TESTIMONY AS PREPARED
OHIO ATTORNEY GENERAL MIKE DEWINE
U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
SUBCOMMITTEE ON CONSUMER PROTECTION,
PRODUCT SAFETY, INSURANCE, AND DATA SECURITY
WASHINGTON, DC
MARCH 21, 2017

Thank you Chairman Thune, Subcommittee Chairman Moran, and Ranking Member Blumenthal for holding this important hearing today to discuss how scams are affecting families in my home state of Ohio and families all across our country.

I have served now as Ohio Attorney General for just over six years. One of the things I am continually amazed by is both the number of scams that constituents report to my office and the increasing creativity of the scammers! As you all know, there have always been scam artists and cons. But, what is different today is that they now have the long arm of both the Internet and phones!

The Internet and social media have transformed the world we live in and the way we communicate. For example, grandparents who live miles apart from their grandkids, can now see them with the touch of a button on their mobile devices. Unfortunately, scammers also use these modern conveniences to commit fraud and satisfy their greed.

"Grandparent scams" are one of the most frequently reported -- and most gut-wrenching -- scams my office receives. My wife Fran and I are the parents of eight children -- and now grandparents of 22 grandchildren. Like any grandparent, there is nothing we wouldn't do for our grandkids. And that is exactly the mentality that the scammers prey upon.

The scam often begins with a phone call telling grandparents that one of their grandchildren has been in a car accident, caught with drugs, or put in jail. The caller pretends either to be the grandchild, an attorney, or a law enforcement officer and tells the grandparent to send money to have the charges dismissed, to cover court costs, or to allow the grandchild to return home.

There is always a sense of urgency with these scams. The grandparent is told to go to the store right away, to buy several gift cards, and to read the card numbers over the phone. Using this information, the scammer then drains the funds on the cards almost instantly.

As part of the scheme, grandparents often are instructed not to talk to other people (such as the grandchild's parents) about the problem. Callers may even threaten to shoot or harm the grandchild if the grandparent refuses to pay.

And, if grandparents pay once, they likely will receive additional calls seeking more money, supposedly for attorney's fees or other unexpected costs. Eventually, grandparents discover that their grandchild was not truly in trouble. But by then, it is too late. The average loss to an

individual Ohioan because of this scam is $5,309. And that's just based on the cases reported to my office. Because so many go unreported, that figure is likely much higher.

Another popular scam is the "romance scam!" In a typical romance scam, the con artist "meets" the victim online through a dating or social networking site. The scammer often claims to live in the United States, but says he or she is temporarily located overseas due to a military assignment, business trip, or personal vacation.

One common theme of this scam is that the victim never actually meets the scammer face-to-face. Instead, the scammer may spend months developing a relationship with the victim online. Eventually, he or she asks the victim to send money to help cover some type of cost, such as airfare to visit the victim, medical expenses, or fees associated with military leave. The scammer often asks the victim to send the money via wire transfer or prepaid money card. Not surprisingly, once the money is sent, it is nearly impossible to recover. The average loss to an individual Ohioan for this scam is $26,518! And again, that number is just based on cases reported to my office. It, too, is likely much higher.

As Attorney General, I have been committed to treating these scams as what they are -- crimes. In 2011, I established an Economic Crimes Unit in my Consumer Protection Section. The unit includes seasoned prosecutors and investigators tasked with holding these fraudsters accountable and assisting local law enforcement and prosecutors in identifying, investigating, and prosecuting consumer fraud of a criminal nature. The unit consists of three attorneys and four investigators who are dedicated solely to criminal investigations.

To assist even more in the fight against scams, my office sought additional investigative power from the Ohio General Assembly in 2012. The result was new telecommunications fraud subpoena authority that our investigators and lawyers use every day to obtain financial and electronic evidence that furthers investigations and leads to arrests and prosecutions. This subpoena power is crucial in investigating scams that are exclusively Internet or phone-based.

Telephone and electronic communication are the major tools that scammers use to initiate contact with consumers. Unlike in the past, phone numbers are no longer a reliable indicator of where a call is coming from or who is making it. Voice over Internet Protocol (VoIP) phones allow callers to use area codes and phone numbers linked to a particular city or state, even though the person making the call is nowhere near there.

These services use a computer or smartphone to make calls through the Internet. Calls can be made using WiFi hot spots commonly found in airports, restaurants, coffee shops, and libraries. Criminals use the perceived legitimacy these phone numbers provide to help persuade unsuspecting victims into sending them money. We commonly see this tactic being used in IRS scams where the call appears to be originating from Washington, DC or Northern Virginia, but is instead coming from overseas.

Changes in how money is transferred have created additional challenges. Money transfer services, such as Western Union and Moneygram, were the traditional methods scammers used

to get money. While those methods are still in use, we've learned that scammers now rarely receive the money directly. They tend to use "Money Mules," who are people who've often been duped into thinking they're "Secret Shoppers" or getting an advance for a babysitting job or think they have a job processing payroll to receive the money and send it on -- often to someone overseas. These multiple steps are used to frustrate law enforcement and throw them off the trail. Also, people picking money up are required to provide very little, if any, formal identification, which further impedes our efforts to identify them.

Criminals have discovered another tool for moving money -- prepaid gift cards and reloadable debit cards. Scam victims are instructed to purchase prepaid or reloadable cards, most recently iTunes cards. They then provide the unique identifying number from the back of the card to the scammer, and the money is transferred from the prepaid card or reload card to the scammer's account almost immediately, leaving the victim holding nothing but a useless piece of plastic.

My office recently spoke with a victim who received a call telling her that her grandson had been in a car accident and that the judge would drop the charges if she paid $4,500 to an insurance company to cover the damage to a rented vehicle. The victim purchased prepaid cards, provided the card numbers to the scammer over the phone, and then was told to mail the cards themselves to an "insurance office" in Columbus, Ohio. My investigators found the address. As you would suspect, there was no insurance company.

Separate, but related, it's probably no surprise to you that many scam victims are targeted solely because of their age. To address this issue, my office created the Elder Justice Initiative and assigned staff to work with law enforcement, prosecutors, Adult Protective Services, and communities to identify, investigate, and prosecute elder abuse cases. We also host forums in local communities to educate seniors about how to protect themselves from cons.

As much as we try to educate consumers about potential scams, these cons are good at what they do and continue to rip off the vulnerable. Though many times, our investigations lead to dead ends, sometimes our work pays off in getting these bad guys. In 2013, for example, my office indicted and convicted 18 defendants for a national telemarketing ring that stole more than $2 million from thousands of victims in 41 states over a five-year period. That group used dozens of VoIP phone numbers, seasoned telemarketers, false websites, elaborate lies, and multiple businesses in Ohio and Florida to prey on owners of vacant, nearly worthless land throughout the desert southwest.

Also in 2013, attorneys from our Special Prosecutions Section convicted John Donald Cody of running a charity scam that stole millions of dollars intended for Navy veterans. Cody, who had assumed the identity of a man named Bobby Thompson, was sentenced in an Ohio courtroom to 28 years in prison and ordered to pay more than $6.3 million in fines.

Just last month, my office partnered with local law enforcement and indicted a 66 year-old-woman for her role in an alleged romance scam. According to investigators, the suspect lied to people about needing money for various reasons, such as claiming she had a serious illness or that she was at risk of losing her home. The victims, who included the suspect's family and

friends, believed her. Although the suspect generally promised to pay people back promptly, investigators determined that she sent the funds overseas to a man she had been communicating with online. This person's lies and deception cost her friends and family over $730,000!

This case comes on the heels of a 2014 investigation that my office initiated that led to a federally-convicted drug dealer pleading guilty to a running a romance scam that robbed over $1.1 million from unsuspecting victims across the country. The case began when my office received a complaint from an Ohio resident who had lost over $800,000 to a man she met online. My investigators tracked our victim's money to accounts in Maryland. We then reached out to local law enforcement, shared what we had learned, and provided evidence linking a convicted drug dealer to the scheme.

The drug dealer was the ringleader to a group of scammers who used a number of false stories and promises to convince the victims to give money, including stories about investing in fake gold that required payments for shipping and storage, fictitious sick family members who needed money, fake hospital bills, and fake plane trips to visit the victims. To help conceal the scheme and by using false documents, the conspirators were able to convince the victims to mail checks to a corporation that one of the cons had created and controlled or to wire money into bank accounts held in the name of that corporation.

Because of that single lead, we were able to develop that case into a federal investigation. It is that kind of state and federal cooperation that has brought justice not only to our Ohio victim, but also to victims throughout the United States.

As we approach April, IRS scams become more prevalent. The IRS scams and tax preparer frauds pose special challenges for law enforcement. Because of federal law, the Internal Revenue Service cannot and will not share tax or taxpayer information with our state criminal investigators. Let me tell you why that's important.

Our investigators will receive a complaint about someone who is doing taxes and is alleged to be stealing part of the taxpayer's refund by personally diverting the money. This single taxpayer can get his or her own records and provide them to us, but our investigators have no way of knowing how much larger the crime may be or how many more people may be being victimized because the IRS can't tell us anything at all. State subpoenas won't work, so our investigation ends up at a dead end.

The individual loss for this type of scam is generally less than $2,500.00. But, because we can't get access to information about other potential victims, that's where the case stops.

Whenever we receive an allegation of tax preparer fraud, IRS scam calls, or refund theft, we tell the consumer to contact the Treasury Inspector General for Tax Administration (TIGTA). Very few of these cases are ever likely to meet the dollar threshold required to get the attention of an IRS inspector, let alone a U.S. Attorney. Giving state and local law enforcement the ability to obtain the information needed to effectively investigate and prosecute tax preparer fraud, IRS scams, and refund theft wouldn't just protect taxpayers, it would conserve valuable federal resources and help ensure the integrity of our tax collection program.

There is strength in numbers. When multiple agencies put their resources, intelligence, and ingenuity together, great things can happen.

Ohio is a home rule state, with 88 counties and 88 county sheriffs and prosecutors acting independently from the other 87. That local control ensures that those elected officials are accountable to the people in their communities. It also ensures that these sheriffs and prosecutors know what's happening in their counties.

But, there are also challenges. A law enforcement officer in Jackson County, for example, may know about the three people who were ripped off in that county, but may not know about the three people who were victimized in Greene County, or the two people who were victimized in Clark County, or the person who was conned out of her life savings in Ashtabula County. Imagine how much bigger that problem gets when you start talking about victims in multiple states and victims who are hundreds or even thousands of miles away.

One of the reasons our Economic Crimes Unit has been successful is that we're able to see patterns of conduct occurring across multiple counties, make connections with law enforcement and victims, and show the true scope of a criminal enterprise. We need to apply that same logic to scams and economic crime nationwide. To be successful, we need to break down barriers to communication, sharing information, and resources and work together to combat crime on the national and international level.

We've seen that model work in Project JOLT, where the U.S. Department of Homeland Security has partnered with the Jamaican Constabulary Force, industry, and other law enforcement agencies to take down Jamaican lottery scammers -- a number of whom have recently been extradited to the United States to face federal charges. Now is the time to apply those lessons to others scams and crimes.

I am very proud of the work my office has undertaken to go after the scammers that prey on Ohio families. My office will continue to provide support for local law enforcement in an ongoing effort to hold scammers accountable. We're also committed to providing Ohioans with the information and education they need to avoid being victims in the first place. By doing these things, we are making a difference.

Thank you, again, for the opportunity to testify here today. I'm happy to answer any questions.