exercised in these situations to not revoke the credential of an innocent victim. The credential must

be named in the report but not revoked. If the credential is fraudulent and expired no further action is taken. If the fraudulent credential is current the innocent victim should be contacted and offered to obtain a new credential with a new number assigned to it. In any transfer of information and assignment of a new number the driver history file must also reference the old and new numbers and the associated history.

There are situations where an individual has initiated a fraudulent file by providing false demographics and then a different individual has appeared and that image is now in the file. This file is to be revoked and the new non matching image processed through the FR system to determine if there is any additional fraud using the same image.

Where an individual indicates they have information or documentation that would clarify or correct a record, an informal conference is scheduled. Action may or may not be taken based on the documentation presented at this conference. If the issue can be clarified any suspension issued may be rescinded. At times only a specific credential may be withdrawn from the action (if documents support) and the rest of the file may continue to be investigated.

In the event the respondent can show a set of circumstances that explain the identified duplicate credential in the absence of any fraud on their part DMV may close the case. In this situation narratives of the facts that substantiate the reversal must be documented. This narrative must include the name, DOB, credential number and type of credential.

Fraud Type	Characteristics	Method	Prevention & Detection	
Establish a single Identity	Only 1 identity & credential	Fraudulent breeder documents	Fraudulent document recognition	• Documents examined or proofed by trained staff at issuing locations • Documents examined or proofed by specialist at central location (requires original documents)
Establish Multiple Identities	Multiple new credentials	Fraudulent breeder documents	Fraudulent document recognition	• Documents examined or proofed by trained staff at issuing locations • Documents examined or proofed by specialist at central location (requires original documents)
			Detect Previous Identities	FR 1:Many comparison
Identity Theft	Imposter in valid credential file	Impersonates a valid customer and obtains a duplicate credential	Recognize imposter is not who they claim to be	FR 1:1 Recognized by DMV employee
			Detect Previous Identities	FR 1:Many comparison
Employee selling credentials	Credential produced at DMV		Internal Controls	Transaction Audits Physical Controls and accounting of materials FR 1:Many
Employee selling credential materials	Credential produced by counterfeiter		Internal Controls	Physical Controls and accounting of materials

Department of Motor Vehicles
Agency of Transportation

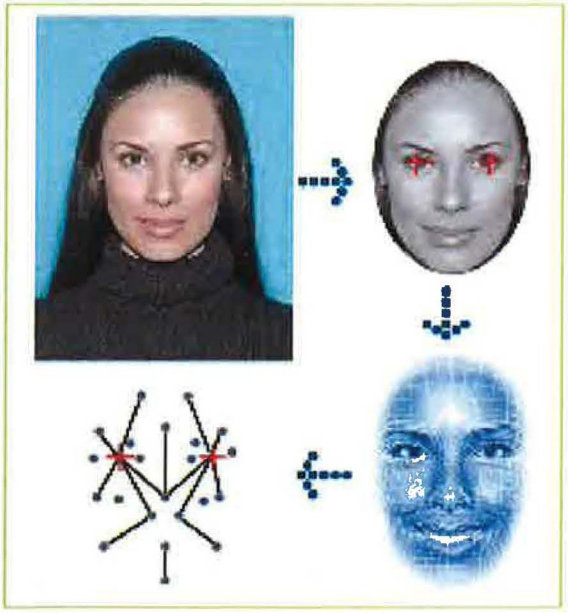
Vermont Department of Motor Vehicles
120 State Street
Montpelier, Vermont 05603-0001
802.828.2000
dmv.vermont.gov

DMV uses facial recognition to protect your identity

The Vermont Department of Motor Vehicles (DMV) uses facial recognition as part of our ongoing effort to prevent individuals from obtaining multiple licenses or ID cards or attempting to obtain a Driver's License or Non-Driver ID in the name of another Vermont resident. Vermont DMV is committed to doing everything it can to combat identity theft and protect the identities of Vermont residents.

How does the facial recognition system work?

Using your regular driver license or ID card photo, the system creates a digital template using a precise map of facial features that are not easy to alter, such as eye sockets, cheekbones and sides of the mouth.



The system compares the template it creates to all the templates currently in our database and determines if someone is applying for a license using a name other than their own. When mismatches are detected, the system flags them for review by specially-trained DMV staff.

DMV's facial recognition system is designed to be an accurate, non-obtrusive fraud detection tool. When staff investigators confirm an individual may have more than one identity in our system, DMV offers the individual an opportunity to explain at a hearing before any administrative action to suspend or cancel a license or ID card is taken.

Facial recognition templates are not shared

DMV does not release facial recognition system results. If DMV investigators find probable fraud or identity theft, we will inform appropriate partner agencies who can investigate for identity-based crime or entitlement fraud.

Frequently Asked Questions (FAQs)

Q: What is facial recognition?

A: Facial recognition is an exciting and effective technology that motor vehicle agencies across the country have been using for over a decade to:

- protect the privacy and integrity of customer accounts
- make the experience of getting a driver license faster and more efficient
- enhance public safety

Facial recognition technology makes it much more difficult for individuals to commit identity fraud by preventing them from obtaining driver licenses under assumed identities and prevent them from establishing multiple identities which can then be used for illegal purposes.

Q: How does it work?

A: Recent advances in facial recognition technology have made the process of reliably verifying the identities of individuals highly accurate and fast. Like fingerprinting, facial recognition is a form of identification that allows a computer to quickly establish your identity based on physical features that are unique to you. But unlike fingerprinting, it does not require you to ink your fingertips or use fingerprinting machines. It simply uses the photograph of you that will be printed on your license.

It works like this: When you come to DMV to apply for or renew your license, you pose for the photograph that will appear on your license, the resulting image is analyzed by sophisticated facial recognition software. The software takes precise measurements of features that do not typically change as you age and are unrelated to gender or race, such as the distance between your pupils. These measurements are combined in a "template" that is unique to you, and that template is linked to other basic demographic information that helps establish your identity, such as your name and your Driver's License number.

If someone who has information about you attempts to impersonate you and obtain a License or ID in your name, facial recognition software will compare their photograph to the one that is already in your record to ensure there is an exact match. While a person may do their best to attempt to look like you, such as growing a mustache or cutting or coloring their hair, they cannot change the distance between their eyes or the height of their cheeks, etc. and the system will alert DMV Investigators of a potential mismatch. DMV staff then review a number of different factors; such as determining if there is a clerical error or if there is a significant fraud attempt. Ultimately, our goal is to ensure your identity is protected.

The software will also look for matches with other templates to ensure that a person's photograph is not already associated with another Driver's License under a different name. This is to ensure that each person with a Driver's License only has one, so that they don't use one for legal purposes and additional licenses for illegal purposes. If potential matches turn up the software produces a file, which is then carefully reviewed by a highly-trained member of our staff. In any instance where identity fraud is suspected, the file is immediately provided to trained investigators for follow-up.

Q: I see pictures on TV and on the Internet of faces with grids on them. What does my facial recognition template look like?

A: Hollywood depicts facial recognition in ways that increase its dramatic effect for entertainment purposes. In real life, facial recognition uses math to calculate measurements of your facial features and then stores calculations of those numbers in a database. DMV employees do not see a grid on your face, nor do they see the calculations. In fact, the software doesn't even look at your photographs for comparisons. Only the software knows how to take your template and compare it to other templates. It's not a function that humans can perform.

Q: Why are you using facial recognition?

A: Identity fraud costs individuals and organizations billions of dollars each year, and victims can consume months or even years undoing the damage and re-establishing a trusted identity.

Protecting the integrity of every Driver's License is essential to minimizing identity fraud, because it is the trusted ID used most often by Americans to establish their identity and gain access to the essential benefits and services that enhance their lives – whether making a major purchase, opening a bank account, taking a plane, seeking credit or applying for retirement benefits like Medicare or Social Security. Secure Driver's Licenses benefit everyone who engages in trusted transactions, and our goal is to issue them in a manner that establishes the highest level of confidence and security using proven procedures that are fast, unobtrusive and convenient.

Facial recognition technology has been adopted by the majority of state motor vehicle agencies nationwide because it works. It is the fastest, most accurate, most cost-effective technology for deterring individuals from attempting to get driver licenses or ID cards under multiple names or stolen identities, and for detecting fraud when it occurs. It also helps us identify duplicate records and data discrepancies so that we can ensure the information in your driver record is always up to date and entirely accurate.

Because of the unprecedented speed and precision of facial recognition technology and its ability to automate verification processes, we can take the staff that used to work behind the scenes on manual processes and move them to positions where they can focus on delivering excellent customer service to you and other customers.

Q: Does the use of facial recognition technology mean it will take longer to get my driver license?

A: No. The system uses your photograph that is already part of the process. In fact, in many cases, it will actually speed up the process and improve the accuracy of identity verification. This is because it replaces manual processes that used to be done by our staff with automated processes that happen much faster than a person could ever perform them.

Q: Who has access to facial recognition data specific to my driver license record?

A: In accordance with our mission to provide customers with the safest and most secure access to our services, we carefully protect all the data associated with your Driver's License record, including your facial image and its facial recognition template. As an agency of the State, access to data in our systems is strictly controlled and regulated. It is stored in highly secure servers in our data centers, and is managed using the most advanced government-level security practices. Access to images is strictly limited to authorized entities. Protecting the integrity of your data and your identity is our highest priority. Authorized Law Enforcement agencies may submit images of suspects in crimes for analysis by DMV Investigators.

Vermont Department of Motor Vehicles Facial Recognition Access Memorandum of Understanding

This Memorandum of Understanding (MOU) is entered into between Vermont DMV, (hereinafter referred to as DMV), an agency of the State of Vermont, and the *LE Agency name here*, (hereinafter referred to as LE User), and dated *June 26, 2013*.

PURPOSE: The purpose of this Memorandum of Understanding (MOU) is to document the agreed responsibilities and functions of the Parties with respect to conducting searches of the Vermont (VT) Department of Motor Vehicles (DMV) facial recognition (FR) photo repository, which contains license (DL) photos. These searches will be performed for the purpose of comparing suspect probe photos against photos housed in the VT DMV's FR photo repository and obtaining information that will advance active investigations, apprehend wanted fugitives or known or suspected terrorists, and locate missing persons. A probe photo refers to the photo of the subject of an active investigation that is submitted for search against a photo repository. The anticipated result of that search will be a photo gallery of potential matches. These potential matches (candidates) will be forwarded to the LE User, along with any associated information stored with the photo in the VT DMV FR system. The LE User will then perform comparisons of the candidate photo(s) against the probe photo(s) to determine their value as investigative leads.

PARTIES:

- The VT DMV provides a variety of services such as law enforcement, driver licensing, document forensic analysis, training and safety education. For the purposes of this MOU, the VT DMV Point of Contact (POC) is the DMV FR Program Manager, Michael Charter. For certain day-to-day operations of the activities described by this MOU, the LE Users will contact the VT DMV POC Director of Enforcement, Glen Button.

- The *LE Agency name here* provides a variety of public safety services such as law enforcement, communications, criminal identification, criminal and arson investigation, forensic analysis, training, safety education and emergency management. For certain day-to-day operations of the activities described by this MOU, the *LE Agency name here* POC with the VT DMV will be *contact name here*.

BACKGROUND: The Vermont DMV hosts Vermont's Facial Recognition System (FR). FR provides facial search capabilities, subject information, and face image comparison tools, to authorized Vermont law enforcement agencies.

- Authorized Law Enforcement personnel may have a subject photo as part of an active investigation. These probe photos may be compared to photographs in the VT DMV database. The probe photo is sent to the VT DMV. The VT DMV compares the probe photo to its database. Candidates produced as a result of the search are sent to the LE User. The LE User compares VT DMV candidate list against the submitted probe in an effort to narrow down to the one or two most likely candidates. The list of candidates may then be used as an investigative lead. The number of candidates produced and provided to the LE User as a result of these searches is dependent upon many factors.

- The intent of this service is not to provide a positive identification, but to provide the LE User with an investigative lead and analysis to support that lead. The LE User will utilize the VT DMV FR photo repository to supplement information provided by existing investigative practices.

SPECIFIC RESPONSIBILITIES:

The VT DMV will:

- Compare the LE User submitted probe photo against the VT DMV FR photo repository.

- Return electronic photos of all possible candidates to the LE User via e-mail.

- Upon request, return additional biographical information associated with each photo determined to be a most likely candidate.

- Ensure that only authorized VT DMV personnel will handle requests submitted by the LE User. Authorized VT DMV personnel refer to personnel who are currently trained to perform FR queries against the VT DMV FR photo repository for law enforcement purposes.

- Destroy all probe photo images, and any associated data submitted from the LE User, once the search has been completed and the response has been sent to the LE User.

- Ensure that photos received from the LE User will not be electronically transmitted by any internal or external VT DMV systems except as necessary to effectuate this agreement.

- Prohibit the sharing and/or dissemination of any information associated with LE Users requests beyond the authorized VT DMV personnel, unless required by Vermont state law. If sharing or dissemination is required, the VT DMV will notify LE User as soon as possible and before the release of the information.

LE Agency name here:

- Submit probe photos, via official departmental Law Enforcement e-mail or by traceable courier (FedEx, UPS, etc.) to the VT DMV for the purposes of comparing the probe photos with photos in the VT DMV FR photo repository.

- Manually analyze, compare, and evaluate the returned candidate photo gallery against the probe photo to determine the most likely candidate.

- If necessary, request additional biographical information associated with each photo determined to be a most likely candidate via a secure email communication.

- Securely store photo images and text associated with the DL of the most likely candidate(s) to the probe in an official case management system for record keeping purposes.

- Immediately destroy all other gallery photos and associated information.

PRIVACY AND SECURITY

- The information involved in the MOU may identify U.S. persons, whose information is protected by the Privacy Act of 1974. Both parties will ensure that all such information will be handled lawfully pursuant to the provisions thereof.

- For purposes of this MOU, Personally Identifiable Information (PII) is defined as information which can be used to distinguish or trace an individual's identity, including any personal information which is linked or linkable to a specific individual. Examples of PII are name, social security number, date of birth, place of birth, citizenship, mother's maiden name, photographs and fingerprints.

- Each party that discloses PII is responsible for making reasonable efforts to ensure that the information disclosed is accurate, complete, timely, and relevant.

- Each party will immediately report to the other party each instance in which information received from the other party is used, disclosed, or accessed in an unauthorized manner (including any information losses or breaches).

- All hardcopy facial images, along with all associated textual information, will be disposed via confidential trash. All electronic facial images, including those saved on thumb drives, determined not to be a most likely candidate, along with all associated textual information, will be deleted.

- Photo images of the most likely candidate will be retained in a case management system. All others will be securely destroyed.

- The information and/or documents provided by VT DMV will contain PII about persons retained in the VT DMV FR system. ***LE Agency name here*** will use this information for lawful/authorized purposes only.

- Each party shall be responsible for the safeguarding of any equipment used by it to access records and shall limit access to authorized users with a need to know the information and who have been properly instructed as to their duties and responsibilities under this MOU.

- Each party shall implement procedures to ensure that such equipment is located in a secure area and to prevent information, including any printed copies of records, from being viewed by individuals not authorized to use the equipment and from being viewed by individuals not authorized to see or have access to this information.

EFFECT OF THIS AGREEMENT:

- Each party is responsible for ensuring that information it discloses was not knowingly obtained or maintained in violation of any law or policy applicable to the disclosing party, and that information is only made available to the receiving party as may be permitted by laws, regulations, policies, or procedures applicable to the disclosing party.

- Each party will provide appropriate training regarding the responsibilities under this MOU to individuals whose information-sharing activities are covered by the provisions of this MOU.

TERMINATION: This MOU may be terminated by either party without cause, upon no less than thirty (30) calendar days written notice. VT DMV reserves the right to terminate service, without notice, upon presentation of reasonable and credible evidence that the User is violating this MOU.

TERM OF AGREEMENT: This MOU will become effective upon signature of both parties and will remain in force until it is determined by VT DMV that a new agreement is required. The LE User should initiate the execution of a new agreement when a change of agency head occurs.

IN WITNESS HEREOF, the parties hereto have caused this MOU to be executed by the proper officers and officials.

LE Agency name here

AGENCY HEAD

_____ TITLE _____
(PLEASE PRINT)

_____ DATE _____
(SIGNATURE)

Vermont Department of Motor Vehicles

AGENCY HEAD

_____ TITLE _____
(PLEASE PRINT)

_____ DATE _____
(SIGNATURE)

Contact Information

LE Agency name here Administrative POC:

Name: _____

Title: _____

Phone: _____

Email: _____

LE Agency name here Day to Day POC:

Name: _____

Title: _____

Phone: _____

Email: _____

VT DMV Administrative POC:

Name: _____

Title: _____

Phone: _____

Email: _____

VT DMV Day to Day POC:

Name: _____

Title: _____

Phone: _____

Email: _____

Initial Call Information - [Assist - Facial Recognition] 01/22/14 12:12 : 120 State St, Montpelier, VT

Incident Number: 14MV000558
Call Time: 2014-01-22 12:12:38 -0500
Call Type: Assist - Facial Recognition
Primary Ofc.: ADM1: Codling, Kathy

Call Type	*Call Priority*	*Call Origin*	*Date & Time of Call*	*Location of Call*
Assist - Facial Recognition	In Progress	E-mail Request	01/22/2014 12:12	120 State St, Montpelier, VT, 05603

Area	*Team*	*Incident Number*			*Common Call Type*
Washington County	HQ Admin	14MV000558	☐ *Flag For Roll Call*	☐ *Call Cancelled By Complainant*	Owner Assist ADM1

☐ *Mental Health* ☐ *Alcohol related* ☐ *Drug related* ☐ *DOMV* ☐ *Cargo theft* *Drug Types*

Dispatch Narratives

```
------------- ADM1: Codling - 01/22/14 13:33 -------------
Facial request from Cari Crick case # 14-VIC-00333
```

Witness List

Person Type		*Name*	*DOB*	*Primary Phone*
Complainant	*Bus.*	Vermont Information & Anal		802-872-6110
		Address		
		188 Harvest Ln, Williston		

Responding Officers

Officer name		*Dispatched*	*Enroute*	*OnScene*
ADM1: Codling, Kathy	☑ *Primary*	01/22/14 12:12:46	01/22/14 12:12:51	01/22/14 12:12:52

Cleared
01/22/14 12:13:04

Secondary Location.

MRI# *NCIC NIC#* *Narrative* ☐ *Cancelled*

Incident Detail - : ADM1: Codling, Kathy

Incident Number: 14MV000558
Call Time: 2014-01-22 12:12:38 -0500
Call Type: Assist - Facial Recognition
Primary Ofc.: ADM1: Codling, Kathy

Occurred From	*Occurred To*	*Invest./Primary Officer*
01/22/2014 12:12	01/22/2014 12:12	ADM1: Codling, Kathy

Attachment	*Description*	*Uploaded at*			
Image/Photo	Image of individual	01/22/2014 13:33	14mv000558.jpg	*ADM1: Codling, K*	*Confidential*
Attachment	*Description*	*Uploaded at*			
Report	Top 50 matches fem	01/22/2014 13:35	14mv000558.pdf	*ADM1: Codling, K*	*Confidential*
Attachment	*Description*	*Uploaded at*			
Other	Facial Request Form	01/22/2014 13:37	14mv000558 request.pdf	*ADM1: Codling, K*	*Confidential*

☐ *TRO/FRO Exists*	☐ *Alcohol Involved*	☐ *911 Call Exists*	☐ *Medical Release*	☐ *Audio Recordings*	☐ *DCF Notified*	☐ *Crisis Svc Involved*	☐ *Swabbings*	☐ *SIU Contacted*	*SVU Contact*
☐ *Video Recordings*	☐ *Photos Taken*	☐ *Prints Lifted*	☐ *Diagrams*	☐ *Clothing Evidence*	☐ *K9*	☐ *Miranda Warning*	☐ *Other Evidence*	☐ *Crime Scene Processed*	*Lpr Used*

Evid. Search Conducted *Physical Evidence* *Media/Press Summary* *Opiate blocker*

Category	*Sub category*	*Violation*	*NIBRS Vio Type*	*Counts*	*#Premises*
Comm/Att	*IBR Scene/Loc Typ*	*IBR Crim Act Typ*	*IBR Gang Affil*	*IBR Agg.Aslt/Hom.*	*IBR Weapon Typ*	*NIBRS Override*
Point Of Entry	*Force/No Force*	*Point of Exit*	*Campus Code*	*Justifiable Homicide*	*Significant Event*

Narrative Type	*Officer*
	ADM1: Codli

Narrative

Ran photo through facial recognition. Provided response to Cari.

Offense Suspect	*Offense Victim*	*IBR Victim-Offender*		*Bias/Motivation (anti)*
V. was LEO	*V was LEO Assignment*		*Other ORI*	*LEOKA Narrative*

DMV - Enforcement

From: DPS - VT Intelligence Center
Sent: Friday, January 06, 2017 12:32 PM
To: Kentucky Intelligence Fusion Center
Cc: DMV - Enforcement
Subject: RE: FRS Request

Paul,

I CC'd the office in which you need to fill out their request form for a photo line up.

Thanks,

Rachel Cosker
Criminal Cyber Analyst
Vermont Intelligence Center
188 Harvest la.
Williston, VT 05495
802.872.6184

From: Vermont Intelligence Center [mailto:VIC@LISTSERV.DPS.STATE.VT.US] **On Behalf Of** Kentucky Intelligence Fusion Center
Sent: Friday, January 6, 2017 11:58 AM
To: DPS - VIC <VIC@listserv.dps.state.vt.us>
Subject: [VIC] FRS Request

It is requested that the attached probe photo images(s) of USMS federal fugitive [redacted] be forwarded to all Fusion Centers for exploitation by state Department of Motor Vehicles (DMV) facial recognition software (FRS).

[redacted] is being sought by the United States Marshals Service (USMS) for Violating Conditions of Supervised Release ordered in July 2010. [redacted] has convictions for Fraud and Misuse of Visas. Case number 2:09-CR-6-DLB. ORI #[redacted]

The following are some of [redacted]' identifiers:

DOB: [redacted]
POB: [redacted]
SSN:
FBI: [redacted]
HGT: 5'03"
WGT: 165
EYES: Brown
HAIR: Black

VERMONT

Request for Facial Recognition Investigation

DEPARTMENT OF MOTOR VEHICLES
Agency of Transportation

120 State Street
Montpelier, Vermont 05603-0001
802.828.2067
888-99-VERMONT
dmv.vermont.gov

Request to search the Vermont (VT) Department of Motor Vehicles (DMV) facial recognition (FR) photo repository, which contains license (DL) photos. These searches will be performed for the purpose of comparing suspect probe photos against photos housed in the VT DMV's FR photo repository and obtaining information that will advance active investigations, apprehend wanted fugitives or known or suspected terrorists, and locate missing persons. A probe photo refers to the photo of the subject of an active investigation that is submitted for search against a photo repository. The anticipated result of that search will be a photo gallery of potential matches. These potential matches (candidates) will be forwarded to the authorized requester, along with any associated information stored with the photo in the VT DMV FR system. The requester will then perform comparisons of the candidate photo(s) against the probe photo(s) to determine their value as investigative leads.

The intent of this service is **not** to provide a positive identification, but to provide the Law Enforcement (LE) User with an investigative lead and analysis to support that lead. The LE User will utilize the VT DMV FR photo repository to supplement information provided by existing investigative practices.

You agree to –

- Securely store photo images and text associated with the DL of the most likely candidate(s) to the probe in an official case management system for record keeping purposes.
- Immediately destroy all other gallery photos and associated information.

Date of Request:	Location of Incident:
Date of Incident:	Type of Incident:
Agency Name:	Case #:
Name of requester:	Title of requester:
Contact phone:	Contact email:
Charges:	

Suspect Information (if known)

Approximate age:	Gender:
Approximate height:	Race:

DMV Use Only

Received by:	Date Received:
☐ Approved By:	Valcour Case #
☐ Not Approved By:	