

Jul 18, 2023

Contact Kylie Mason

Phone (850) 245-0150



OFFICE OF
ATTORNEY GENERAL
ASHLEY MOODY
— Stronger, Safer Florida —

Attorney General Ashley Moody News Release

VIDEO: Attorney General Moody Announces Cyber Fraud Enforcement Unit to Combat Increase in Cybercrime



TALLAHASSEE, Fla.—Attorney General Ashley Moody today announced the Cyber Fraud Enforcement Unit to combat illicit online activity in Florida. According to the Federal Bureau of Investigation’s Internet Crime Complaint Center, [more than 42,000 Floridians lost a combined total of more than \\$844 million](#) to cybercrime last year. The Cyber Fraud Enforcement Unit is a team of criminal and civil attorneys in the Florida Attorney General’s Office who work with Florida Department of Law Enforcement analysts and other law enforcement agencies to solve cybercrimes that may be overlooked by federal authorities due to the size of the case.

Attorney General Ashley Moody said, “As online crime increases, the enforcement gap continues to grow as federal agencies often focus attention on cases involving multimillion-dollar losses. Noticing this gap in enforcement, I worked with legislative leaders and our law enforcement partners to build a team of expert attorneys to help fill that void and protect Floridians from emerging high-tech schemes.”

Florida Department of Law Enforcement Commissioner Mark Glass said, “FDLE’s cyber fraud team will help keep Florida citizens safe by investigating and stopping these pervasive

crimes. Our analysts are on the frontlines researching cybercrime and criminal organizations, identifying the players, learning how these crimes work and who is being victimized. These behind the scenes heroes are an important resource, not only for FDLE, but also for our law enforcement partners.”

Attorney General Moody’s Cyber Fraud Enforcement Unit is already working with FDLE and law enforcement on cybercrime investigations across the state. Last week, the unit and FDLE announced the [shutdown of a complex criminal enterprise](#) that used the dark web and cryptocurrency to commit massive identity theft and launder more than \$350,000. If convicted, the ringleader in the case could potentially face up to 135 years in prison.

Other cases handled by the Cyber Fraud Enforcement Unit include:

- [Kevin Anderson](#)—Anderson fraudulently purchased more than \$150,000 worth of items using credit cards created with the personal information of 20 victims residing in Florida and internationally. Anderson pleaded guilty and is sentenced to more than five years in prison, followed by 10 years’ probation to pay restitution.
- [Cathy Green](#)—Green used privileged access to an employer’s computer systems to adjust personal pay to include fraudulent overtime payouts of more than \$107,000. Green also used a company’s Amazon account to illicitly purchase more than \$41,000 of items. Green is sentenced to 15 years’ probation and ordered to pay more than \$109,000 in restitution.
- [Cynthia Sirmans](#)—Sirmans, a former live-in caretaker, charged more than \$47,000 to an elderly client’s credit card during a four-month period. Sirmans is sentenced to 16 months in prison for elderly exploitation.
- [Maninder Singh Bawa](#)—Bawa stole thousands of dollars from more than a dozen senior victims in a tech-support scam. Bawa targeted the victims by sending pop-up computer notifications claiming the victims’ devices were locked, prompting the seniors to call the number listed for service, where he tricked the victims into sending thousands of dollars in fees as payment. This case is still pending and Bawa is facing charges of money laundering and organized scheme to defraud.

[Victims of cybercrime should](#) immediately:

- Secure devices by changing all passwords;
- Preserve evidence by taking screenshots;
- Report the crime to [FDLE’s Computer Crime Center](#);
- If the crime involved unauthorized access to financial accounts, notify the bank and credit card company—monitor accounts to check for identity theft;
- Freeze credit; and
- Update antivirus, firewall and security software.

To freeze your credit to prevent further damage from identity theft, visit each of the three credit bureaus:

- [Equifax](#)
- [Experian](#)
- [TransUnion](#)

Prevention is also key. For more tips and updates on emergency cybercrimes and other schemes, visit [MyFloridaLegal.com/ConsumerAlert](https://www.myfloridalegal.com/consumer-alert).

#