DEPARTMENT OF CONSUMER AFFAIRS DEPARTMENT OF CONSUMER AFFAIRS DENTITY THEFT & SCAMS REPORT

EXECUTIVE SUMMARY

IDENTITY THEFT

- The 2023 report contains information from 359 reports of identity theft reported from January 1 to December 31, 2022.
- The top three types of identity theft were: Financial (69.36%), Government (26.74%) and Medical (1.39%).
- Twenty-nine percent of identity thefts were reported to the police.
- Top three discovery methods for identity theft: Bank Notice (27.71%), Business Notification (17.27%) and Credit Report (14.86%).
- The sum total of potential losses to the consumer was \$1,292,351 and the sum total of actual losses reported was \$587,892.
- Top three counties for identity theft: Richland (11.42%), Greenville (10.58%) and Spartanburg (8.91%).

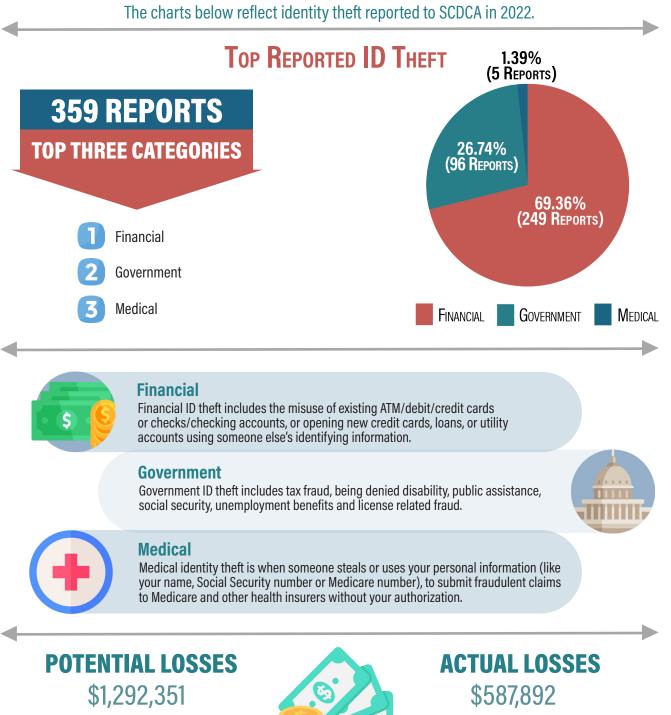
Scams

- The 2022 report contains information from 601 scams reported from January 1 to December 31, 2022.
- The top three types of scams were: Purchase (20.47%), Lottery/Prizes/Sweepstakes (12.81%) and Service/Repair (12.15%).
- Fifty percent of consumers who reported scams were contacted by phone.
- Top three scammer types: Imposter-Business (61.40%), Imposter-Government Agency (11.98%) and Imposter-Relationship (8.49%).
- The sum total of potential losses to the consumer was \$1,239,705 and the sum total of actual losses reported was \$2,433,974.
- Top three counties for scams: Richland (10.15%), Lexington (8.82%) and Horry (8.82%).



IDENTITY THEFT IN SOUTH CAROLINA

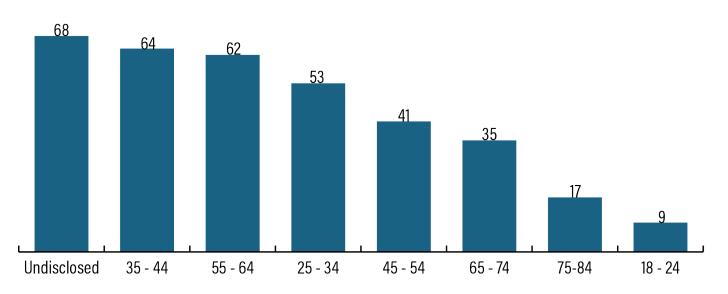
Identity thieves can use your information anyway you do. Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax return in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



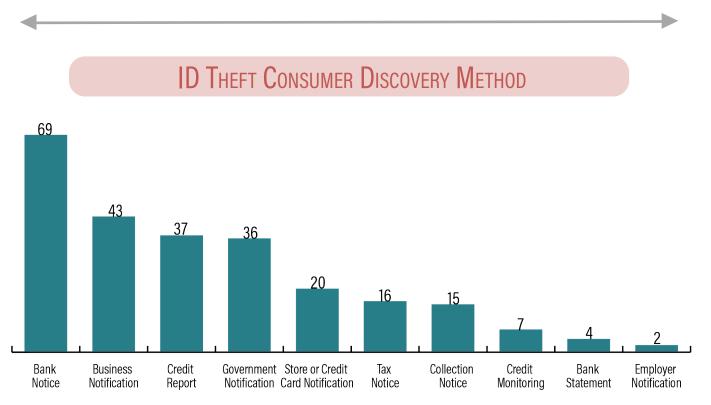
This is the total amount of money reported stolen through ID theft that the consumer was able to get back or credited to their account(s). This is the total amount of money reported lost to

SCDCA by consumers who were ID theft victims.

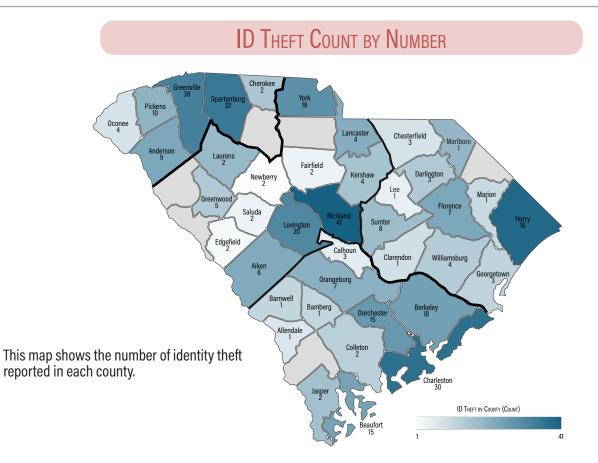


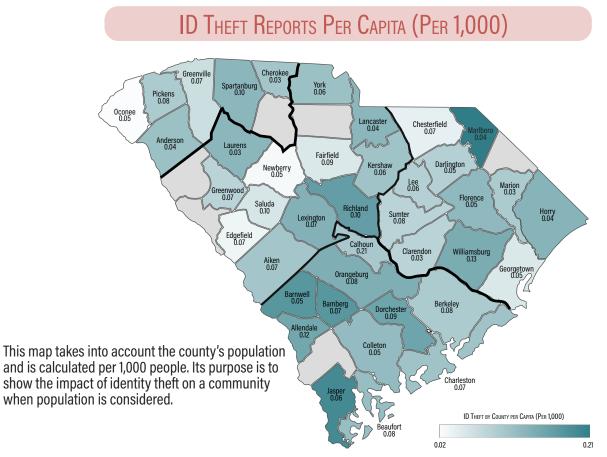


This graph shows the age ranges of consumers who reported being affected by identity theft. Undisclosed means that the consumer did not give their age when filing a report.



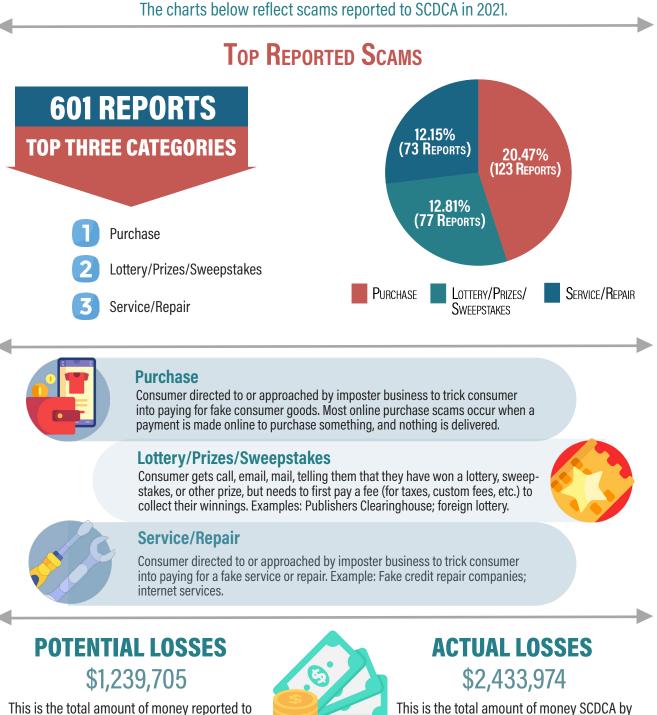
This graph shows the way consumers found out that they were victims of identity theft. Top three categorized discovery methods for identity theft: Government Notification (21.23%), Store or Credit Card Notification (19.38%), and Bank Notice (15.38%).





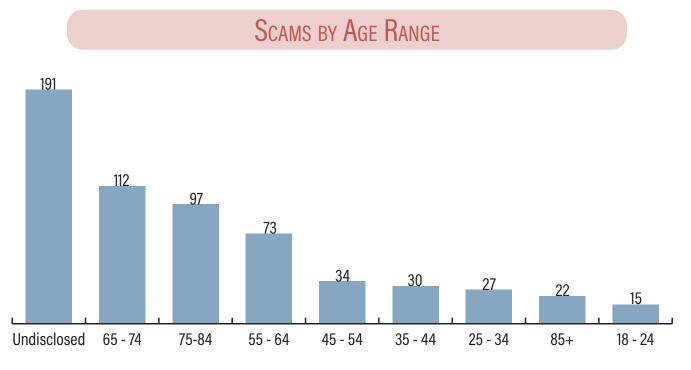
Scams in South Carolina

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.

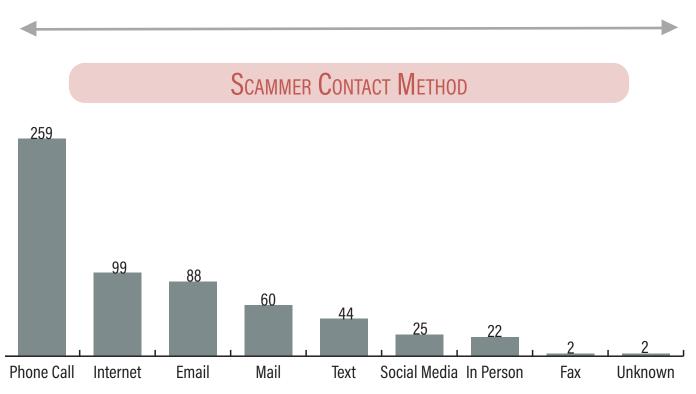


This is the total amount of money reported to SCDCA by consumers who did NOT fall for a scam.

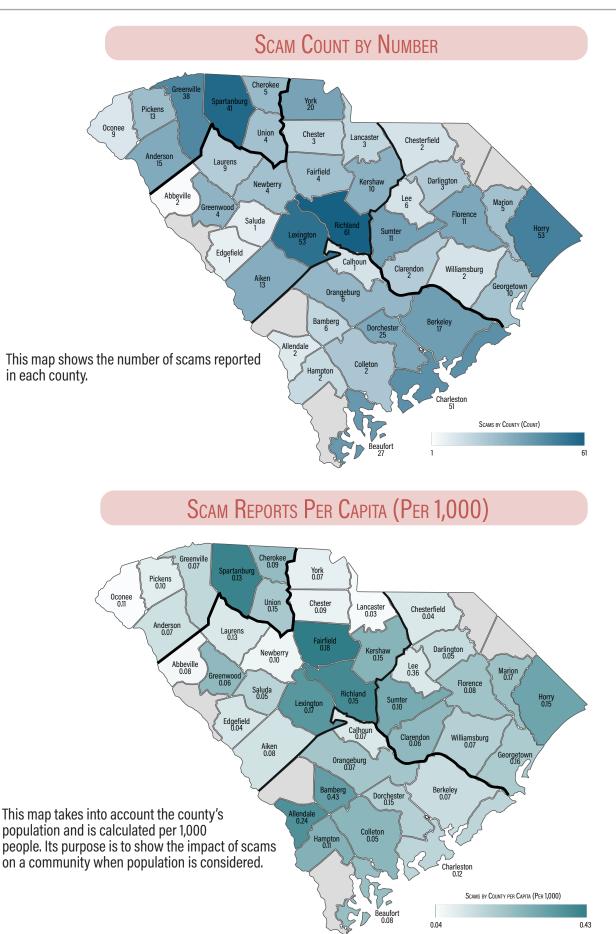
consumers who DID fall for a scam.



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-four 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.

These alerts can make watching existing accounts less of a hassle.

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."





