Photo by iStockphoto.com/ablokhin

What is the Difference Between Swiping and Scanning?

HOW DRIVER'S LICENSE RECOGNITION WORKS TODAY

BY BRIE PETERSON

When a security provider mentions driver's license recognition, what is your first thought? Maybe you see the benefits and think that capturing a driver's information at a gate increases the security of your community. Perhaps you view it as a security risk, a potential invasion of privacy. Concerns of that nature are valid,

especially as technology continues to advance. It seems stories in the news too often mention passwords and personal information being apprehended or credit cards getting hacked. Thankfully, when it comes to community security, the state of Florida has a law in place to protect community residents and their visitors when it comes to drivers' licenses.

Florida Statute 322.143 prohibits the "swiping" of drivers' licenses which could capture personal information from the magnetic strip or a bar code. Swiping is defined in the statute as "the act of passing a driver license or identification card through a device that is capable of deciphering, in an electronically readable format, the information electronically encoded in a magnetic strip or bar code on the driver license or identification card." If swiping is prohibited, then what happens at a gated entrance when you hand your license to a guard or insert it into a machine?

To provide communities with enhanced security, some providers will employ driver's license scanning. The difference with scanning is that it is the capture of the front of an ID. In other words, the scanner takes a picture of the front of the license; swiping does not take place, and the

sensitive information on the back of the card remains secure. The images obtained help communities when security companies are able to provide visitor records, like the name and image of a driver at a gate, without accessing or obtaining a driver's confidential information.

While driver's license scanning is one of the most secure forms of verification at communities, there are also added benefits. In some cases, a security company can use the image captured to expedite the entry process for permanent visitors associated with a community. This is typically through a method called optical character recognition,

which takes the image and converts it into data. When that data is recognized, a gate can automatically open for a guest. The advantage of this feature for communities is the fast entry for repeat visitors without losing security at an entrance.

After the definitions and processes are clarified, the next question that many ask is, "How does a guest enter if he does not or will not provide a driver's license?" The answer is simple: it is each community's decision. A security provider should abide by a community's orders regarding whether or not an ID is given. Some associations decide that entry can still be granted as long as the driver will say which resident he or she is going to visit. Other communities will say that entry is not allowed for the safety of the community if a driver is unwilling or cannot provide identification.

There are many vendors who can offer driver's license scanning to communities in Florida. Some may have the guards scan identification at an entrance, virtual guards may be used with driver's license scanning at a kiosk, or both on-site guards and virtual guards may be in place at an entrance. Whichever method is decided, an association should discuss the company's privacy policy for the images captured and how that information is stored. Each company will have differences in their policies, but they will help a community know how each user's information is protected.

If your community is considering the installation of driver's license recognition, it is important to explain the difference between scanning and swiping to the entire community. In addition, explaining the security benefits of capturing each visitor's ID can help avert misunderstandings and controversy. Still, if scanning of drivers' licenses is not the right direction, there are similar options that can be explored by communities. For instance, automatic license plate recognition also utilizes optical character recognition by converting vehicle tags to digital data and associating each tag with the corresponding guest.

Ultimately, the verification method at a gated entrance is chosen by the association and property manager. The security of the community is an investment that should not be taken lightly. It is also in the best interest of the community that gate systems be researched extensively by staff to determine what will best fit the needs of the community. Speak with a provider who knows the details of driver's license technology as well as a community attorney before finalizing a decision. Knowing the details of a new system will help the entire community transition smoothly if and when the time comes.

Please note, the author is not an attorney. If you have security questions or concerns, please email ask@enverasystems.com. ■