Jerry Hill
State Attorney

LEGAL ADVISOR

OFFICE OF THE STATE ATTORNEY TENTH JUDICIAL CIRCUIT

July 2016

INSIDE

Credit Card Fraud

By: Michael Hrdlicka

From the Courts

Office Locations

Bartow
P.O. Box 9000, Drawer SA
Bartow, FL 33831-9000
Phone: (863)-534-4800
Fax: (863)-534-4945

Child Support Enforcement
215 N. Floral Avenue
Bartow, FL 33830
Phone: (863)-519-4744
Fax: (863)-519-4759

Lakeland
930 E. Parker Street, Suite 238
Lakeland, FL, 33801
Phone: (863)-802-6240
Fax: (863)-802-6233

Sebring
411 South Eucalyptus
Sebring, FL 33870
Phone: (863)-402-6549
Fax: (863)-402-6563

Wauchula
124 South 9th Avenue
Wauchula, FL 33837
Phone: (863)-773-6613
Fax: (863)-773-0115

Winter Haven
Gill Jones Plaza
3425 Lake Alfred Rd. 9
Winter Haven, FL 33881
Phone: (863)-401-2477
Fax: (863)-401-2483

Credit Card Fraud

Michael Hrdlicka, Assistant State Attorney

Since banks introduced credit cards as a form of payment, criminals and scammers have been hard at work figuring out ways to steal, forge, and profit off them. Last year alone, criminals stole or compromised the cards of nearly 32 million Americans. Credit card fraud accounts for countless billions of dollars in theft. While retailers and consumers are moving to more secure alternatives, credit card fraud will likely always exist.

The new chip and PIN system that American banks and retailers are adopting is an improvement on the old magnetic strip. However, this advancement is quite a long ways away. The new system will include a chip on each credit card which will assist in securing transactions. But only 50% of cards in consumers' hands will include the new technology by the end of 2016. Likewise, only 50% of retailers will even be prepared to offer point of sale terminals to handle the new cards by June of 2016.

Banks are encouraging retailers to adopt these changes more quickly by holding them liable for fraud if they haven't updated their equipment. However, the cost of updating those systems will likely prevent smaller chains from updating quickly. That in combination with the fact that there will be plenty of old cards floating around without the new chip, means that credit card fraud will continue to be a tool for criminals and an issue for law enforcement agencies.

Michael Hrdlicka ,
Assistant State Attorney

Credit Card Fraud 101

The easiest way to commit credit card fraud is simply to steal the actual physical credit card from a victim. However, that method of credit card fraud isn't the focus of this article. Instead, I'm going to discuss larger scale credit card fraud. These crimes involve identity theft and the production of fraudulent credit cards.

Initially, the criminal has to obtain the credit card information from his victims. The tried and true method of this is through the use of credit card skimmers. These are small devices that criminals place inside points of sale. The purpose of these devices is to log the credit card information of any card that is swiped at that point of sale. The traditional spot that criminals place these is at the gas pump. Skimmers are placed inside the point of sale at the pump and then retrieved later. At a busy gas station, it isn't unthinkable that these skimmers might log hundreds of unique credit cards.

Recently, groups have been able to compromise points of sale through other means. Hackers have also been able to access information databases from retailers that have given them long lists of potential victims and their credit card information. This information, either stolen using skimmers or from hacking commercial databases, is then used to create fraudulent credit cards. Websites even exist where criminals can purchase large quantities of credit card information complete with reviews by other purchasers.

Having obtained that information, criminals begin the process of creating their fraudulent credit cards. This process is extremely simple. Every card with a magnetic strip—from the credit card in your wallet, to your driver's license or even a hotel room key—can be reprogramed in seconds. Criminals can use simple devices hooked up to a PC or even a cellphone to encode stolen credit card information onto a credit card's magnetic strip. In addition to these devices, blank credit cards or gift cards and embossers are available for sale on the internet. These blank cards can be used to create fraudulent credit cards. Criminals then use these fraudulent credit cards to make purchases or sell them to others.

Evidence of Credit Card Fraud

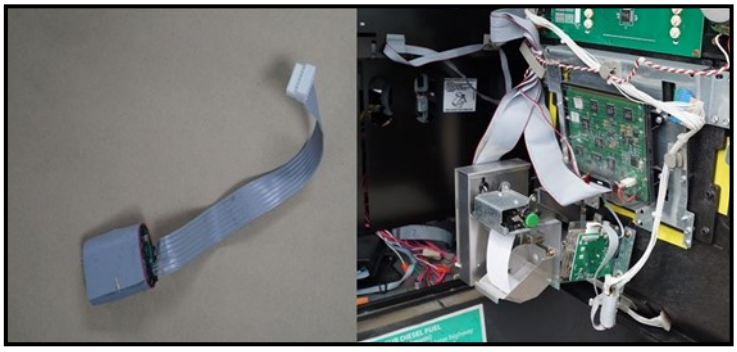
One of the key takeaways from the process of how criminals carry out credit card fraud is that evidence of credit card fraud doesn't always immediately suggest criminal activity. A potential suspect may have ten credit cards on his person, but that by itself is not necessarily illegal activity. So what are some signs that a suspect is involved in credit card fraud?

Typically when arrests are made of credit card fraud suspects, they have a high number of credit cards in their possession. These cards also tend to have the names of other people on them. However, even if all the cards have the name of the suspect embossed on them, it can be useful to review any credit card receipts that may be available. If a suspect with a large

number of credit cards in their name has receipts that have the names of other people on them, it is likely that those credit cards have been re-encoded with stolen credit card information.

Likewise, the tools discussed above are all signs of credit card fraud. Blank cards, embossers, and reencoders are all telltale signs of credit card fraud. Skimmers come in a variety of shapes and sizes. In the past, skimmers were designed to be placed over the outside of point of sale devices. Criminals would simply attach a skimmer that mocked the credit card receptacle to the outside of the point of sale. They might also combine this device with a camera that could be installed to view people inputting PINs.

However, recently skimmers have moved inside the devices themselves. Criminals will open up the point of sale devices and install skimmers in the wiring that will log credit card information. Obviously, it is a little more difficult to determine the criminal nature of these types of skimmers. However, these devices can be used to tip the balance of what may otherwise appear to be innocent conduct to conduct that supports a finding of probable cause or reasonable suspicion.



State of Credit Card Fraud Law

Crimes involving credit card fraud can be found in Chapter 817 of the Florida Statutes. Specifically, F.S. 817.57 to 817.685 cover credit card fraud. A number of different statutes from this section can be used to charge suspects.

In addition to those statutes, another important statue to be aware of with credit card fraud is F.S. 817.568. That statute covers identity theft. In order to charge under that statute, you would likely have to identify someone whose identity has been stolen and contact them.

An issue that may arise during the investigation of credit card fraud is whether reviewing the information contained on the magnetic strip by running them through a reader constitutes a search under the Fourth Amendment. This issue has not been litigated in Florida courts to this date. However, there are two federal cases that cover the subject and both agree that this does not constitute an illegal search.

In 2013, a US district court reviewed this issue in US. V. Alabi, 943 F.Supp.2d 1201. In that case, law enforcement officers had seized 31 credit cards during a traffic stop. They then ran those cards through a reader and used information from those cards in support of a search warrant. The defendants in that case argued that was an illegal, warrantless search.

The court ruled that this was not a search, because there was no physical trespass and the defendants did not have a reasonable expectation of privacy. The court analyzed the purpose of credit credits. Credit cards are designed to be used at retailers. Their very nature requires that the information on them be dispersed to third parties. While we definitely take efforts to keep that information private and secure, the court highlighted that credit card information is information that is designed to be disclosed and given away.

There was no evidence presented in that case that the credit cards seized had ever been used, so the court ruled that the defendants may have a subjective expectation of privacy. However, because of the way we use credit cards, the court concluded that there was no reasonable expectation of privacy and, thus, it was not an illegal search to review the credit card information on the cards that had been lawfully seized incident to arrest.

Since that case, we have had a number of court decisions in regards to cellphones by our Florida Supreme Court and the US Supreme Court. In US v. Bah, 794 F.3d 617, another district court reviewed a similar fact pattern and issue. That case was published in 2015 after those cellphone court decisions had been published. In its review of those cases, the court in Bah still agreed with the court in Alabi and upheld the review of credit card information in that case. They declined to extend the protections afforded in the cellphone cases to credit card information, due to the type of information stored on credit cards and the purpose of that information.

Keep in mind that in both of these cases, the cards were seized incident to arrest. A big factor in the court's determination was that law enforcement already had access to the cards. They did not rule whether running a card through a reader prior to seizing them would be a search. In that situation, a court may still rule that there was no expectation of privacy, but consent is always your friend and clears up many search and seizure issues.

Criminals and scammers will always be looking for new ways to make money off of unsuspecting victims. It is up to us to be aware of their techniques and know what to look out for. Because of the easy availability of the tools of the trade, it doesn't take a specialized set of knowledge to produce fraudulent credit cards. Knowing the some of the signs of credit card fraud can help turn an ordinary traffic stop into the seizure of dozens of fraudulent credit cards and an arrest on several different felony charges. Stay safe and good luck!

FROM THE COURTS...

SEARCH AND SEIZURE – TRAFFIC STOP

The defendant was driving on a highway at 45 mph. The speed limit was 65 mph, with a minimum of 40 mph. Traffic was light and nothing prevented other vehicles from passing the defendant in another lane. Nevertheless, a deputy stopped the defendant for impeding the flow of traffic. It was discovered that the defendant was driving on a suspended license and was a felon in possession of a gun. The trial court denied the defendant's motion to suppress and the defendant pled. On appeal, the Second District Court reversed the trial court, holding that the vehicle was driving within the permissible range of speed and was not being driven at such a slow speed as to impede or block the normal flow of traffic. Additionally, any concerns the deputy had for the medical condition of the driver were simply not supported by the circumstances. His driving pattern was normal, just slow, but within the limits permitted by law. Agreda v. State, 39 Fla. L. Weekly D2516a (Fla. 2nd DCA December 3, 2014).

www.SAO10.com

The Legal Advisor is published by:

Office of the State Attorney,
10th Judicial Circuit
P.O. Box 9000 Drawer SA
Bartow, FL, 33831

– The Legal Advisor Staff –

Jerry Hill, Publisher
Email: jhill@sao10.com

Brian Haas, Managing Editor
Email: bhaas@sao10.com

Nicole Orr, Content Manager
Email: norr@sao10.com

Steven Titus, Graphic Design
Email: stitus@sao10.com