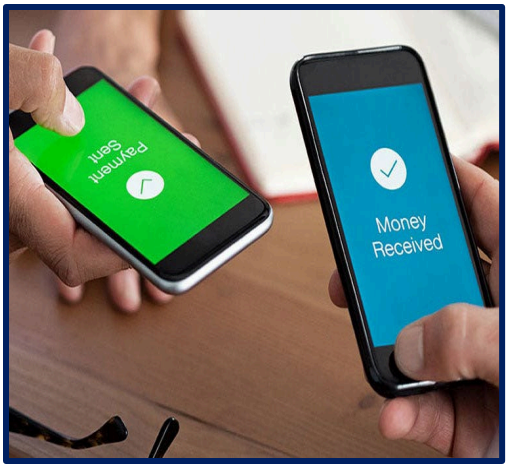
Financial Exploitation Newsletter

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 fourth issue, you'll find information about payment app fraud, key financial exploitation statistics, and a look at some of the latest scams making their way into Alabama.



What are "Payment Apps?"

Mobile payment apps are a convenient way to send, receive, and manage money using your smartphone. Most mobile payment apps connect to your bank account, debit card, or credit card, making it easy to transfer money, pay bills, shop online, or make purchases in stores.

Some popular payments apps are Venmo, Cash App, Zelle, and PayPal.

Types of Payment App Scams

Scammers use payment apps to steal money or personal information in many different ways. Here are a few common techniques.

Accidental Payment Scam

A stranger may send you a payment, then contact you to say they sent it by mistake. They will then ask you to send the money back as a new payment. Cyber-criminals are using stolen credit card information to act like they are sending you money. Once the card is reported as stolen, the credit card company will refund the fraudulent transfer. Meanwhile, the money you send back to the fraudster comes directly from your account!

Fraudulent Activity Alert Call or Text from Payment Apps

Scammers may impersonate customer representatives from payment apps to trick you into giving them account information. They may call or text you to inform you that an unauthorized transaction occurred or that hackers are trying to access your account. They may tell you that they need to secure the account and will need to reset your password.

Imposter Scams

Bad actors may attempt to replicate a profile picture on a fake account to impersonate your friend, co-worker, potential new employer, landlord, or love interest. They will impersonate someone in your social circle and request money.

ASC recently released a video showcasing how a payment app scam works. CLICK HERE to watch the video.

Reporting Statistics (Q2 2026)

Thanks to Alabama's financial industry, we have prevented millions of dollars from being lost to fraud and theft. A decision to delay, or hold, a disbursement or distribution can be a lifesaver for many victims when fraud is apparent. Alabama's financial institutions have the authority to hold or delay transactions when fraud is suspected against a senior or vulnerable adult. More than **2,000** reports have been filed since 2016 when the reporting laws were enacted.

244

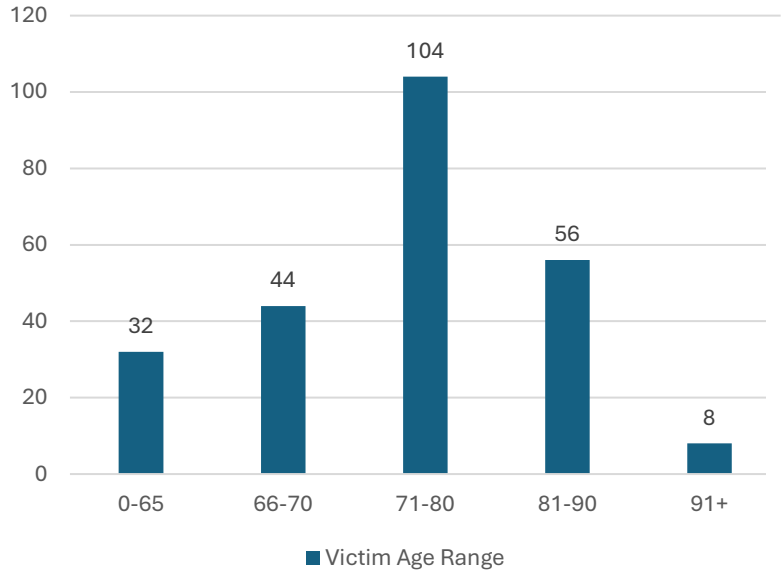
Reports from Industry

(Apr.1 – Jun. 30, 2026)

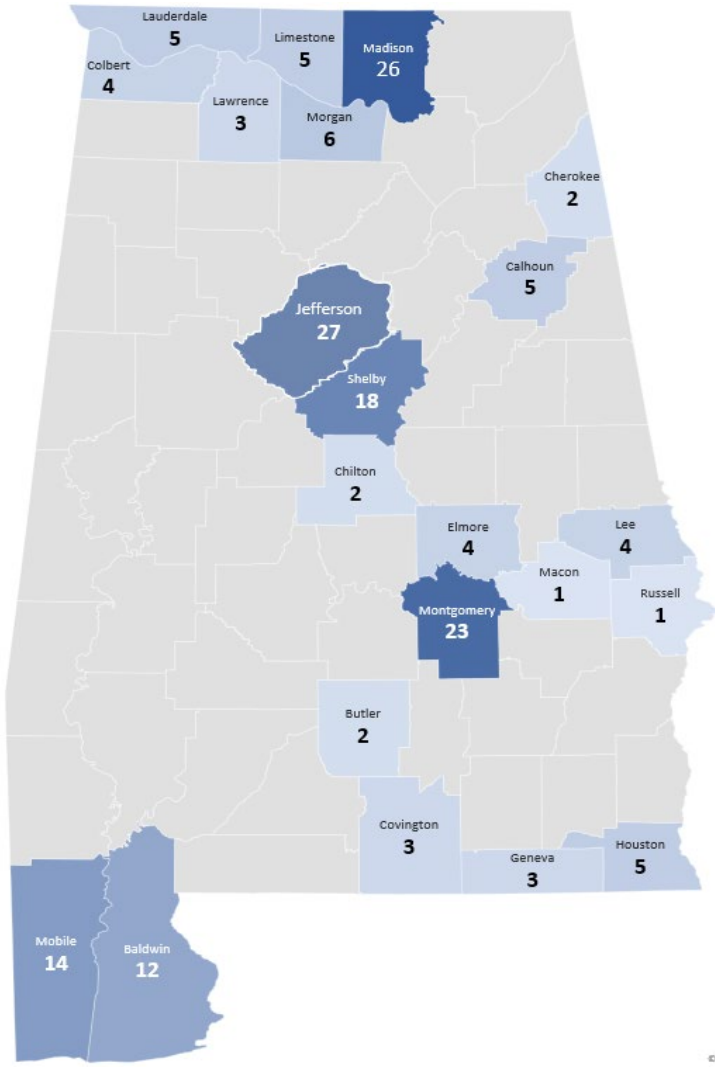
30%

Increase in reports from Q1 2026.

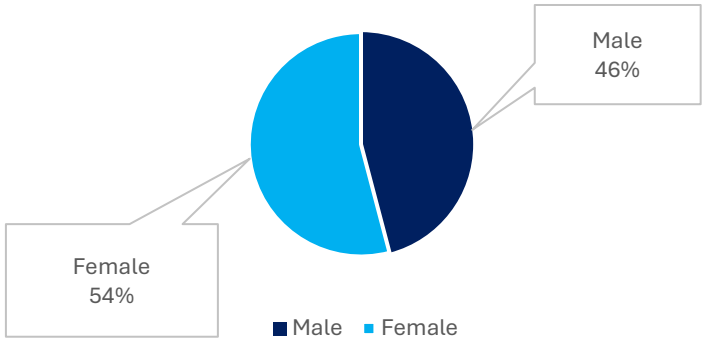
Victim Age Range



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.*

Financial Exploitation of a Family Member



Many of the financial exploitation reports that ASC receives are related to deception and theft by a family member of the victim. In several recent reports from financial institutions, the child or grandchildren of a senior adult has been added to the account as a joint owner or given permission to make withdrawals on the senior's behalf for specific purchases, such as buying household items, groceries, or getting cash for the senior adult. Upon further investigation, it was found that the family members were making unauthorized purchases or withdrawals that were not approved, such as buying cars and taking out cash, totaling more than $90,000 in a two-year period without the victims' knowledge. In cases where the family member has been added as a joint owner, those family members technically have rights to the funds in the account. We encourage senior adults to have a trusted contact on their accounts instead – a person who can be notified if there is an issue with the account, but that cannot make withdrawals or financial decisions on the account.

In Person Romance Scam

ASC received a report from a financial institution with concerns that one of their clients was involved in a romance scam. The victim had been sending funds to a "friend" who said that she was training for a new job. After speaking with the client, the financial institution found that he had been in a two-year relationship with this individual whom he met in person. Throughout the two-year relationship, he'd sent her nearly $200,000 for various family expenses, such as funerals, travel, children's items, medical expenses, and car troubles. He also liquidated funds from a brokerage account and took out loans to help her. ASC's Victims' Services Officers met with the client to inform him that he was involved in a romance scam.



Payment App Scam – Customer Service Impersonation



In many fraud cases involving payment apps, the scammer is impersonating a customer service representative or someone known to the victim. ASC recently received a report from a victim who received an email from "PayPal" with concerns of fraudulent activity on her account. The victim did not have a PayPal account but responded to the email. She was then contacted by someone posing as the Federal Trade Commission claiming that her social security number was compromised due to the fraudulent PayPal account activity. The scammer convinced her that she needed to liquidate her checking and savings accounts for "safe keeping." She liquidated $30,000 from both accounts. The victim reported that a man came to her house to retrieve the money, and she gave him envelopes of cash. When she attempted to liquidate her investment accounts, her investment firm asked her to come into the office for a meeting along with her daughter. They informed her that she was involved in a scam.

Protect Yourself from Payment App Scams!

For Accidental Payment Scams:

- Never exchange payments with people you don't know.
- Contact the app's customer service to reverse a payment from an unknown sender.
- Never communicate with a stranger who sends you money.



For Fraudulent Activity Alert Scams

- Never provide verification codes, passwords, or remote access to your device.
- Never install third-party apps.
- Never let someone create accounts on your behalf.
- Remember that payment apps will never redirect you to send money through a different platform or ask you to send money to verify an account.

For Impersonation Scams:

- Contact the real person outside the app by phone using a known number.
- Never send money to strangers you haven't met in person.
- Check the account creation date and transaction history for red flags.