

My name is Sheryl Harris. I'm the Director of the Cuyahoga County, Ohio, Department of Consumer Affairs. Thank you so much for the invitation to speak in front of this committee.

Consumer Affairs organizes and convenes the Scam Squad, a financial fraud task force. Scam Squad's members include nonprofit and social service agencies that primarily serve seniors, county agencies, and enforcement agencies ranging from local police to the Cleveland offices of the FBI, the U.S. Department of Justice and the Federal Trade Commission.

Our members have three shared goals:

- Encourage county resident to report scams
- Share scam reports with the agency best suited to investigate
- Alert residents to current scam threats

We want to create easy ways for people to effectively report scams to enforcement agencies. We encourage members to share scam reports in databases that multiple agencies can access – primarily the FTC's Sentinel database. We create innovative scam alerts and reminders that can be replicated at scale. You have examples of those.

My office receives a small sliver of the scam reports filed by county residents – roughly 800 to 1,000 a year. About 10 percent of those involve a dollar loss. The majority of our scam reports come from our older residents. We interview people who report scams to us, regardless of whether they lost money, to help consumers limit the fallout from scams and spot changes in scam techniques and payment methods.

What I can tell you from these interviews is that scammers have designed psychologically complex scams designed to make people believe the scammer is a trusted authority. The scammer tells the person they're facing a dire problem – for example, they're about to be arrested, or the government is about to seize their bank account. The scammer is able to isolate the victim by giving a plausible-sounding reason they can't tell anyone else. The victims then become reliant on the scammer, whose "solution" routes money to the scammer.

Scammers use all sorts of technology in these scams. They pose as trusted authorities by spoofing Caller ID. They know information about people when they call, because of all the consumer data companies collect and sell – or fail to protect. And many scammers convince panicked people to allow them remote access to their home computers, so they can further manipulate victims.

Today, we're seeing individuals lose much larger amounts to scams in shorter periods of time than ever before. Scam losses reported to my office have doubled in the last year, from \$1.2 million in 2023 to \$2.7 million so far this year. That doesn't include losses reported to our partners.

In one scam, scammers posing as federal agents panic people into believing they are under investigation because drug traffickers are using their bank accounts. These scams are designed to terrify people into believing they're going to lose all their money – so when the nice, fake federal agent tells them they can protect their life savings by moving it to a government "wallet" – scam speak for crypto – people do it.

We know of at least two cases in which scammers posing as federal agents not only took victims' life savings, but they then told them they were in mortal danger and needed to move. When the

victims sold their houses, the scammers got the proceeds from the sales too. Many of those payments were made in crypto.

Crypto payments are fast. And they're final. There's no protection for consumers.

Just last week, the FTC said Sentinel data shows that from 2020 to 2023, scam losses involving crypto increased TENFOLD, to over \$110 million nationwide. Consumers over 60 are three times more likely than other adults to lose money in crypto.

I'm thrilled the banking committee is delving into meaningful ways to stop scams. Through your work, you have the ability to help Older Americans avoid life-altering losses to scams.

You can update regulations to ensure that ALL payment methods provide consumer protections that allow scam victims a way to get their money back.

No matter how someone pays a scammer – gold, crypto, gift cards -- the place consumers get the cash for those transactions is the bank. Banks have to do a better job protecting their customers from scams.

Thank you for your time and for the opportunity to speak.