

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 Non-Driver ID cards. Vermont DMV is committed to doing everything it can to combat identity theft and protect the identities of Vermont residents.

Frequently Asked Questions

Q: What is facial recognition?

A: Facial recognition is an 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 from establishing multiple identities which can then be used for illegal purposes.

Q: How does it work?

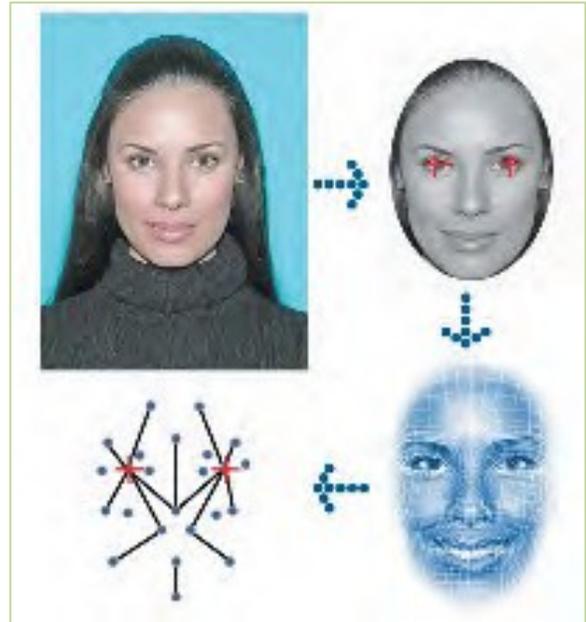
A: Recent advances in facial recognition technology have made the process of verifying the identities of individuals highly accurate and fast. Like fingerprinting, facial recognition is a form of identification that allows a computer to quickly establish your identity based on physical features unique to you. It simply uses the photograph of you 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 Driver’s License or Non-Driver ID in your name, facial recognition software will compare the photograph to

the one 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 Staff of a potential mismatch. Specially trained 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 also looks for matches with other templates to ensure a person's photograph is not already associated with another Driver's License under a different name. This is to ensure each person with a Driver's License, only has one. In any instance where identity fraud is suspected, the photos are immediately provided to trained staff 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 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. The software only knows how to take your template and compare it to other templates. It's not a function humans can perform.

Q: Why do we have facial recognition?

A: DMV wants to protect your identity from being stolen.

Identity fraud costs individuals and organizations billions of dollars each year, and victims can spend 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 we can ensure the information in your driver record is always up to date and entirely accurate.

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

A: No.

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

A: No one outside of DMV. Only specially trained DMV employees have access to your record.

In accordance with our mission to provide customers with the safest and most secure access to services, we carefully protect all the data associated with your DMV 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 has been, and continues to be, our highest priority. Authorized Law Enforcement agencies may submit images of suspects in crimes for analysis by DMV Investigators. No outside Law Enforcement agency has direct access to DMV FR system.