Jun 27, 2019

**Contact** Whitney Ray

**Phone** 850-245-0150

OFFICE OF THE ATTORNEY GENERAL STATE OF FLORIDA

# Florida Attorney General's Office News Release

## Consumer Alert: New Skimming Spoofing Stealing Scam


TALLAHASSEE, Fla.—Attorney General Ashley Moody is issuing a Consumer Alert following growing reports of a new multilayered scam involving skimming, spoofing and stealing financial information. The scam works like this: a scammer uses a skimmer to steal credit or debit card information, then uses spoofing technology to pose as the representative of a financial institution. Once the scammer reaches the target, they inform the target that an account is compromised and the CV2 security code is needed to freeze the account. The scammer then takes this information to make purchases, withdraw funds or sell the stolen account information. Attorney General Ashley Moody said, “This scam incorporates some of the worst uses of modern technology to drain victims’ bank accounts and ruin their credit. Floridians must arm themselves with the latest information and take steps to avoid these fraudsters to protect their hard-earned money.”

FDLE Commissioner Rick Swearingen said, “Scammers looking to prey off the hard work of Floridians have no place in our great state. While FDLE and our law enforcement partners continue to work to combat scams like this and bring the perpetrators to justice, we urge all Floridians to learn about this and other scams to better protect themselves from becoming victims.”

The Florida Department of Law Enforcement is receiving a growing number of reports about this multilayered scam. To protect sensitive financial information, consumers should first guard against skimming by:

· Paying with cash or a credit card with chip technology instead of a debit card. Most credit cards

offer additional fraud protections;
· Monitoring transactions on financial accounts regularly to spot any unauthorized charges;
· Reporting unauthorized charges immediately and closing down compromised accounts; and
· Inspecting card readers, especially at outdoor locations such as gas pumps and ATMs, to see if a skimming device is placed over the card reader or if the security seal is broken.

For more tips on avoiding skimmer fraud, click here. To report skimmer fraud, contact the Florida Department of Agriculture and Consumer Services by calling 1(800) HELP-FLA or by clicking here.

This new scam also involves spoofing. Spoofing allows scammers to change the display on caller ID to make it appear as though the call is coming from a financial institution or government agency. To prevent scams involving spoofing, like this one, consumers should:

· Never automatically trust the number listed on caller ID;
· Just hang up if a caller claims to be from the consumer's financial institution asking to verify or confirm account information. Then call the phone number listed on the back of the card or on account statements;
· Not provide any financial account numbers, pins, Social Security numbers or other personal information in response to a solicitation; and
· Tell the financial institution to cancel the affected card or account, if it is determined that a caller is in possession of sensitive account information.

Anyone who may be the victim of this scam should contact local law enforcement and report the scam to the Florida Attorney General's Office by visiting MyFloridaLegal.com or calling 1(866) 9NO-SCAM.

# # #

*The Florida Attorney General's Consumer Protection Division issues Consumer Alerts to inform Floridians of emerging scams, new methods used to commit fraud, increased reports of common scams, or any other deceptive practice. Consumer Alerts are designed to notify Floridians about scams and available refunds in an effort to prevent financial losses or other harm caused by deceptive practices. Anyone encountering a scam should report the incident to the Florida Attorney General's Office by calling 1(866) 9NO-SCAM or visiting MyFloridaLegal.com.*