

EXECUTIVE SUMMARY

IDENTITY THEFT

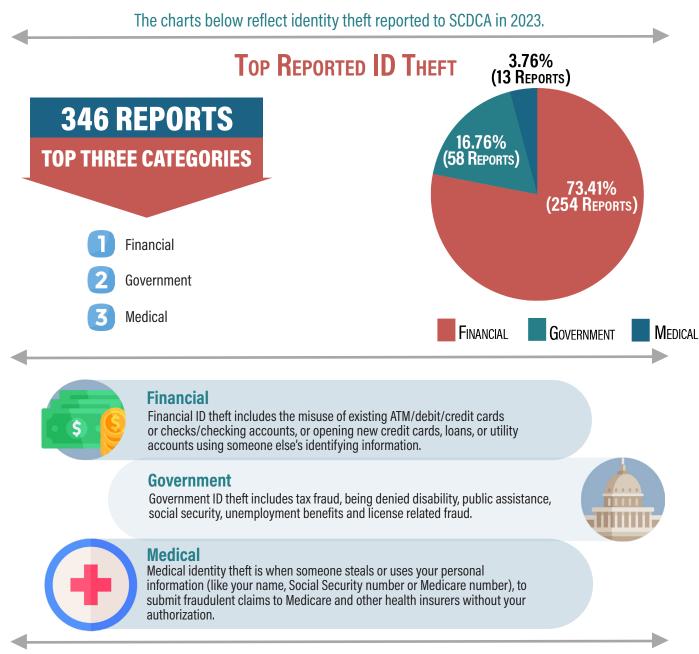
- The 2024 report contains information from 346 reports of identity theft reported from January 1 to December 31, 2023.
- The top three types of identity theft were: Financial (73.41%), Government (16.76%) and Medical (3.76%).
- Nearly thirty-one percent of identity thefts were reported to the police.
- Top three discovery methods for identity theft: Business Notification (33.62%), Bank Notice (24.26%) and Government Notification (12.77%)
- The sum total of potential losses to the consumer was \$578,738 and the sum total of actual losses reported was \$1,026,915.
- Top three counties for identity theft reports: Richland (15.90%), Lexington (8.67%) and Greenville (7.51%).
- Nearly 19 percent of those filing an identity theft report did not provide their age when filing. The largest groups of people that provided their ages were 35-44 year-olds (15.98%), 55-64 year-olds (15.38%) and 65-74 year-olds (14.2%).

SCAMS

- The 2024 report contains information from 963 scams reported from January 1 to December 31, 2023.
- The top three types of scams were: Purchase (18.59%), Service/Repair (10.70%) and Lottery/Prizes/Sweepstakes (10.38%).
- Fifty-three percent of consumers who reported scams were contacted by phone.
- The sum total of potential losses to the consumer was \$1,575,945 and the sum total of actual losses reported was \$5,983,011.
- Top three counties for scam reports: Richland (13.60%), Horry (9.14%) and Charleston (7.48%).
- Nearly 21 percent of those filing a scam report did not provide their age when filing. The largest groups of people that provided their ages were 65-74 year-olds (21.18%), 55-64 year-olds (16.18%) and 75-84 year-olds (15.58%).

IDENTITY THEFT IN SOUTH CAROLINA

Identity thieves can use your information anyway you do. Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can also file a tax return in your name and get your refund.



POTENTIAL LOSSES

\$578,738.44

This is the total amount of money reported stolen through ID theft that the consumer was able to get back or credited to their account(s).



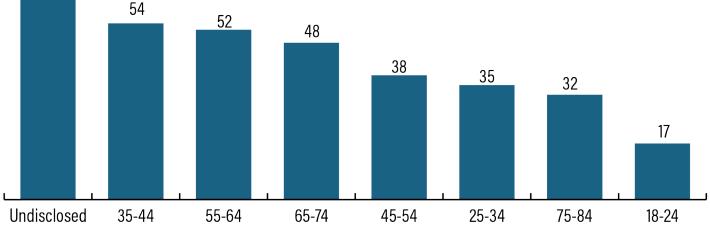
ACTUAL LOSSES

\$1,026,915.10

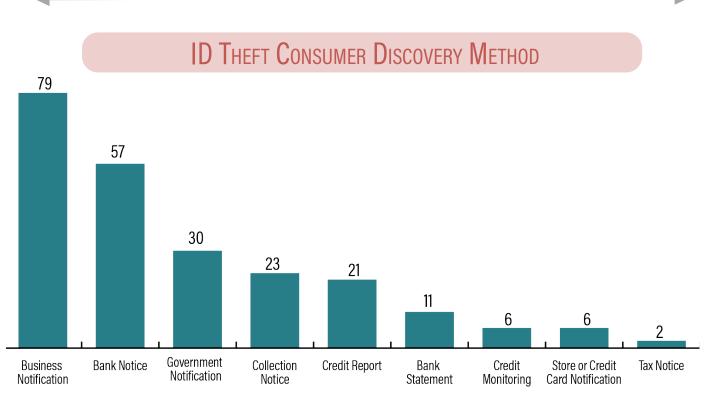
This is the total amount of money reported lost to SCDCA by consumers who were ID theft victims.

62

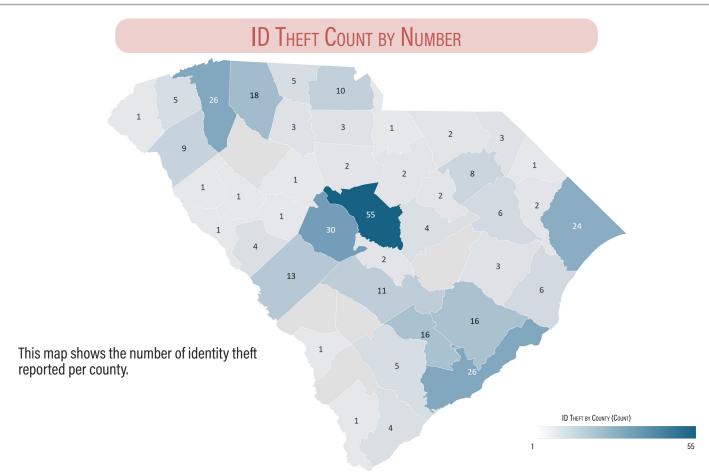
ID THEFT BY AGE RANGE

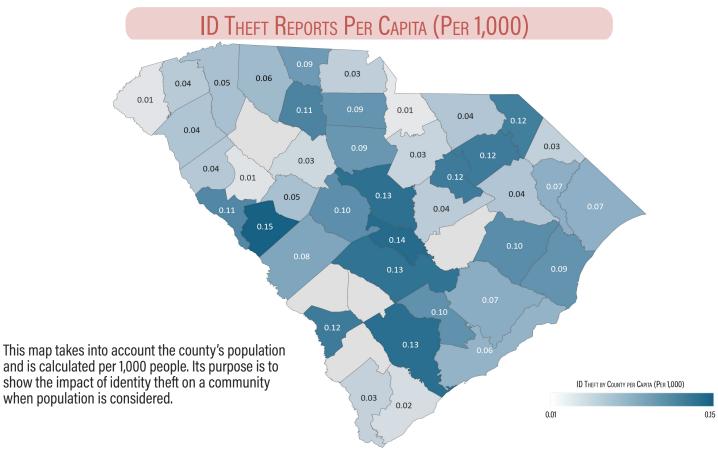


This graph shows the age ranges of consumers who reported being affected by identity theft. Undisclosed means that the consumer did not give their age when filing a report.



This graph shows the way consumers found out that they were victims of identity theft. Top three categorized discovery methods for identity theft: Business Notification (33.62%), Bank Notice (24.26%), and Government Notification (12.77%).





SCAMS IN SOUTH CAROLINA

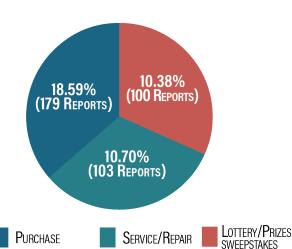
Crooks use clever schemes to defraud millions of people every year. They often combine sophisticated technology with age-old tricks to get people to send money or give out personal information. They add new twists to old schemes and pressure people to make important decisions on the spot. One thing that never changes: they follow headlines—and the money.

The charts below reflect scams reported to SCDCA in 2023.

Top Reported Scams



- Purchase
- Service/Repair
- 3 Lottery/Prizes/Sweepstakes





Purchase

Consumer directed to or approached by imposter business to trick consumer into paying for fake consumer goods. Most online purchase scams occur when a payment is made online to purchase something, and nothing is delivered.

Service/Repair

Consumer directed to or approached by imposter business to trick consumer into paying for a fake service or repair. Example: Fake credit repair companies; internet services.





Lottery/Prizes/Sweepstakes

Consumer gets call, email, mail, telling them that they have won a lottery, sweepstakes, or other prize, but needs to first pay a fee (for taxes, custom fees, etc.) to collect their winnings. Examples: Publishers Clearinghouse; foreign lottery.

POTENTIAL LOSSES

\$1,575,945.12

This is the total amount of money reported to SCDCA by consumers who did NOT fall for a scam.

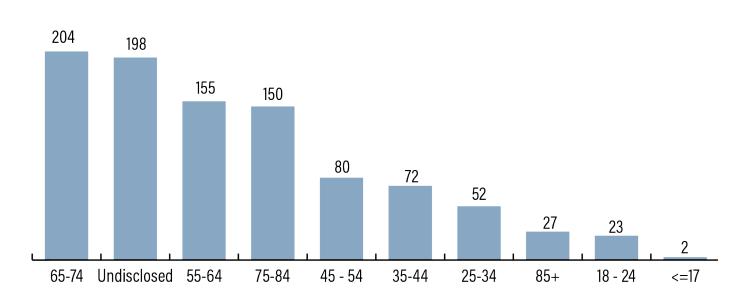


ACTUAL LOSSES

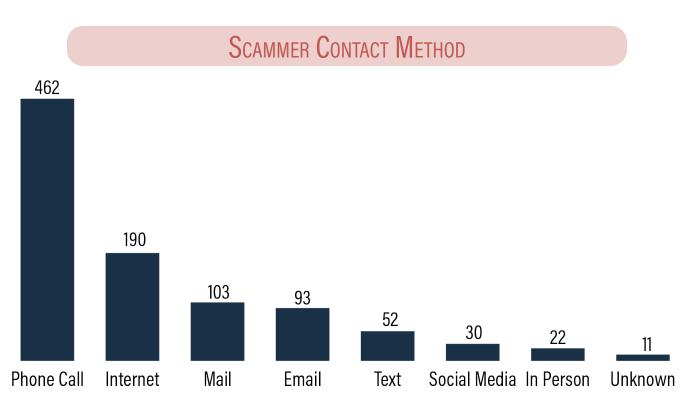
\$5,983,011,48

This is the total amount of money reported to SCDCA by consumers who DID fall for a scam.

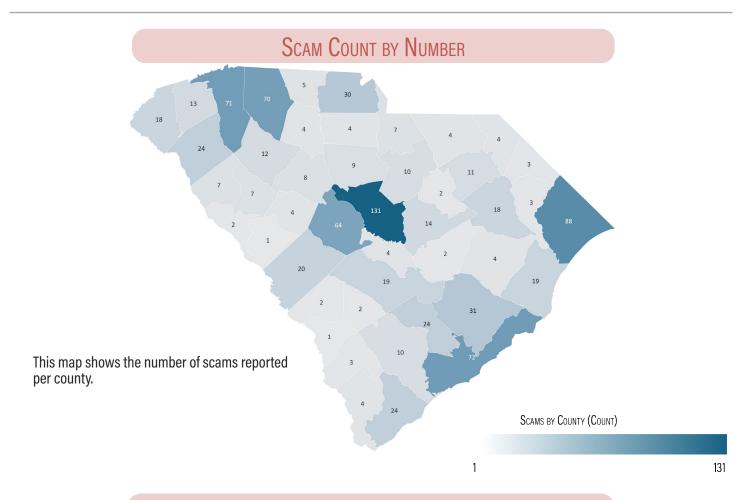
Scams by Age Range



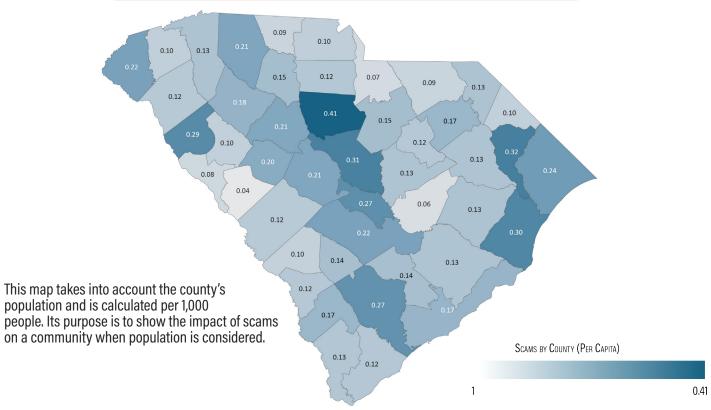
This graph shows the age ranges of consumers who reported being affected by a scam. Undisclosed means that the consumer did not give their age when filing a report.



This graph shows the way scammers contacted consumers who filed reports with SCDCA. Fifty-three percent of consumers who reported scams were contacted by phone.







ID THEFT CLUES WHAT TO WATCH OUT FOR:

IDENTITY THIEVES CAN USE YOUR INFORMATION ANYWAY YOU DO

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax return in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.

SIGNS YOU MIGHT BE A VICTIM OF IDENTIFY THEFT

Financial Accounts

- You see withdrawals from your bank account that you can't explain.
- You don't get your bills or other mail.
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar addresses, accounts or charges on your credit report

Other Benefits

- Medical providers bill you for services you didn't use.
- Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
- A health plan won't cover you because your medical records show a condition you don't have.
- The IRS notifies you that more than one tax return was filed in your name, or that you
 have income from an employer you don't work for.
- You find errors on your social security statement.

THINKING OUTSIDE THE BOX

Consider these other tools for protecting your accounts.

Many banks offer account alerts that can fit your needs:

- Get a text if your balance falls below a certain number.
- Get an email or phone call if a charge greater than \$X (i.e. \$100) hits your account.

Use two-factor authentication. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone, a fingerprint or a face scan.

WATCH OUT FOR SCAMS

Scam artists follow the headlines. Don't give your personal information to someone you don't know. Be wary of calls, emails, texts and pop-ups you did not solicit. Scammers can use information taken from a breach to make their request seem legit. When in doubt, cut-off contact. To report a scam or to get help if you gave your info to a scammer, contact SCDCA's Identity Theft Unit at (800) 922-1594 or by visiting <u>consumer.sc.gov</u> and clicking "Identity Theft Unit."





Contact SCDCA's
Identity Theft Unit
for guided identity
theft help.