Financial Exploitation Newsletter

Financial exploitation is on the rise, and the Alabama Securities Commission (ASC) is strengthening its commitment to investor education through a Financial Exploitation Newsletter. In our second issue, you'll find information about the ASC's new Financial Exploitation Division, financial protection resources from one of our partners, key financial exploitation statistics, and a look at some of the latest scams making their way into Alabama.

The ASC launched a **new Financial Exploitation Division** to better support Alabama's investors and financial industry. The new division has decades of collective experience with financial exploitation and is also available as a resource to the public to provide guidance on a number of challenging issues confronting victims and their families, communities, and firms.

(Pictured is the Division and other members of ASC that provide support: Back row, left to right - Special Agent Adam Patterson; Senior Special Agent Miles Faggert; Chief Deputy Steve Feaga; Special Agent Charles Traywick; Executive Assistant Kim Booher; Securities Regulatory Manager Michael Gantt; and Senior Special Agent Chip Harrison

Front row – Deputy Director of Enforcement Louis Franklin, Sr.; Attorney Jake Howell; Director Amanda Senn; Special Agent Elizabeth Planer; Victims' Services Officer Kasey Hartzog; Victims' Services Officer Deanna Thompson; and Senior Securities Analyst Tate Duncan

AARP FRAUD WATCH NETWORK ™

AARP Fraud Watch Network™ is a free resource to spot scams and get guidance from AARP's fraud specialists. In 2025, the AARP Fraud Watch Network helpline received **22,155** reports which identified **Identity Theft** (6298) as the top reported fraud. Other reports included **Imposter Businesses** (4839), **Romance Scams** (1960), **Tech Support** (1436), and **Investment Fraud** (826). **Cryptocurrency scams** accounted for $1.5 billion in losses.

The AARP Fraud Watch resources include:

- A Fraud Resource Center with more than 60 tip sheets providing dos and don'ts on common scams and fraud.
- A toll-free Fraud Watch Network Helpline, 1-877-908-3360, whose trained specialists offer peer counseling, support and referral services to fraud victims and their family members.
- Watchdog Alerts delivered by email or text message, on the latest scams and tips on how to spot them.
- A nationwide Scam-Tracking Map, where you can find the latest alerts from your state attorneys general and other officials, read what people are reporting in your state and report scams or suspicious emails and phone calls in your area.
- Hear stories of real scams on our award-winning podcast, *The Perfect Scam*. Explore fraud from the viewpoint of victims, law enforcement and criminals.
- Get social with the AARP Fraud Watch Network on Facebook and Twitter, where they will have access to online events.
- Check out online resources to help protect veterans, service members and their families against scams at the AARP Veterans Fraud Center.

Find out if a financial organization has received the AARP BankSafe training to fight financial exploitation at aarp.org/banksafe.

Reporting Statistics (2025)

Thanks to Alabama's financial industry, we were able to prevent millions of dollars last year from leaving investors' accounts and into the hands of fraudsters. A decision to delay, or hold, a disbursement or distribution can be a lifesaver for many victims when fraud is apparent. All of Alabama's financial Institutions have the authority to hold or delay transactions when fraud is suspected. The ASC continues its commitment to provide assistance to the industry to help combat fraud. The number of reports received doubled this year over last year.

653

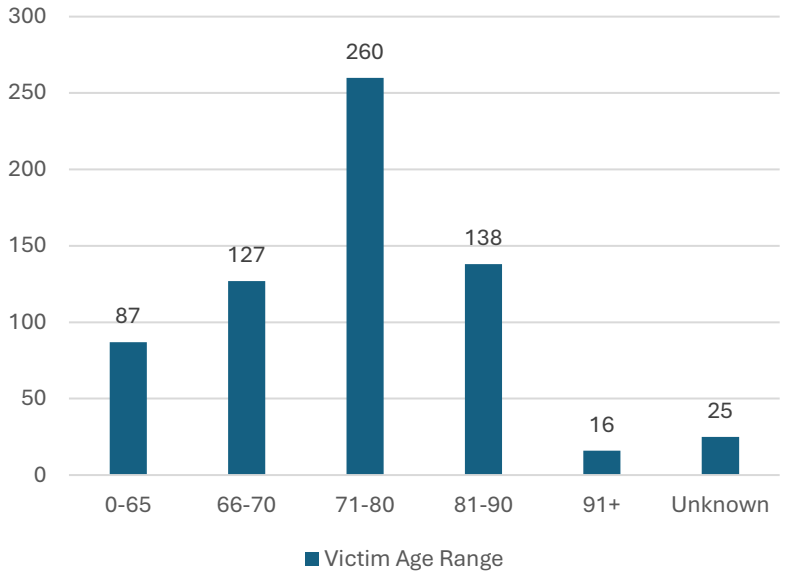
Reports from Industry

(2025)

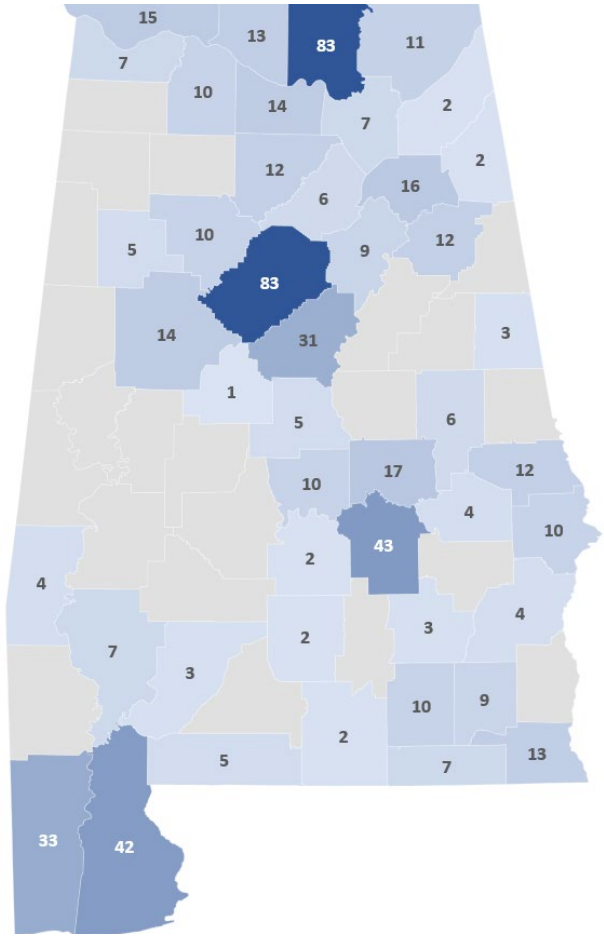
319 Reports (2024)

159 Reports (2023)

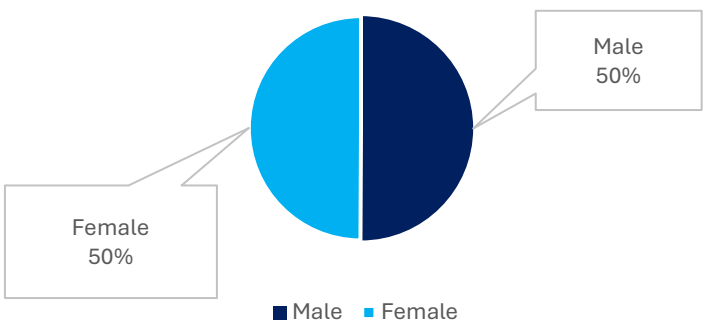
Victim Age Range



Victim Location by County



Victim Demographics



Report suspected financial exploitation to the Department of Human Resources and the ASC's Financial Exploitation Division at Financial Exploitation Reporting Form – Alabama Securities Commission.

SCAM ALERT

*The ASC receives a wide range of financial exploitation reports where scammers utilize various tactics to take advantage of unsuspecting victims. The **Scam Alert** page on our website provides the latest information on the most common fraud techniques and how Alabama residents can protect themselves from scams. The cases described below are examples of reports the Commission has received.*

Account Takeover Scam

The ASC has received several reports of account takeover scams. The victims received a message or pop-up notification from a scammer pretending to be Microsoft or McAfee. The victims clicked on the pop-up and allowed the scammer remote access to their device. The scammers logged into the victims' devices and were able to access their personal and financial information. The ASC informed individuals that McAfee or Microsoft will not ask for private information, such as your social security number, PIN numbers, or bank details. Account takeover scams can have long lasting detrimental effects and can leave a victim vulnerable to further exploitation, such as identity theft and financial losses.

Imposter Scam from Financial Institutions

Many Alabama residents have reported spoofing scams related to their financial institution. In the cases reported to the ASC, the victims received a text from a person or phone number identifying themselves as a representative from the bank or financial institution the victim uses. In most cases, the scammer has "spoofed" the legitimate number of the financial institution or bank. The fraudster then asks victim about a transaction that the fraudster claims was conducted on their account. When the victims respond that they are not aware of the transaction, a follow-up text or phone call occurs telling the victim they need to update their account information. Once the scammers receive this information, they immediately withdraw funds from the account. The ASC encourages individuals to always verify who they are communicating with before providing any personal or financial information. Banks and financial institutions will never ask for your account login information over the phone or text.

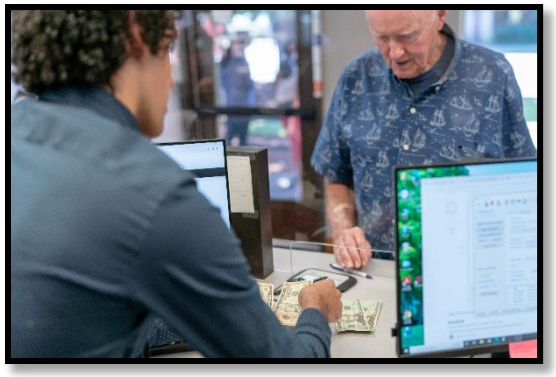
Mirrored Financial Institutions Website Scam

Scammers are creating fake websites that look identical to the real websites for banks and investment firms. When the victims click on the fake website and enter their login credentials, the scammer captures those credentials and uses them on the real company's site to log into the victims' real accounts. The scammers can also capture two-factor authentication codes sent to phones and emails in real time. To avoid mirrored website scams, always ensure the site is secure and has a lock icon with "https" in the URL. Check for any signs of inconsistency, spelling, or grammatical errors in the site before using it. Avoid clicking on sponsored ads for the company you are searching for online.

Money Mule Scams

The ASC received a report of a woman who was unknowingly being used as a "money mule". A money mule is someone recruited to transfer illegally obtained money for criminals, often through their own bank account, hiding the true source and identity of the fraudsters. This is a form of money laundering. The victim met the scammer on social media. They built an emotional connection, and the scammer told the victim he needed her to open an account to transfer money to a different currency. The victim wanted to help him, so she made transfers through a crypto exchange and other wire transfers. The victim did not realize her actions were illegal. The ASC cautions individuals to never hold or transfer money on behalf of others.

Family Member Exploitation



Family member, or domestic exploitation, is a frequently reported crime. Cases often involve estranged family members who suddenly become more involved as the named victim is advanced in years. Many of these victims are entirely capable of caring for themselves but "friends" or family attempt to gain access to financial accounts through fraudulently obtained Powers of Attorney or other estate documents including wills and trusts. The ASC encourages individuals to always have a trusted contact on their financial accounts. The contact should be someone you trust that can be contacted if you are unreachable or incapacitated. This person cannot change your accounts or make financial decisions on your behalf, but they can serve as an extra layer of protection for your accounts.