Financial Exploitation Newsletter

BY THE ALABAMA SECURITIES COMMISSION

Financial exploitation is on the rise, and the Commission is strengthening its commitment to investor education through a new Financial Exploitation Newsletter. In our first issue, you'll find information about financial exploitation in Alabama, including key laws, statistics, and a look at some of the latest scams making their way into Alabama.

Each quarter, we'll also cover important topics like artificial intelligence, cybersecurity, and cryptocurrency— explaining how fraudsters are using these technologies to deceive investors and steal their hard-earned money. We'll share real examples of cases being reported here in Alabama so you can stay informed and pass this information along to your clients, customers, and members. By spreading awareness, we can continue to work together to prevent the harm caused by financial exploitation and help keep Alabama a safe place to invest.

The Alabama Securities Commission's **"Scam Alert"** website page provides detailed information about the common techniques scammers use to manipulate emotions and threaten finances.

WHAT IS FINANCIAL EXPLOITATION?

Essentially the unauthorized or wrongful taking, withholding, appropriation, or control or conversion, of money, property, or assets through fraudulent of deceptive means. This can include through the use of a power of attorney, guardianship or conservatorship.

AUTHORITY TO DELAY AND HOLD TRANSACTIONS

All financial institutions are authorized to delay or hold financial transactions when there is reasonable cause to suspect that financial exploitation may have occurred, may have been attempted, or is being attempted.

REPORTING REQUIREMENTS

Mandatory Reporting by Agents, Investment Adviser Representatives.

Discretionary reporting by depository institutions, mortgage loan originators, pawnbrokers, small loan lenders.

To help protect Alabamians from financial harm, the Legislature has passed two important laws: the **Protection of Vulnerable Adults from Financial Exploitation Act (2016)** and the **Elderly and Vulnerable Adult Financial Protection Act (2021).** These laws give financial institutions stronger tools to identify and stop fraud, and to notify law enforcement when suspicious activity arises.

Since 2016, we've received **1,053 reports** of financial exploitation. Thanks to the reports we've received from financial institutions across the state, millions of dollars have been prevented from leaving Alabama due to fraud. Their partnership plays a critical role in protecting vulnerable adults and strengthening the safety of our financial system.

Financial institutions can help protect their clients by encouraging them to list a trusted contact on their contacts. This is a person the institution can contact if the client cannot be reached in case of an emergency or suspected fraud. The trusted contact cannot make financial decisions on the client's behalf.

Our Education and Public Affairs team developed a video to depict the devastating impact of financial exploitation on the victim. **CLICK HERE** to watch the video.

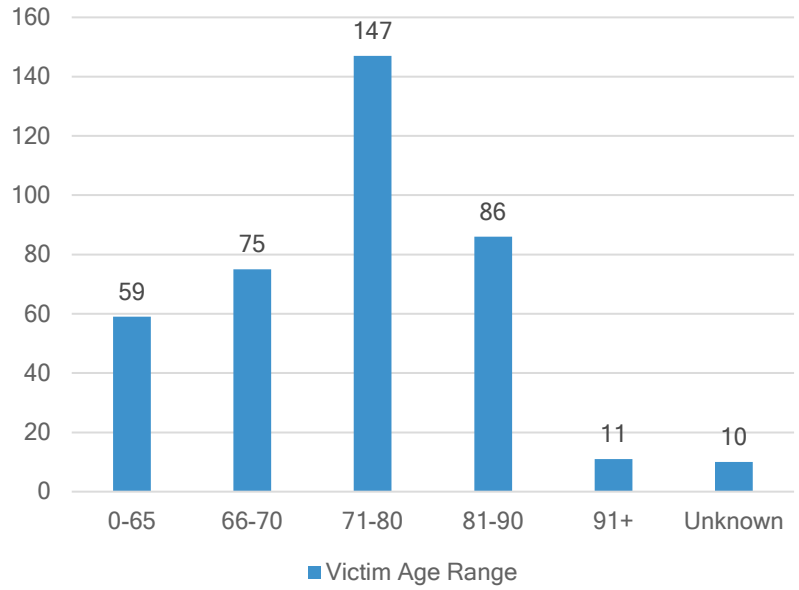
Reporting Statistics (Jan. – Aug. 2025)

ASC's Victims Services Officers (VSOs) receive financial exploitation reports and partner with the Alabama Department of Human Resources (DHR) to pursue them. Our VSOs receive reports from several sources, including banks, credit unions, investment firms, law enforcement, and law firms as well as family members, friends, and self-reports from victims.

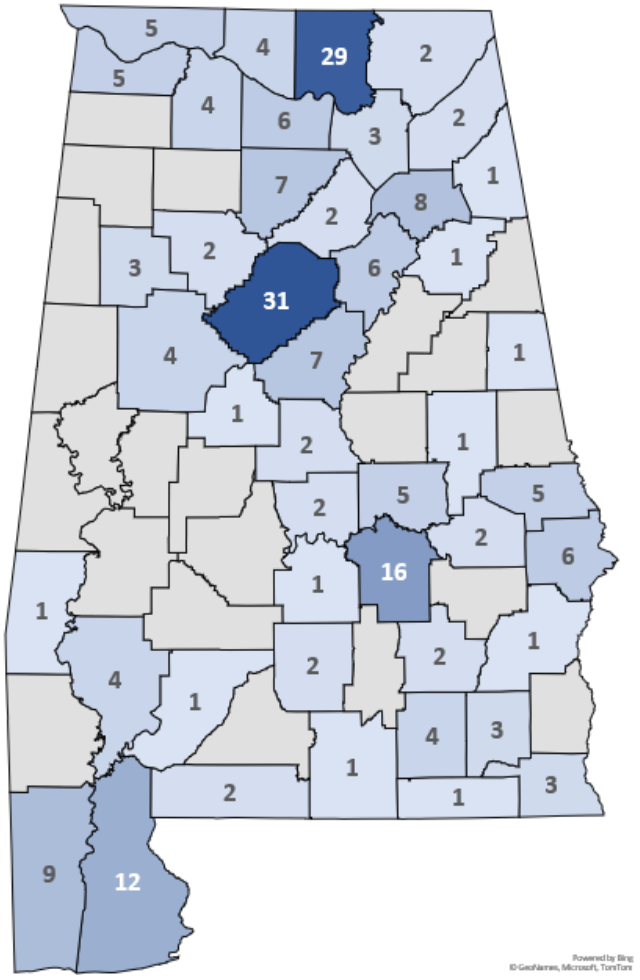
388 Reports

(Jan. 1 – Aug. 31, 2025)

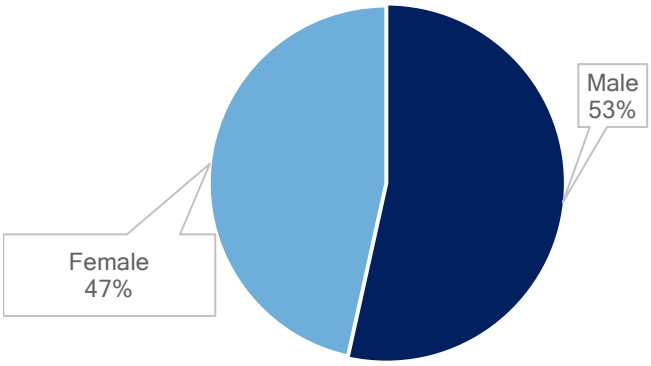
Victim Age Range



Victim Location by County



Victim Demographics



To report suspected financial exploitation, contact the local Department of Human Resources (DHR) in your county and the Alabama Securities Commission.

SCAM ALERT

The Commission 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 summaries of selected reports of scams in Alabama.

Publisher's Clearing House/Sweepstakes Scam

In 2025, the Commission received a report from a family member of an elderly victim. The victim believed that she had won a large Publisher's Clearing House lottery prize. The scammer informed the victim that she needed to pay taxes and fees in the form of cash and gift cards before receiving the prize money. The victim sent funds multiple times and attempted to take out a loan to pay the taxes and fees. The Commission, local law enforcement, and the Department of Human Resources attempted to inform the victim that she was being scammed, but she continued to send money to the scammer. In a final attempt to send money to the scammer, the victim placed her debit card inside of box and intended to conceal the contents of the package in order to mail send money to the scammer.

Pig Butchering Scam - Romance

The Commission received a report in 2025 from a community leader with concerns of financial exploitation against one of their elder community members. The victim became romantically involved with a man she met on social media. The man claimed to be a marine engineer in the Middle East who recently quit his job and needed $5,000 to fly to the U.S. to see her. He asked the victim to send him money via gift cards, wire transfers, and a cryptocurrency ATM for various expenses. Several community members and representatives from the Department of Human Resources informed the victim that she was being scammed, but she refused to believe them because she had grown to trust the scammer. Over time, the victim sent the scammer more than $40,000. The Commission met with the victim and her family to notify them that that she was a victim of the pig butchering scam.

Pig Butchering Scam – Cryptocurrency (Mandated Reporting)

The Commission recently received a report from a financial institution regarding one of their elderly clients. The victim transferred $300,000 from his investment account to his bank account to invest in cryptocurrency. He then requested an additional $110,000 to pay fees on his cryptocurrency profits so he could withdraw his returns. The Commission met with the victim and learned the victim was communicating with a stranger on social media. The new social media connection instructed him to make

his crypto investments using a crypto trading platform. The stranger told the victim that her uncle was a multimillionaire who could help the victim learn how to make money in cryptocurrency. The victim continued to communicate with the stranger on WeChat and Telegram. The victim was led to believe that his investments grew to nearly $600,000. The victim learned that there was trouble when he tried to make a withdrawal from his profits and was told he needed to pay additional fees. It was also discovered that the crypto-trading platform was fake. The victim was never investing. He was making deposits straight into a scammer's digital wallet.

Pig Butchering Scam – Cryptocurrency (Self Reporting)

The Commission received a report directly from a victim who was involved with a cryptocurrency scam. The victim received a text message from an unknown sender. After the initial communication, the scammer requested to move the communication to WhatsApp. The scammer encouraged the victim to purchase cryptocurrency and coached him on how to invest on a fake cryptocurrency trading platform. Between January 2024 and May 2025, the victim purchased more the $1.2 million of cryptocurrency. When he tried to make a withdrawal, the victim was notified that he would need to pay an additional $300,000 in fees to complete the transaction. After receiving this notification, the victim decided to research the trading platform and found that the Commission had issued a Cease-and-Desist order against them in November 2024. He immediately contacted the Commission and was informed that he was a victim of the pig butchering scam.

Romance and Employment Imposter Scam

A financial firm filed a report through the Commission's website for one of their clients who they believed was involved in multiple imposter scams. The victim believed she was in an online relationship with a famous actor and sent him thousands of dollars through Apple gift cards. After depleting her bank accounts, the victim contacted her financial firm to request $800 to purchase a plane ticket to Los Angeles to meet with the actor. She then informed her financial firm that she was speaking with someone who claimed to be "technology executive Elon Musk" who wanted to make her part of his management team for a salary of $10,000 a month. The victim contacted her financial advisor requesting to completely liquidate all her accounts, totaling nearly $130,000. Since the firm suspected that the client was being scammed, they denied her request, placed a temporary disbursement restriction on her accounts, and notified her trusted contact.