

Healthcare and Regulatory Subcommittee

Tuesday, September 26, 2023

Contents

AGENDA	2
MINUTES	4
AGENCY SNAPSHOT	7
AGENCY PRESENTATION	10
AGENCY SUPPLEMENTAL DOCUMENTS	151
CREDIT REPORTS: What they are and why the matter.	152
CYBER SECURITY BASICS.....	162
RECOVERING FROM A DISASTER.....	165
DITCH THE PITCH: A guide for guarding against scams.	174
HOW TO PREVENT IDENTITY THEFT.....	186
IDENTITY THEFT TOOLKIT.....	197



AGENDA



South Carolina
House of Representatives
Legislative Oversight Committee

**HEALTHCARE AND REGULATORY
SUBCOMMITTEE**

Chairman Joseph H. "Joe" Jefferson, Jr.

The Honorable April Cromer
The Honorable Roger K. Kirby
The Honorable Thomas Duval "Val" Guest, Jr.
The Honorable Marvin "Mark" Smith

AGENDA

Tuesday, September 26, 2023

10:30 a.m.

Room 110 - Blatt Building

Pursuant to Committee Rule 4.7, S.C. ETV shall be allowed access for internet streaming whenever technologically feasible.

AGENDA

- I. Approval of Minutes
- II. Discussion of the study of the Department of Consumer Affairs
- III. Adjournment



MINUTES



South Carolina House of Representatives Legislative Oversight Committee

Chair Jeffrey E. “Jeff” Johnson

William H. Bailey
Gary S. Brewer
April Cromer
Kambrell H. Garvin
Leon Douglas “Doug” Gilliam
Thomas Duval “Val” Guest, Jr.

William M. “Bill” Hixon
Joseph H. “Joe” Jefferson, Jr.
Wendell Keith Jones
Roger K. Kirby
Josiah Magnuson
John R. McCravy, III

First Vice-Chair Chris Wooten

Timothy A. “Tim” McGinnis
Adam M. Morgan
Travis A. Moore
Russell L. Ott
Marvin R. Pendarvis
Marvin “Mark” Smith

Charles L. Appleby IV
Legal Counsel

Cathy A. Greer
Administration Coordinator

Lewis Carter
Research Director

Roland Franklin
Counsel/Associate General Counsel for Litigation

Riley E. McCullough
Research Analyst

Post Office Box 11867
Columbia, South Carolina 29211
Telephone: (803) 212-6810 • Fax: (803) 212-6811
Room 228 Blatt Building

Tuesday, September 26, 2023

10:30am

Blatt Building Room 110

Archived Video Available

- I. Pursuant to House Legislative Oversight Committee Rule 6.7, South Carolina ETV was allowed access for streaming the meeting. You may access an archived video of this meeting by visiting the South Carolina General Assembly’s website (<http://www.scstatehouse.gov>) and clicking on *Committee Postings and Reports*, then under *House Standing Committees* click on *Legislative Oversight*. Then, click on *Video Archives* for a listing of archived videos for the Committee.

Attendance

- I. The Healthcare and Regulatory Subcommittee meeting was called to order by Chair Joseph H. Jefferson, Jr. on Wednesday, August 9, 2023, in Room 110 of the Blatt Building. Four subcommittee members (Chair Jefferson; Representative Marvin “Mark” Smith; Representative Roger Kirby; and Representative April Cromer) were present, and one absent (Representative Thomas Duval “Val” Guest, Jr.) for all or a portion of the meeting.

Minutes

- I. House Rule 4.5 requires standing committees to prepare and make available to the public the minutes of committee meetings, but the minutes do not have to be verbatim accounts of meetings.

Approval of Minutes

Representative Smith made a motion to approve the meeting minutes from the Thursday, July 20, 2023, meeting. A roll call vote was held, and the motion passed.

Rep. Smith's motion to approve meeting minutes.	Yea	Nay	Not Voting
Rep. Cromer	✓		
Rep. Guest			✓
Rep. Kirby	✓		
Rep. Smith	✓		
Rep. Jefferson	✓		

Discussion of the Study of the Department of Consumer Affairs

- I. Chair Jefferson states the purpose of the meeting, which is to begin the study of the South Carolina Department of Consumer Affairs (SCDCA or DCA).
- II. Sims Floyd, Executive Vice President of the South Carolina Automobile Dealers Association, provided testimony regarding the Department of Consumer Affairs' relationship with the state's automobile dealers. Mr. Floyd also discussed legislation passed by the General Assembly regarding how the automobile industry is regulated by the agency.
- III. Carrie Grube-Lybarker, Administrator/ Consumer Advocate, of the South Carolina Department of Consumer Affairs, provided an overview of the agency and addressed outstanding questions raised at the February, 23, 2023, public input meeting.

The following topics were presented during the meeting:

- Public Hearing Follow-Up: Closing Fees; Motor Clubs; and Debit Card Processing Fees
- SCDCA Overview:
 - Organizational Structure
 - Commission on Consumer Affairs members
 - Council of Advisors on Consumer Credit
 - Consumer Services Division
 - Consumer Advocacy Division
 - Identity Theft Unit
 - History of Consumer Credit
 - South Carolina Consumer Protection Code
 - Required Reports
 - Agency Statistics
 - Agency Challenges and Successes

Adjournment

- I. There being no further business, the meeting is adjourned.



AGENCY SNAPSHOT



DEPARTMENT OF CONSUMER AFFAIRS

ABOUT

The South Carolina Department of Consumer Affairs (“DCA”/”Department”) is the state’s consumer protection agency. Established in 1974, DCA has nearly fifty years of experience in protecting South Carolina consumers while recognizing those businesses that act honestly and fairly. The General Assembly has charged the DCA with administering, interpreting and enforcing over one hundred twenty statutes, including the S.C. Consumer Protection Code. Our mission is to protect consumers from inequities in the marketplace through advocacy, mediation, enforcement and education.

HISTORY



- Prior to implementation of South Carolina Consumer Protection Code (SCCPC), little protection existed for consumers in the marketplace.
- The SCCPC is Title 37 of the *Code of Laws of South Carolina*. It was adopted in 1974 and became effective January 1, 1975.
 - Major amendments were made to the SCCPC in 1976 and 1982.
 - The 1976 amendments added the Chapter on Consumer Loans.
 - The 1982 amendments deregulated interest rates in South Carolina.
 - Significant amendments were made to the Chapter on Credit Insurance in 1999.
- Other states having a version of the uniform code are:
 - Colorado, Maine, Indiana, Oklahoma, Iowa, Wisconsin, Utah, Kansas, and Wyoming.

OVERVIEW



45 State FTEs

120 statutes to administer & enforce



Total Funding by Fiscal Year



LEADERSHIP

The Commission on Consumer Affairs is the policy making and governing authority of the S.C. Department of Consumer Affairs, appoints the Administrator and is responsible for enforcement of the S.C. Consumer Protection Code.

Agency Head

- Carolyn Lybarker began her career with the agency in June 2004 as a law clerk, later becoming a Staff Attorney.
- She was named Acting Director of Public Information in July 2010 then Deputy Director of Public Information, Consumer Services and Education in October 2010.
- She served as Acting Administrator from February 2011- October 2011, when she was appointed DCA's fifth Administrator

Commission

- The Commission on Consumer Affairs is composed of nine members, one of whom is the Secretary of State
- The General Assembly elects four other members from outside the legislature
- The Governor appoints four members whose appointments are confirmed by the Senate

DIVISIONS

The Department of Consumer Affairs is organized into six divisions.

Administration

- Provides support for the other Divisions including personnel, accounting, data processing and purchasing.

Public Information and Education

- Serves as the main consumer education portal for consumers, business and the media.
- Informs consumers and businesses on their rights and responsibilities in the marketplace through traditional and alternative media distribution.

Consumer Services

- Takes and attempts to resolve consumer complaints against businesses, with due regard for the rights of the business.
- Handles complaints against industries we regulate, and those where no one else has jurisdiction.

Identity Theft Unit

- Provides education and outreach to consumers across the state to increase public awareness about what identity theft is, the steps consumers can take to protect themselves, and what consumers should do in the event of identity theft.

Advocacy

- Represents the public at large in intervening in rate cases/filings. (Includes investor-owned utilities, homeowner's insurance and worker's compensation insurance).
- Intervenes in state and federal agency rulemaking process when attempting to fix prices for consumer goods or services.

Legal

- Helps the Administrator administer and enforce applicable laws.
- Processes regulatory filings, investigates potential issues, and brings enforcement actions.



AGENCY PRESENTATION

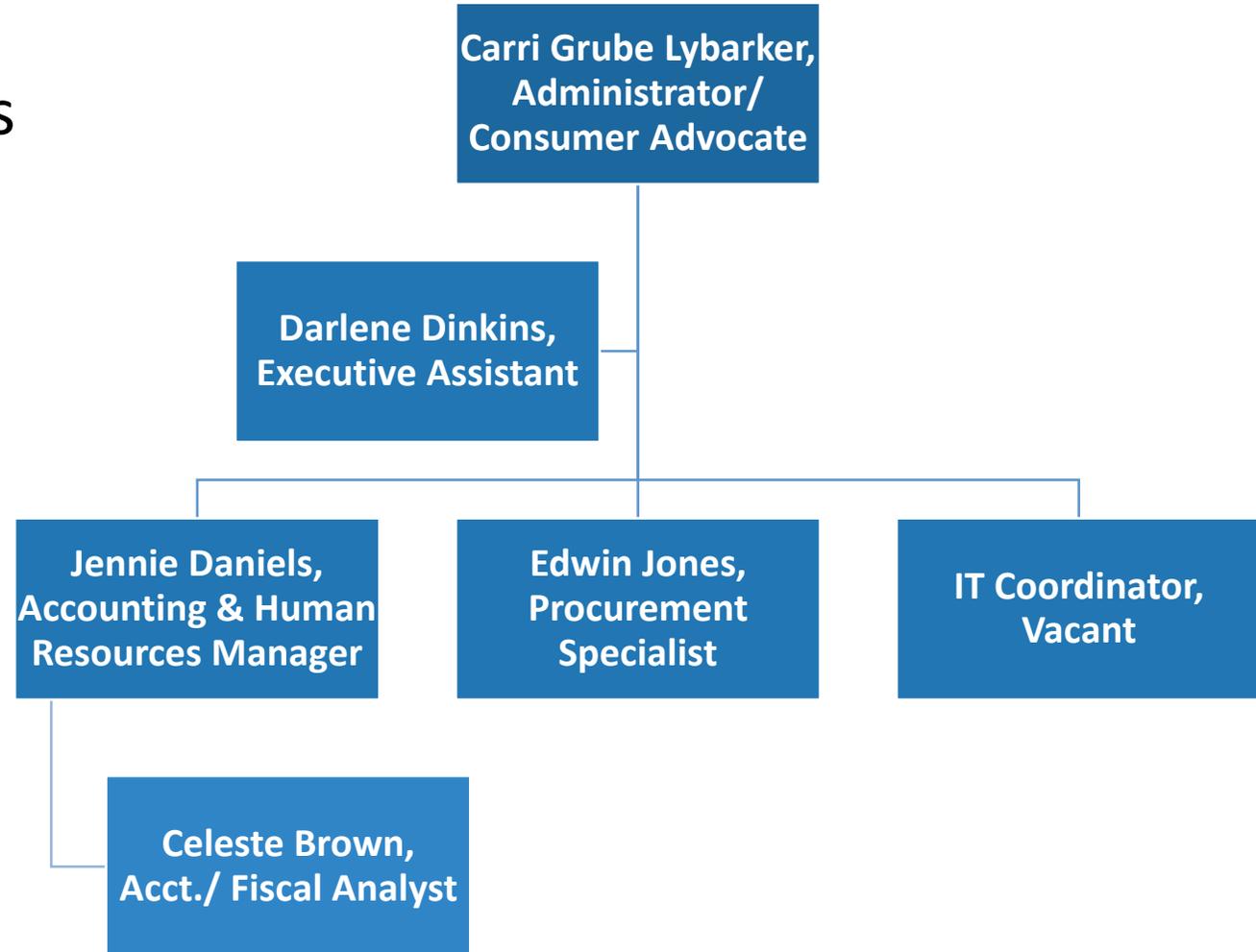


ADMINISTRATION DIVISION

Carri Grube Lybarker
Administrator/ Consumer Advocate

Administration Division

- Provides essential business services and support to DCA operations
- Includes the agency Administrator, Accounting, Procurement, Human Resources, and Information Technology



Administrator's Office: Administrator



Manage day-to-day agency operations

- Strategic Planning
- Mission Fulfillment



Provide guidance & support for each Division

- Chief Financial Officer
- Attorney
- Consumer Advocate
- Information Security Role



Issue Administrative Interpretations, Informal Opinions, etc.



Legislative Involvement

- Draft legislation and regulations
- Testify and/or provide education on issues
- Receive constituent inquiries



Engagement

- Meet with Council and Commission
- Consumer & Business Education
- Serve as agency spokesperson

Administrator's Office: Executive Assistant



Handles constituent inquiries from public officials



Processes procurements related to travel and trainings



Supports Administrator

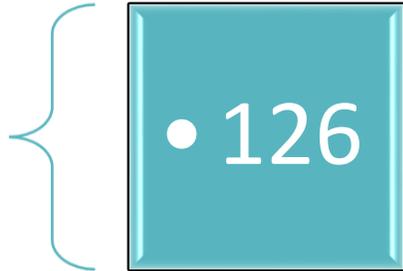


Legislative tracking

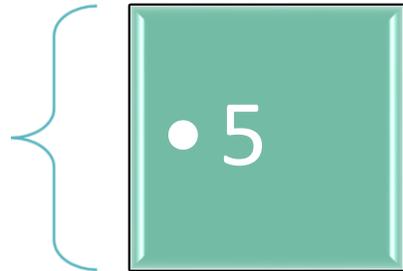
Interpretations & Rulings (131)



**ADMINISTRATIVE
INTERPRETATIONS**



**DECLARATORY
RULINGS**



[Home](#) » [Business Resources/Laws](#) » Administrative Interpretations

Administrative Interpretations

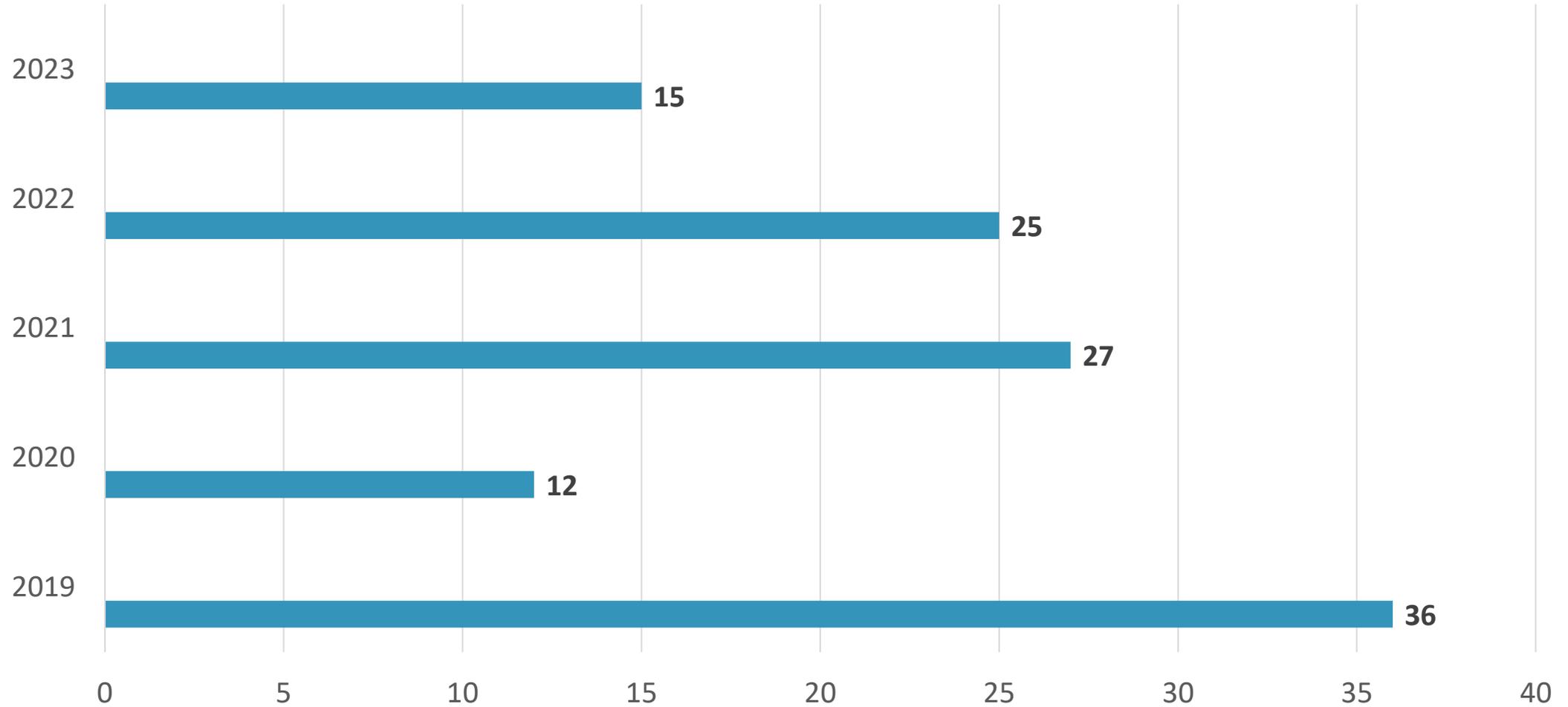
The Administrative Interpretations section of the South Carolina Department of Consumer Affairs Website includes clarifications and explanations of the South Carolina Consumer Protection Code ("the Code"). The interpretations allow for a more detailed look at how the Code applies in specific circumstances, and clarifies terms and concepts used in the Code. To find information regarding a specific chapter of the Code, select the chapter from the list below and you will be directed to a page containing those specific Administrative Interpretations. The naming convention for the Administrative Interpretations can be best understood as chapter, subsection, year issued and interpretation number for that year. A good example is: An interpretation named 3.201-8402 would be in relation to § 37-3-201 and was the second Administrative Interpretation issued in 1984.

You will also find a short summary of what topic the Administrative Interpretation relates to. For situations in which an interpretation was issued and then was further asked to be reconsidered, you will find both the initial Administrative Interpretation as well as the reconsidered Administrative Interpretation listed for completeness.

- ▼ Title 1 - Administration of the Government
- ▼ Title 34 - Banking, Financial Institutions and Money
- ▼ Title 37 - SC Consumer Protection Code



LEGISLATIVE ACTIVITIES BY FISCAL YEAR



Human Resources



Human Resources Activities

- Recruitment
- Retention
- Succession Planning



1 FTE

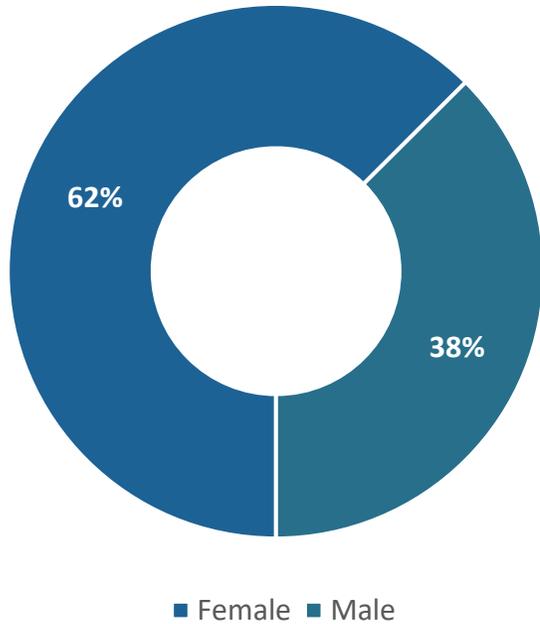


Recent Successes

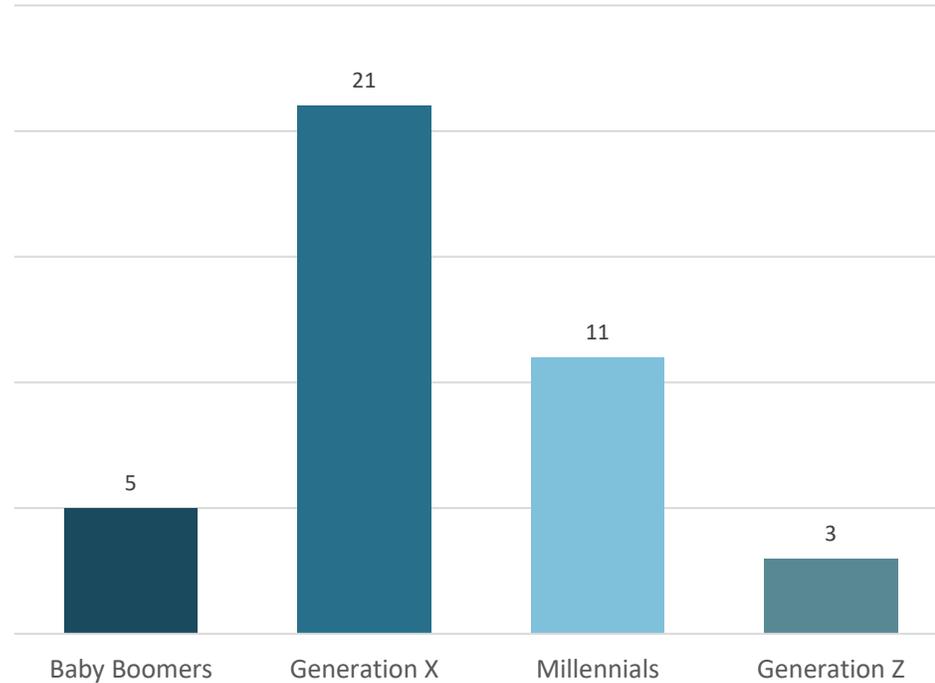
- Great annual audit results
- Agency policies and procedures updates

SCDCA Employee Demographics

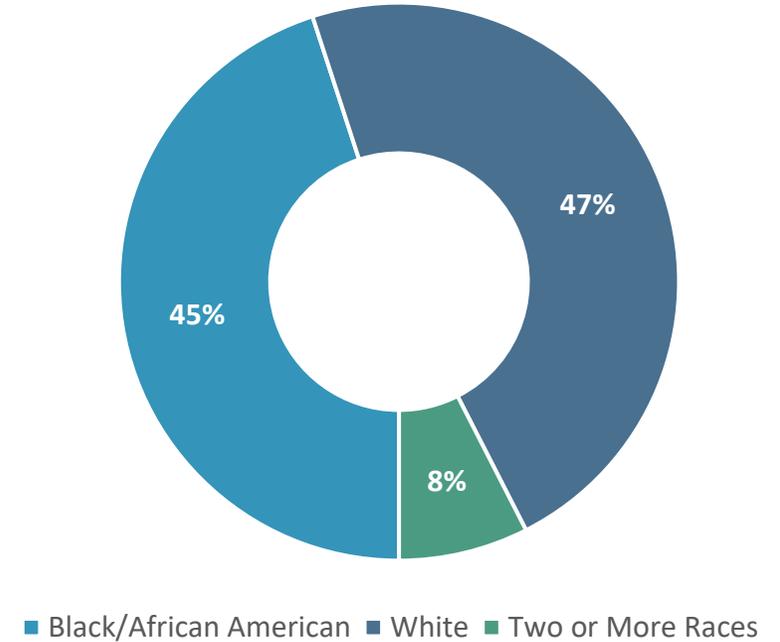
SCDCA Gender Demographics



SCDCA Generational Demographics



SCDCA Ethnicity Demographics



Employee Internal Trainings

Information Security

Agency Policies

Cross-Training

LinkedIn

Civilian Active Shooter

Empathy and Empathy Fatigue

EPMS (one for all staff & one for supervisors only)

Dealing with difficult people/ conflict resolution

EEO Training

Customer Service

Presentation Skills

Supervisory Practices

Email and telephone etiquette in workplace

Employee External Trainings

National Assoc. of Consumer Credit Administrators (NACCA) Examiners' School

Water Utility Policy (NASUCA)

New Mexico State and Michigan State University utility ratemaking courses

Financial Statement Analysis (AARMR)

Leadership Development (AARMR)

Associate Public Manager Program (Admin)

Certified Public Manager Program (Admin)

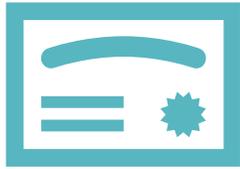
SC Association of Counties CLE

Various SC Attorney General CLEs: Mental Health, SCDEW

Office of Human Resources HR Updates

Equal Employment Opportunity (Human Affairs Commission)

Employee Certifications & Memberships



20+ Professional Certifications

- Certified Public Manager (2)
- SC Associate Public Manager (5)
- Certified Information Privacy Professional/ Manager (4)
- Certified Mortgage Examiner (1)
- Paralegal Certification (1)



20+ Committees Served

- SC Bar Consumer Law Council
- State Coordinating Committee, Conference of State Bank Supervisors
- NACCA Auto Finance Committee
- State Grievance Committee
- Examiner-in-Charge/ Single Point of Contact for coordinated or multistate exams
- SC International Personnel Management Association (SCIPMA) Conference Planning Committee



25+ Professional Organization Memberships

- American Conf. of Uniform Consumer Credit Code States
- National Assoc. of Consumer Credit Admin. (NACCA)
- National Association of State Utility Consumer Advocates
- International Association of Lemon Law Administrators
- Consumer Federation of America
- Government Financial Services Assoc. of SC

Team DCA: Communication, Morale & Teambuilding



2 Full Staff Meetings
per Month

- Progress Reports
- Special



Monthly Deputies/ Directors
Meeting



The Week Ahead



Retreats

- Agency
- Deps/Directors

Team DCA: Communication, Morale & Teambuilding



Employee Appreciation



Wellness Wednesdays

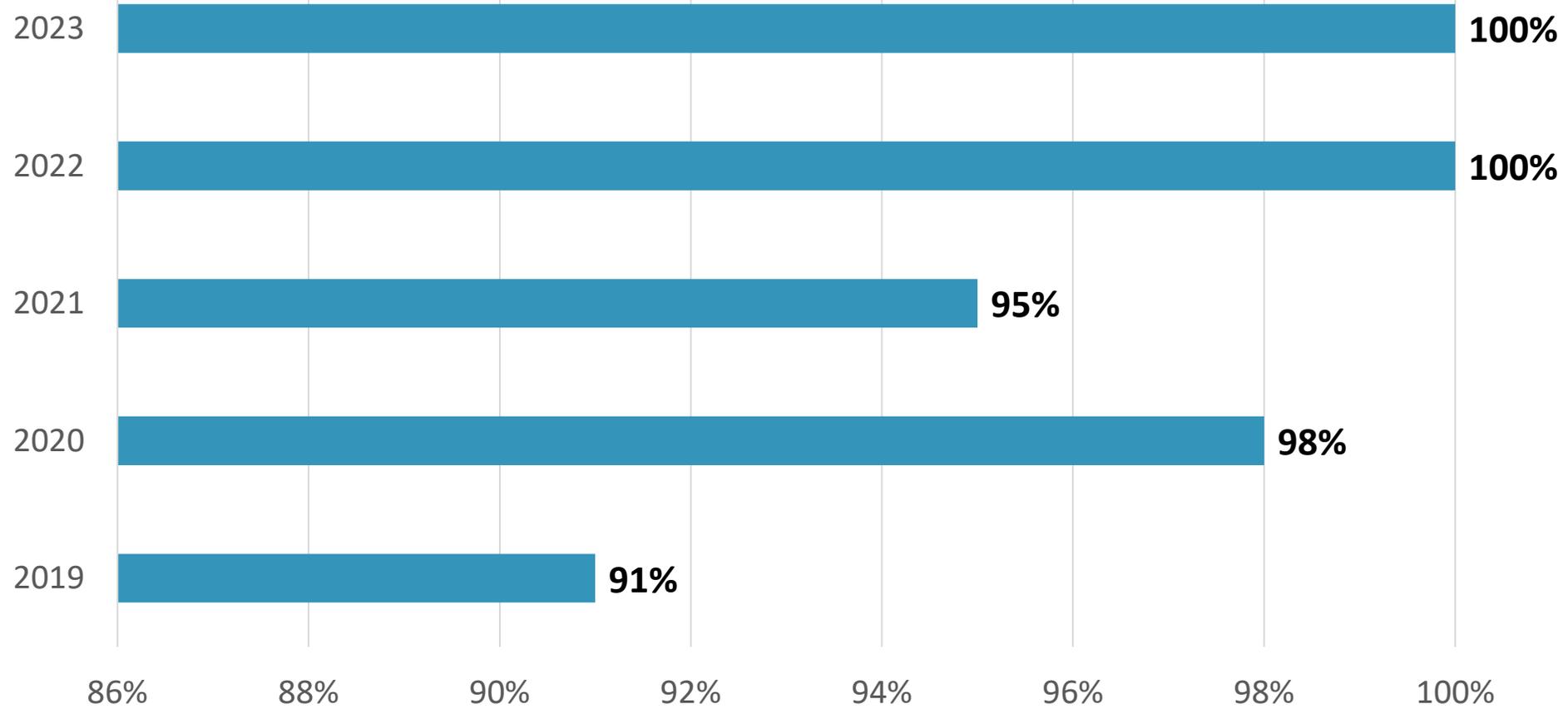


Celebrations/ Fellowship

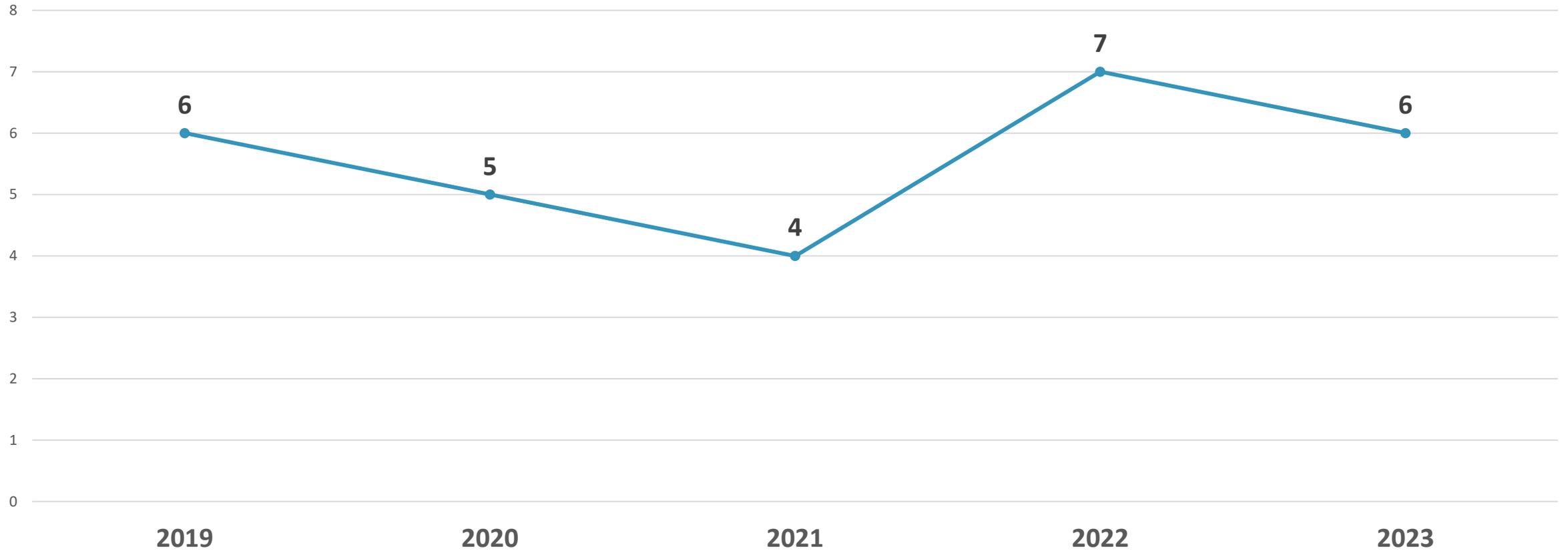


Giving Back

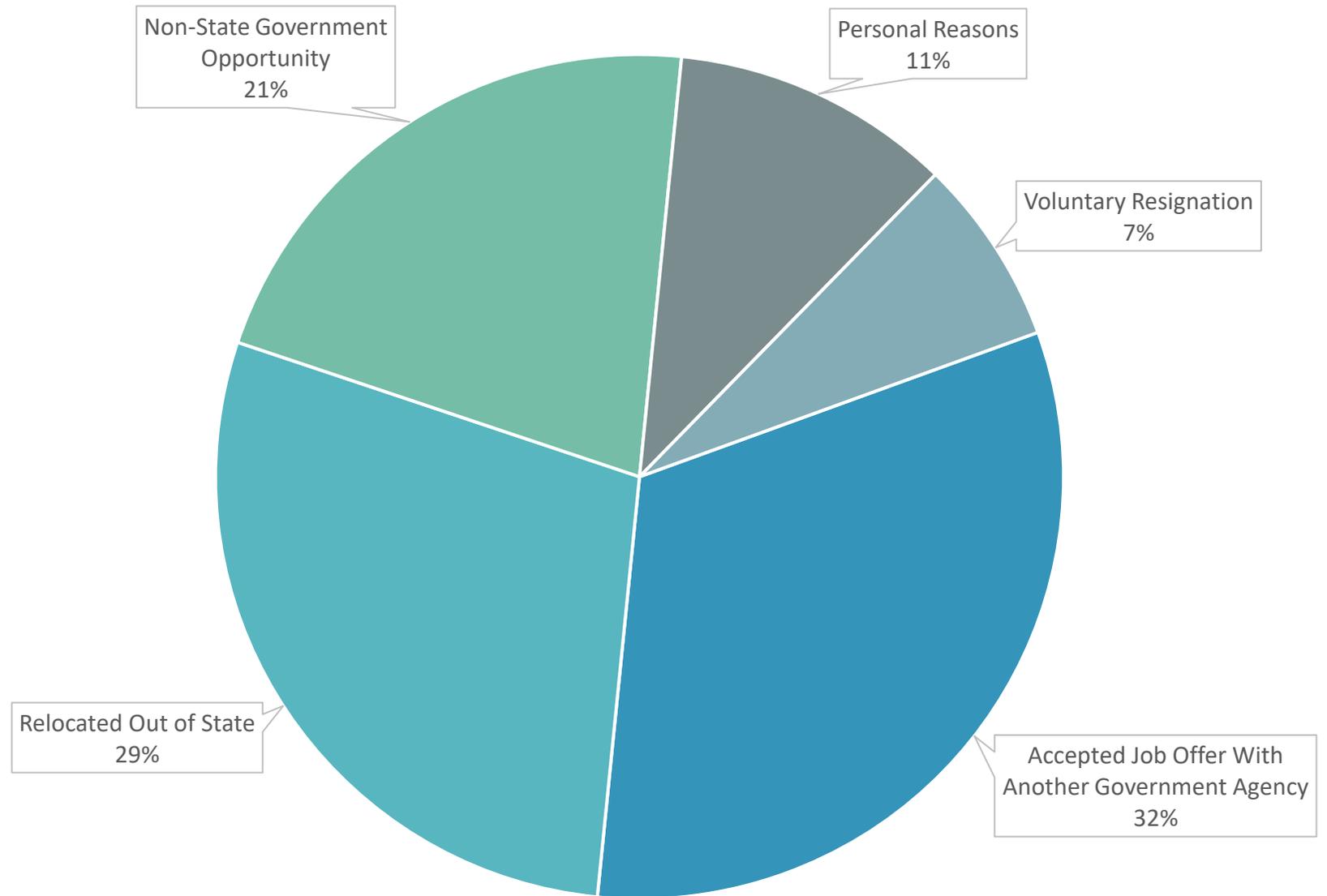
Employee Satisfaction per Fiscal Year



Employee Turnover FY19-FY23



Reasons Employees Left SCDCA FY19-FY23



Hiring Strategies

Skills Focus

- Soft skills plus ability & desire to learn
- Skills fill current gaps?

Clear Job Descriptions

- Comprehensive job descriptions with clearly define required qualifications, skills, and experience & who we are at DCA

Structured Interviews

- Utilize Interview Teams
- Standardized questions for all candidates

Offer Competitive Compensation when possible

- Research and offer competitive salary

Candidate Experience

- Prioritize a positive candidate experience from application to offer

Accounting



Comprised of 1 FTE employee



Helps prepare & manage DCA's budget

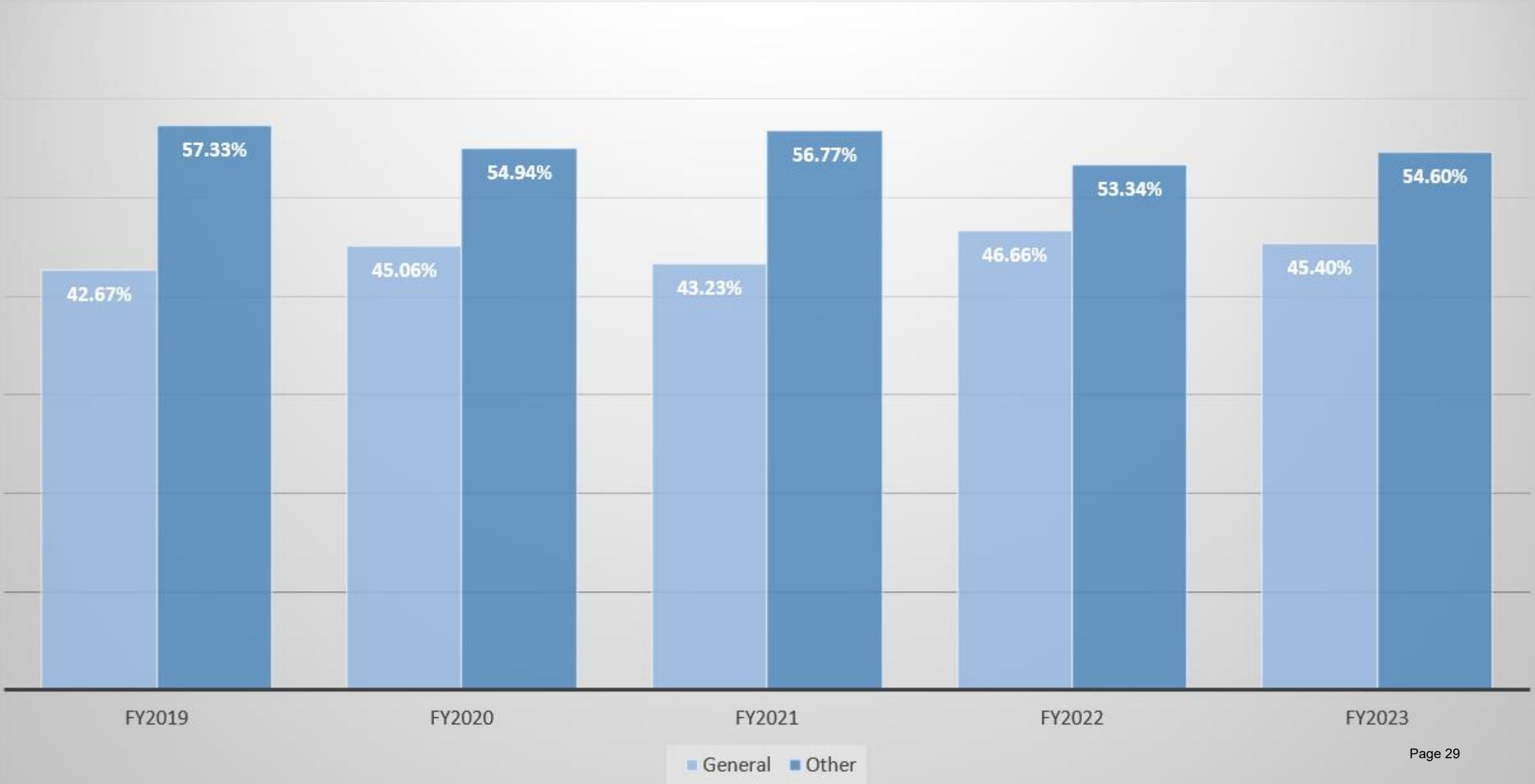


Processes all accounts payable and receivable transactions

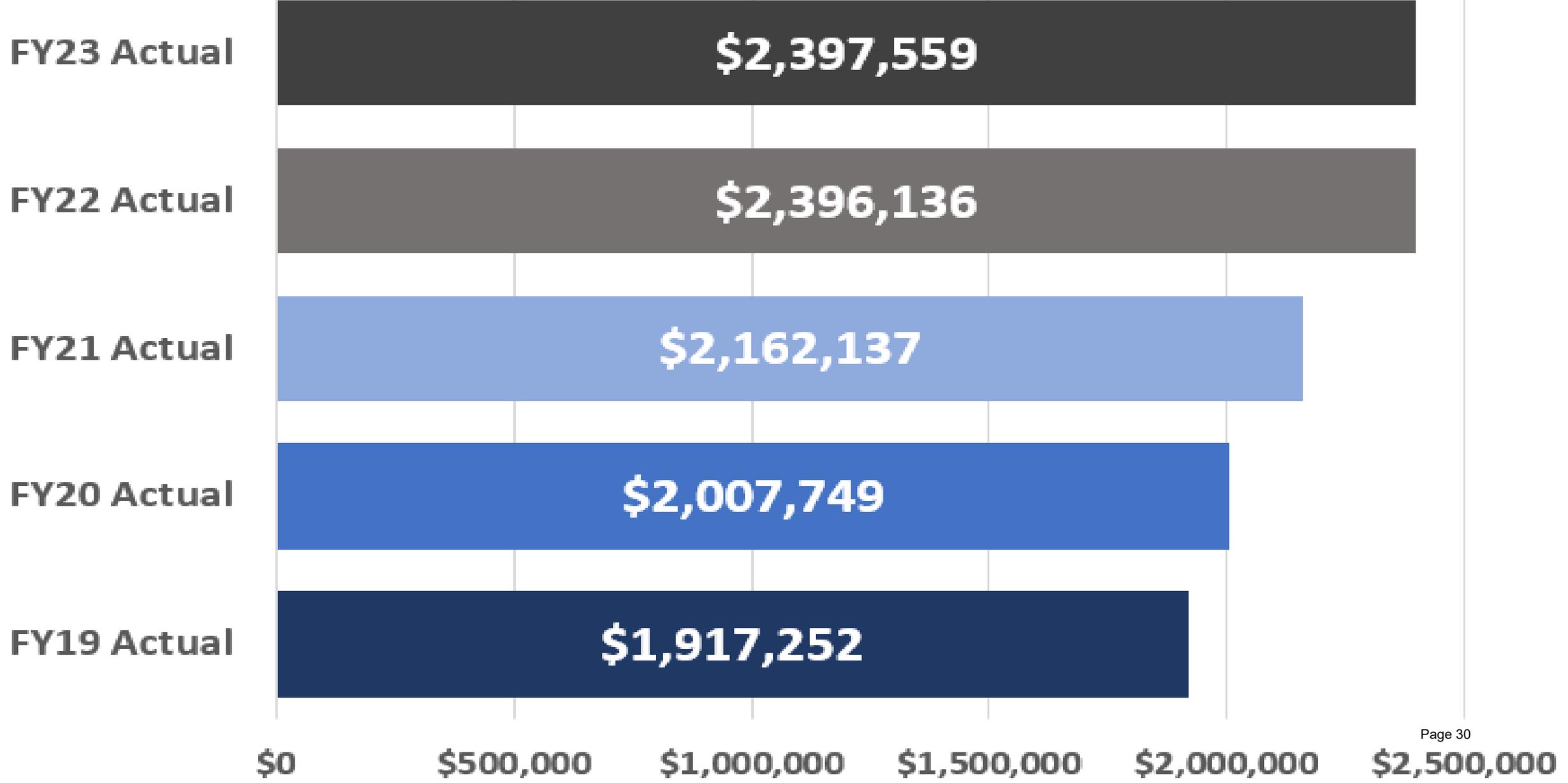


Prepares various financial reports

Source Funding Percentage



Total Revenue Processed by Fiscal Year

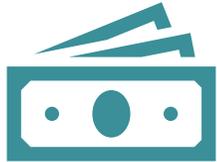


Accounting Success: Stellar State Audits



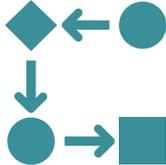
FY19 - 23 Results

2 years = no findings
3 years = 1 issue identified



Technology Contributors

Desktop Deposit
DCA Online Licensing System



Other Contributors

Seasoned Accountant/ Fiscal Analyst,
Licensing Supervisor & License
Examiners
Revenue processing in 1 Department

Procurement



Comprised of 1 FTE employee



Handles purchasing for the Department— including goods and service—according to the S.C. Procurement Code and Regulations



Mail coordinator



Building Issues/ Maintenance

Procurement Audit & Risk Mitigation



P-Card Purchases

- No P-Card purchase transactions without Administrator or Division Director approval
- P-Card transactions are reconciled monthly by the cardholders and reviewed by the Administrator



Purchase Orders

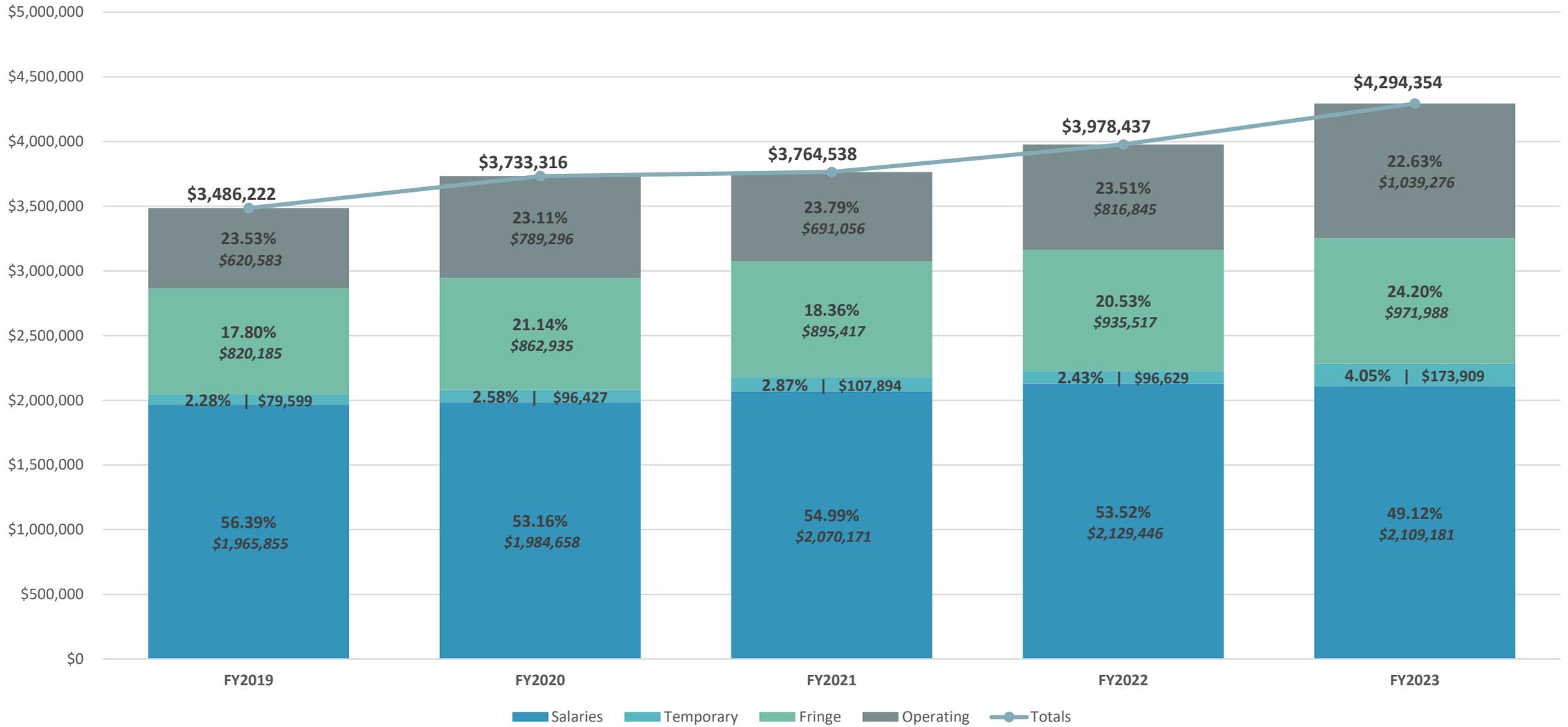
Items \$2,500+. All purchase orders reviewed and approved by the Administrator at the shopping cart level



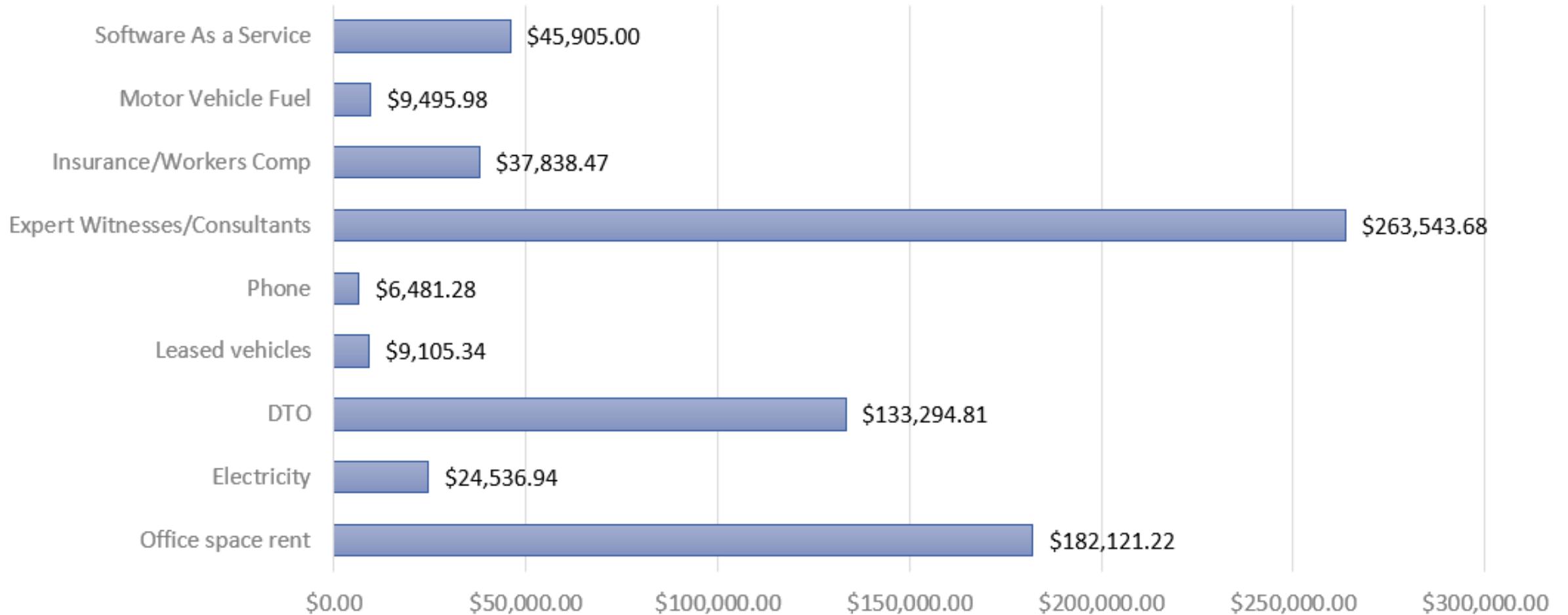
Invoices

All payable documents are processed by accounting workflow and require proper approvals

Agency Expenditures by Fiscal Year



FY23 Fixed Costs



Procurement Success: Vehicle Savings



Initial Vehicle Purchase

4 in February 2017 (\$100,620)
1 in September 2018 (\$25,063)



Cost Comparison thru FY23

Cost if vehicles leased: \$247,830
Purchased vehicles costs: \$192,144



Estimated Savings

Leased vs. Purchased= \$55,687
FY23 alone: \$31,656

Information Technology

DTO administered computers/host systems since 2015

Technology Systems

- Online Complaint System (SC.GOV)
- Online Licensing System
- Online Preamble Contract System (in development)
- Agency Website (SC.GOV)
- App Engine Forms (3/3)

In-House IT Items

Complaint Portal - 2014

01

Expedite the complaint process through online submissions

02

Submit comments to assigned DCA complaint analysts

03

Monitor the status of a complaint with 24/7 system access

04

Search complaints

05

Cost savings:
copier, supply and postage

Consumer Adoption:
FY15 @60%



Complaint Processing Times:
FY15 @32 days



Pre-complaint system processing:
45-55 days

Online Payment Processing - 2017

Expedite license/ filing processing

- *Businesses enter marketplace/ consumer choice*

Reduced human error in processing payments

Compliance with timeliness of deposits

User Adoption:
FY18 @63%

Filing Processing Times:

FY18 @ 87%
within 30 days

Information Technology

DTO administered computers/host systems since 2015

Technology Systems

- Online Complaint System (SC.GOV)
- Online Licensing System
- Online Pneed Contract System (in development)
- Agency Website (SC.GOV)
- App Engine Forms (3/3)

In-House IT Items

- Created databases to track HOA Complaints, Security Breaches and internal IT helpdesk tickets
- Revised existing databases to increase automation and reporting capabilities

QUESTIONS?





Public Information & Education Division

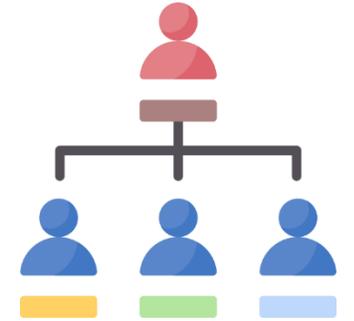
Bailey Parker
Communications Director

Public Information & Education Division



- Education is a central part of DCA's mission.
- Cultivate a marketplace comprised of well-informed consumers and businesses.
- Serve as the main consumer education portal for consumers, business and the media.
- Informs consumers and businesses on their rights and responsibilities in the marketplace.

Public Information Division Organization



Employees:

- Bailey Parker – Communications & Public Information Director
 - Hired in 2018.
- Scott Cooke – Social Media & Web Strategist
 - Hired in 2021.
- Icess Booker – Public Information Coordinator
 - Hired in 2022.

Main Education Tools



Press Releases



Traditional Media

- TV
- Newspaper
- Radio



Reports



Publications

- Written
- Video



Social Media



Website



Presentations

- In person
- Webinars

Press Releases



NEWS FROM SCDCA

SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS
Carri Grube Lybarker, Administrator

FOR IMMEDIATE RELEASE
January 30, 2023 | Release #23-01
Contact: Bailey Parker, (803) 734-4296

Tax Scammers are Waiting Around the Corner

COLUMBIA, S.C. – Scammers are waiting for that January 31, 2023 W-2 deadline to pass so they can start making their rounds. The South Carolina Department of Consumer Affairs (SCDCA) urges consumers to be on guard against tax-time identity theft. 37 SC consumers reported being victims of some type of tax ID theft in 2022, 33 specifically reported that someone had already used their Social Security number to file. This is the most common form of tax fraud; the tips below will help consumers protect their refund and personal information this tax season:

- **File early.** File as early as possible. [The IRS and the SCDOR are now accepting 2022 Individual Income Tax Returns.](#) Identity thieves use consumer information to file fraudulent tax returns and steal refunds before the individual files.
- **Watch out for IRS and tax imposter scams.** Fraudsters often pose as the IRS or even as SCDOR to trick you into disclosing personal information or sending money. Remember: the IRS *will not* call about taxes without sending a notice through the mail first. Report IRS imposter scams to the [Treasury Department](#). For more on how to avoid tax scams, visit [SCDCA's tax scams spotlight](#).
- **File online in safety.** When filing online, use anti-virus software and ensure the computer is connected to a secure internet connection. Use strong and unique passwords and enable multi-factor authentication whenever possible. Do not use public Wi-Fi. There are several websites that allow certain taxpayers to prepare and file their taxes for free, such as the [IRS Free File program](#) and the [options from the SCDOR](#).
- **Get an Identity Protection PIN.** Taxpayers who can verify their identities may opt into the IRS IP PIN program, a free added layer of protection. The ID Protection PIN is a six-digit code known only to the individual and the IRS. Use the [Get an Identity Protection PIN](#) tool to immediately get an IP PIN. Never share the IP PIN with anyone but a trusted tax provider.
- **Use a legitimate tax preparer.** Consumers should make sure their preparer is reputable, licensed and has a [Preparer Tax Identification Number](#) from the IRS. Visit [www.irs.gov](#) or call (800) 906-9887 to see if you qualify for free tax prep services provided by IRS-certified volunteers. For more tips on how to choose a tax professional, [click here](#).

For more information on tax fraud and scams, visit SCDCA's [Scam page](#). Consumers who believe they are the victim of a security breach, scam or identity theft are encouraged to seek



NEWS FROM SCDCA

SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS
Carri Grube Lybarker, Administrator

FOR IMMEDIATE RELEASE
February 2, 2023 | Release #23-02
Contact: Bailey Parker, (803) 734-4296

2023 Homeowners Association Complaint Report Released

COLUMBIA, S.C. – The South Carolina Department of Consumer Affairs (SCDCA) is releasing the fourth Homeowners Association (HOA) Complaint Report. The [2023 Report](#) is a compilation of data from complaints received January 1, 2022, through December 31, 2022. Some of the highlights include:

- SCDCA received 276 HOA complaints filed against 208 HOA/Management Companies. The number of complaints filed in 2022 is a 7% increase compared to 2021.
- Top Three Counties for Complaints: Horry (25.4%), Richland (12.3%) and Greenville (10.9%).
- The complaints raised 651 concerns, with multiple included in a single complaint. The top three types of issues raised were: Failure to adhere to and/or enforce covenants and bylaws (15.1%), concerns regarding maintenance and repairs (12.4%) and failure to notify residents of board actions (11.5%).
- Less than 6% of complaints were closed as "Unsatisfied" due to a business's failure to respond.

SCDCA will offer a free webinar "2023 HOA Complaint Report" on Wednesday, February 22 at 10:30 a.m. The webinar will go over the complaint report, the types of complaints received, complaint trends and the department's role in collecting complaint data. [Register here](#) to watch/listen from any computer or smart phone.

Changes to state law in 2018 require SCDCA to collect certain data from complaints involving homeowners' associations and report it annually. The report is presented in a categorized, filterable and searchable format and can be viewed in its entirety by visiting [consumer.sc.gov](#) and clicking on News, then Reports.

SCDCA processes and mediates consumer complaints against businesses regulated by DCA, refers complaints that fall within another agency's jurisdiction, and mediates those complaints against businesses that are unregulated. To file a complaint, visit our website and click "How Do I..." then the "File a Complaint?" option.

About SCDCA

The South Carolina Department of Consumer Affairs aims to protect consumers from inequities in the marketplace through advocacy, complaint mediation, enforcement and education. To file a complaint or get information on consumer issues, visit [consumer.sc.gov](#) or call toll-free, 1 (800) 922-1594.



NEWS FROM SCDCA

SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS
Carri Grube Lybarker, Administrator

FOR IMMEDIATE RELEASE
May 15, 2023 | Release #23-06
Contact: Bailey Parker, (803) 734-4296

Scammers are Acting like SCDCA to Get Your Info

COLUMBIA, S.C. – A key red flag of a scam is when someone pretends to be from a well-known organization such as federal or state agencies, law enforcement or businesses. The South Carolina Department of Consumer Affairs (SCDCA) is no exception to this rule. We recently learned that scammers are posing as SCDCA staff to trick consumers into handing over their information.

The two consumers who reported the calls say the individuals claiming to be SCDCA said they were calling about the consumers' recent solar panel purchases. One consumer said the caller claimed SCDCA was gathering personal information for a report on pricing comparison. In follow-up calls from the scammers, they acted as if they had complaints about the consumer's current solar panel company.

Remember, SCDCA will never call you out-of-the-blue and ask you for your personal identifying or financial information. If you have any questions about whether an individual who is calling you is from SCDCA, **hang up and call (803) 734-4200. If you have received a phone call like this from someone claiming to be SCDCA, please report it to us by calling call (803) 734-4200.**

Download [Ditch the Pitch](#), SCDCA's guide to guarding against scams for more information on how to spot a scam. Follow SCDCA on [Facebook](#) and [Twitter](#) to receive the latest scam updates and tips on how to keep your information safe.

About SCDCA

The South Carolina Department of Consumer Affairs aims to protect consumers from inequities in the marketplace through advocacy, complaint mediation, ~~enforcement~~ and education. To file a complaint or get information on consumer issues, visit [consumer.sc.gov](#) or call toll-free, 1 (800) 922-1594.

###

Press Releases

How we decide if we need to send out a press release:

Is there an increase in a certain type of scam report?

Is there a specific consumer topic that keeps coming up in calls, emails, presentations?

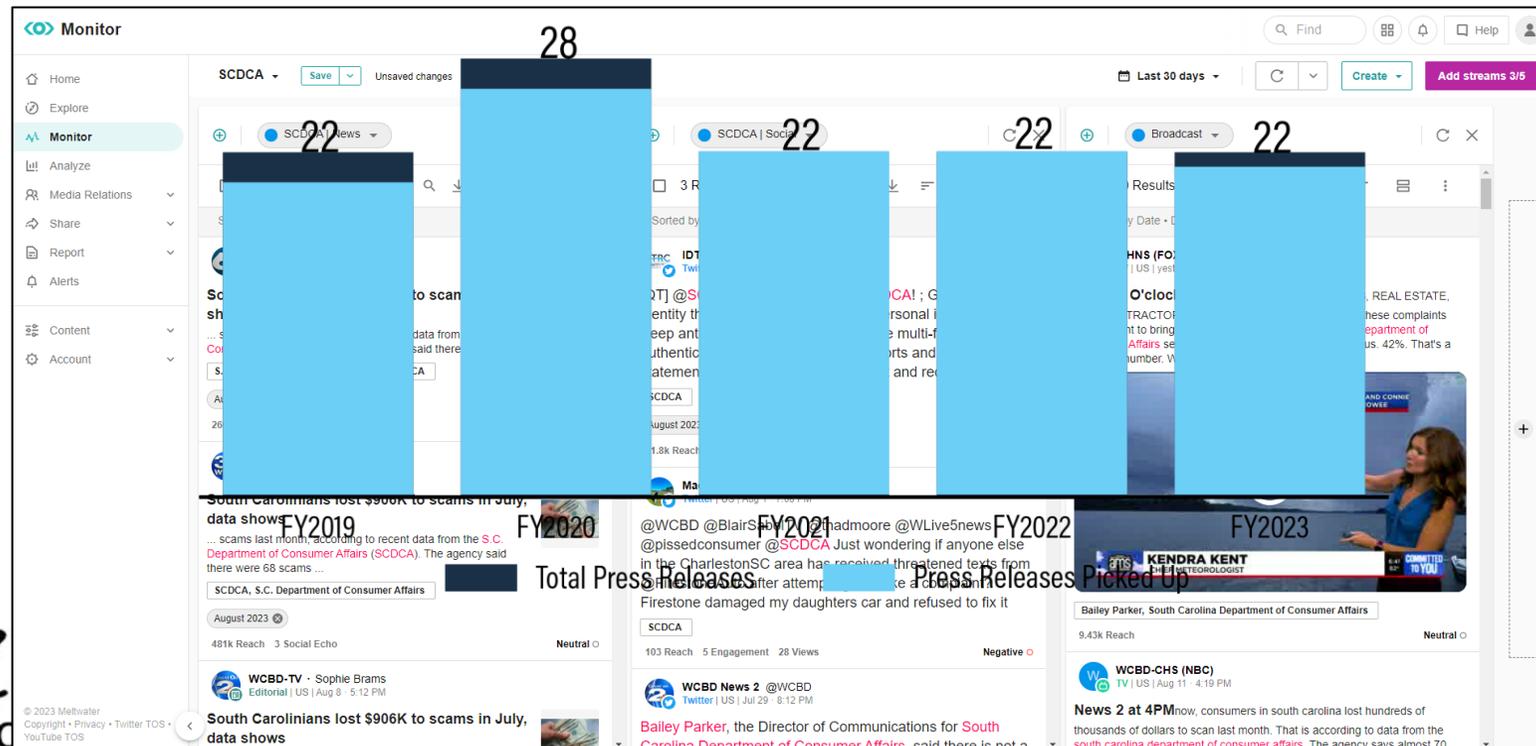
Is there an event coming up that needs to be announced?

Is there a timely topic that needs to be addressed?

Is a report being released?

Traditional Media

- Send all press releases to media outlets across SC, including border outlets like Savannah, GA, Charlotte, NC and Augusta, GA.
- Use Meltwater to track if our content is picked up.



Reports

SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS

SCAMS IN SC | 07/01/23 - 07/31/23

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 from 07/01/23 to 07/31/23

68 REPORTS

TOP THREE CATEGORIES

1. Purchase
2. Lottery/Prizes/ Sweepstakes
3. Service/Repair

Top Reported Scams in South Carolina

Category	Percentage
Purchase	29%
Lottery/Prizes/Sweepstakes	14%
Debt Collection	11%
Service/Repair	11%
Crime/Warrent	9%
Dating	3%
Subscription/Tech	4%

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.

Lottery/Prizes/ Sweepstakes
Consumers are contacted, 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.

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

POTENTIAL LOSSES

\$92,447.94

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

ACTUAL LOSSES

\$906,328.29

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

SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS
293 Graystone Boulevard, Suite 400 | Columbia, SC 29220 | 844-835-5322 | www.consumer.sc.gov

DITCH THE PITCH

2023

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

STATE OF CREDIT REPORT

ADMINISTRATOR: CARRI GRUBE LYBARKER
PO BOX 5757 • COLUMBIA, SC 29250
(800) 922-1594 • WWW.CONSUMER.SC.GOV

2023

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

HOME OWNER ASSOCIATION FIVE YEAR REPORT

HOA ACT HISTORY

The South Carolina "Homeowners Association Act" (S.C. Code Ann. § 27-30-340) became law in May 2018. It applies to communities and horizontal property regimes requiring homeowners to pay assessments. The law requires governing documents to be filed, provides certain meeting notice requirements and access to budget and membership lists, and requires the Department of Consumer Affairs (DCA) to collect specific data from complaints involving homeowners associations (HOA). Our complaint process is one of voluntary mediation. We cannot force a HOA or homeowner to participate in the complaint process, require a specific outcome or attempt to arbitrate the dispute. The information collected, however, must be reported to the Governor, General Assembly and the public by January 31st each year.

The Department issued the first annual report on January 31, 2019 containing information compiled from complaints received June 1, 2018 - December 31, 2018. Every report issued thereafter contains data from the prior calendar year.

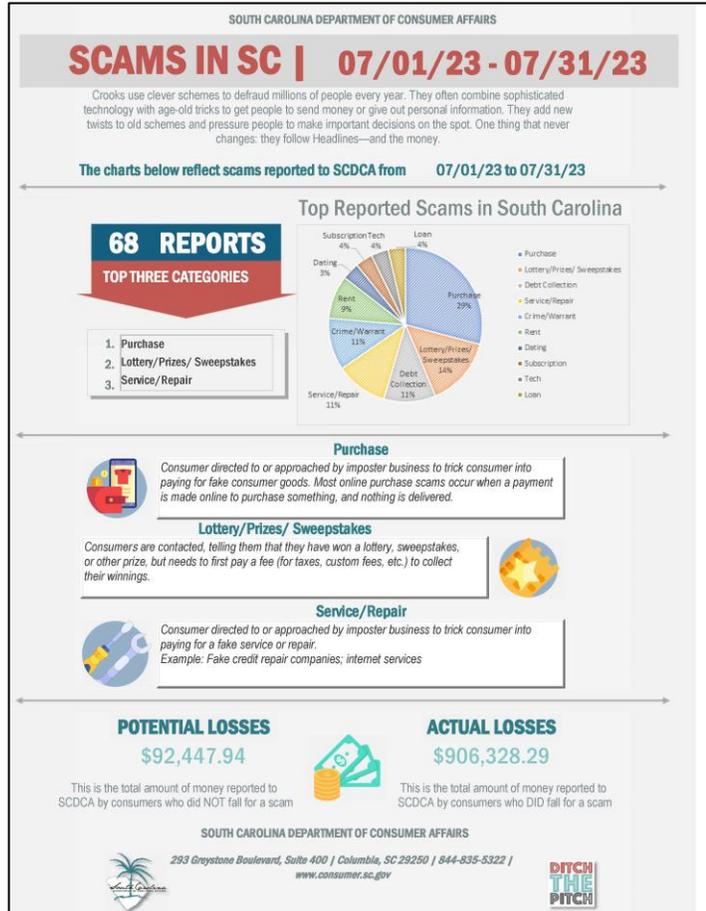
In celebration of the law's fifth anniversary, DCA is releasing a compilation of the HOA complaint data received from June 1, 2018 - December 31, 2022. Individual annual reports can be found on our HOA education webpage. Each report is in a categorized, filterable and searchable format.

EXECUTIVE SUMMARY

- The Department received 1,182 complaints regarding HOAs from June 1, 2018 - December 31, 2022. The five reports issued during that time only included 1,012 complaints as 170 did not meet the statutory requirements for inclusion, were duplicates or were referred to the SC Human Affairs Commission.
- Complaints came from 27 of South Carolina's 46 counties. The top three counties for complaints reported per capita are: (1) Horry (.74); (2) Jasper (.66); (3) McCormick (.42).
- The top complaint concern was a failure to adhere to and/or enforce covenants and bylaws (43%).
- State agency oversight was the number one recommendation for enforcing governing documents (28.1%).

www.consumer.sc.gov | (844) 835-5322

Reports



Count on News 2 SIGN UP

Sports Features Watch Living Local Jobs Contact Us About Us

SOUTH CAROLINA NEWS

South Carolinians lost \$906K to scams in July, data shows

by: [Sophie Brams](#)
Posted: Aug 8, 2023 / 05:12 PM EDT
Updated: Aug 8, 2023 / 05:12 PM EDT

(AP Photo/Elise Amendola, File)

COLUMBIA, S.C. (WCBD)- Consumers in South Carolina lost hundreds of thousands to scams last month, according to recent data from the S.C. Department of Consumer Affairs (SCDCA).

The agency said there were 68 scams reported between July 1 and July 31 which resulted in actual losses of \$906,328.29.

“Crooks use clever schemes to defraud millions of people every year,” the agency wrote in its report. “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

Current	Tonight	Tomorrow
81°	75°	90°
Light Rain with Thunder	Scattered Thunderstorms Precip: 54%	Scattered Thunderstorms Precip: 44%

counton2.com **Strong 2 HURRICANE-READY GUIDE 2023**

Everything you need

Publications - Written

John Doe 123-45-6789

01/20/46

DITCH THE PITCH

a guide for guarding against scams

A Publication from the SC Department of Consumer Affairs

HOW TO PREVENT IDENTITY THEFT

- Your Information has been Breached... What Now? Page 1
- Fraud Alerts, Freezes and ID Theft Protection Services, Oh My! So, What's the Difference? Page 2
- Security Freeze FAQs, Protecting Your Child's Identity and Tools to Consider. Pages 3-4
- Get In the Habit: Everyday Practices that Help You Avoid Identity Theft. Page 5
- Are YOU a Victim of Identity Theft? What to do. Page 6

A Publication from the SC Department of Consumer Affairs

CREDIT REPORTS

What they are and why they matter.

700

A Publication from the SC Department of Consumer Affairs

A PUBLICATION OF THE SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS

Identity THEFT and the LAW

A GUIDE FOR BUSINESS & GOVERNMENT

1 1 0 0 0 0 1 0 0 SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS 1 0 1 0 1 0 1 0

CYBER SECURITY BASICS

Cybersecurity doesn't need to be complicated. Here are the basics of cybersecurity so you can be in control of your information and keep your devices safe.

PROTECT

Your Files & Devices	Your Wireless Network	Your Identity & Privacy
<p>Update your software. Outdated software makes it easier for scammers to hack your device. Set automatic updates.</p> <p>Require passwords. Use passwords for all of your devices. Don't leave these devices unattended in public places.</p> <p>Secure your files. Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.</p> <p>Use two-factor authentication. This requires additional steps beyond logging in with a password – like a temporary code on a smartphone or a key that's inserted into a computer.</p> <p>Encrypt devices. Encrypt devices, files and other media that contain sensitive personal information. Encryption protects information sent over your network so it can't be read by outsiders.</p>	<p>Secure your home router. Change the default name and unique password, turn off remote management, and log out as the administrator once the router is set up.</p> <p>Setup a network firewall. A firewall is a piece of hardware and/or software that protects and controls traffic coming into your network. If your router has a firewall option, enable it.</p> <p>Use at least WPA2 encryption. Make sure your router offers WPA2 or WPA3 encryption, and that it's turned on. Just like on your devices, the encryption will protect your info from being read/accessed by outsiders.</p> <p>Disconnect old devices. Disconnect older devices you no longer use from the network. Their security may be out of date, creating a weak point on your network.</p>	<p>Own your online identity. Every time you sign up for a new account, app, or get a new device, immediately set the information sharing privacy/security settings to what you're most comfortable with. Regularly check these settings to make sure nothing has changed.</p> <p>Share with care. Think before posting online. Consider what a post reveals, who might see it and how it might affect you or others. ID thieves use the information you post online to try and guess your passwords, security questions and/or steal your identity!</p> <p>Beware of free Wifi hotspots. Public Wifi networks are not secure, which means that anyone may see what you are doing while you are connected. Avoid logging into accounts like email and financial services. Consider using a virtual private network (VPN) or a personal/mobile hotspot.</p>

Publications - Written

Overall Publications:

- 50+ publications available for download at consumer.sc.gov
 - Topics range include scam/ID theft education, business education, financial literacy, consumer protection, etc.
- 6 publications available for mail order

Welcome! We're the Department of Consumer Affairs.

 <p>SEARCH FOR COMPLAINTS</p>	 <p>SIGN-UP FOR EMAIL UPDATES</p>	 <p>ORDER FREE BROCHURES</p>	 <p>LICENSEE LOOKUP</p>
---	---	---	---

The South Carolina Department of Consumer Affairs ("SCDCA" / "Department") is the state's consumer protection agency. Established in 1974, SCDCA has more than forty years of experience in protecting South Carolina consumers while recognizing those businesses that act honestly and fairly. If you'd like to learn more about what we do, visit the ["About Us"](#) page.

Brochure Order Form

Questions?
Email ibooker@scconsumer.gov or call 803-734-0043.

* 1. Please select the brochure(s) you want sent

	1	10	20	40	50
Credit Reports-What they are and Why they Matter	<input type="radio"/>				
How to Prevent ID Theft	<input type="radio"/>				
Auto Guide for Consumers	<input type="radio"/>				
Auto Guide for Dealers	<input type="radio"/>				
Recovering from a Disaster	<input type="radio"/>				

What Main Information Sources We Use



Cybersecurity &
Infrastructure
Security Agency –
CISA.gov

FBI's Internet Crime
Complaint Center –
ic3.gov

Federal Trade
Commission –
ftc.gov

Federal
Communications
Commission –
fcc.gov

Consumer Financial
Protection Bureau –
cfpb.gov

Homeland Security –
dhs.gov

National
Cybersecurity
Alliance –
staysafeonline.org

Many more
government
agencies, etc.

Publications - Written

Ditch the Pitch (DTP)

- Released in July 2015
- Goal to educate the general public about the red flags of scams, types of scams, how to protect yourself and who to call.
- Currently updating DTP, releasing for the IDTU 10-year Anniversary
 - Include more cybersecurity, social media scams, etc.
 - Keep things more general



Publications - Written

Ditch the Pitch (DTP)

- We've given out approximately 29,500 DTP's since January 2019.
- We have had other states and other countries reach out and ask for permission to use the content for their own education.



Publications - Written

Publication Process

Research information sources.

Gather & condense information.

Design in Adobe Creative Suites.

Administrator, Legal, IDTU, more review for accuracy, errors, changes.

After at least two rounds of edits, released to the public.



Publications - Written

Special Considerations in the Publication Process

- Grade level of the written content.
 - Goal of 5th grade, 8th grade maximum.
- White Space.
- Font Size and Font Type.
- “Would the average person be able to understand this?”



Publications - Written

If it sounds too good to be true... SCAM RED FLAGS

Below you will find a list of the most common signs of a scam. Be wary if someone:

- Asks you to verify personal identifying information.
- Asks you to wire transfer money or purchase a prepaid/reloadable debit card or iTunes gift card and give them the number off the card.
- Sends you a check, asking you to cash it and wire or send money somewhere.
- Poses as a local, state, or federal law enforcement officer. They may also pose as other government officials.
- Scares you with threats of arrest or garnishment.
- Makes you think their "offer" is time sensitive. "Act NOW, or you won't get this great deal!"



Bottom Line: If you are fielding a cold call (email, text message, etc.) never give information to the person and when in doubt, **hang up and follow up!**

3 ways TO DEFEND against phone scams

1. Don't fall for high pressure tactics
2. Be suspicious of wire transfer or reloadable debit card payment requests
3. When in doubt, hang up and follow up

RED FLAG: Scammers have also been asking consumers to make payments with iTunes gift cards. Businesses and government organizations will not ask for payment this way.

2

SC Department of Consumer Affairs

www.consumer.sc.gov | (844) 835-5322

3

No matter the scam... THE RED FLAGS ARE THE SAME

We may not know be able to know every scam out there, but if you know the red flags, you can avoid getting scammed. Here are the most common signs of a scam:

- Scammers PRETEND to be someone you know or recognize.**
Whether it's a government agency, business or organization you know, scammers love to act like people they think you'll trust. Could even be a "friend" on a social media app like Instagram or Facebook. Scammers do this because they know you're more likely to respond if you recognize the contact.
- Scammers say there's a PROBLEM or a PRIZE.**
They might say you're in trouble with the government, that you owe money or someone in your family had an emergency. Some scammers say there's a problem with a financial account and you need to verify information. Others say you won money in a lottery or sweepstakes but have to pay a fee to get it.
- Scammers PRESSURE you to act immediately.**
Scammers want you to act before you have time to think. They might threaten to arrest you, sue you, take away licenses or deport you. Scammers will say whatever they can to scare you into falling for what they want.
- Scammers tell you to PAY in a specific way.**
Scammers love forms of payment that are difficult to trace. Some include wire transfers, prepaid debit cards, gift cards, cryptocurrency and money transfer services. Some will send you a fake check, tell you to deposit it, and then send them money.

As you read through "Ditch the Pitch," when you see the red flag icon , that's a sign of a common red flag.

2 SC Department of Consumer Affairs



- 1 Don't answer calls or respond to text messages from numbers you don't know. Block these numbers as they come in.
- 2 Don't give personal or financial information for a request that you didn't expect. Legitimate businesses don't do this.
- 3 Don't fall for high pressure tactics. Anyone who pressures you to make a decision, pay or give over personal info is a scammer.
- 4 Know the forms of payment scammers like to use. Beware of gift cards, cryptocurrency and wire transfers.
- 5 Stop and talk to someone you trust. Before you do anything, tell a friend, family member or neighbor what happened.

consumer.sc.gov | (844) 835-5322 3

Publications - Videos



YouTube video player showing a woman speaking in front of a bookshelf. The video title is "Homeowners Associations & DCA". The channel is SDCATV with 328 subscribers. The video has 4.7K views and was posted 3 years ago. The description mentions Homeowners Associations (HOAs) and frequently asked questions regarding DCA and HOAs. A link to "More HOA Resources: consumer.sc.gov/HOA-ed ...more" is provided.

YouTube video player showing a website banner for the South Carolina Department of Consumer Affairs. The video title is "How to file a complaint with the South Carolina Department of Consumer Affairs." The channel is SDCATV with 328 subscribers. The video has 176 views and was posted Dec 15, 2022. The description explains that the department processes and mediates written consumer complaints and encourages consumers to contact the business first. It provides instructions on how to file a complaint on the consumer.sc.gov website.

YouTube video player showing a website banner for the DCA Licensure Gateway. The video title is "DCA Licensure Gateway: Printing Your Certificate". The channel is SDCATV with 328 subscribers. The video has 3,200 views and was posted Dec 15, 2016. The description explains that the video teaches how to use the South Carolina Department of Consumer Affairs' online licensing system, CALAS, to print out a certificate.

Website

SC.GOV Online Services | Agency Listing

You can [file a complaint](#) and submit applications for [licensing online](#). Filings you do not wish to make, or that are not available, online can be submitted via mail for processing. Department staff is available to assist with any questions at (800) 922-1594 (toll free in SC) or 803-734-4200 8:30 a.m. until 5 p.m. Monday through Friday, excluding State holidays. You can also email general questions to scdca@scconsumer.gov.

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

Search Consumer Affairs

About Us Business Resources/Laws Consumer Resources News Identity Theft/Scams Contact Us

Protecting Consumers from Inequities in the Marketplace

How Do I ... ▾

- File a complaint?
- Get a license?
- Background a business?
- Report identity theft?
- Report a scam?
- Request a presentation?

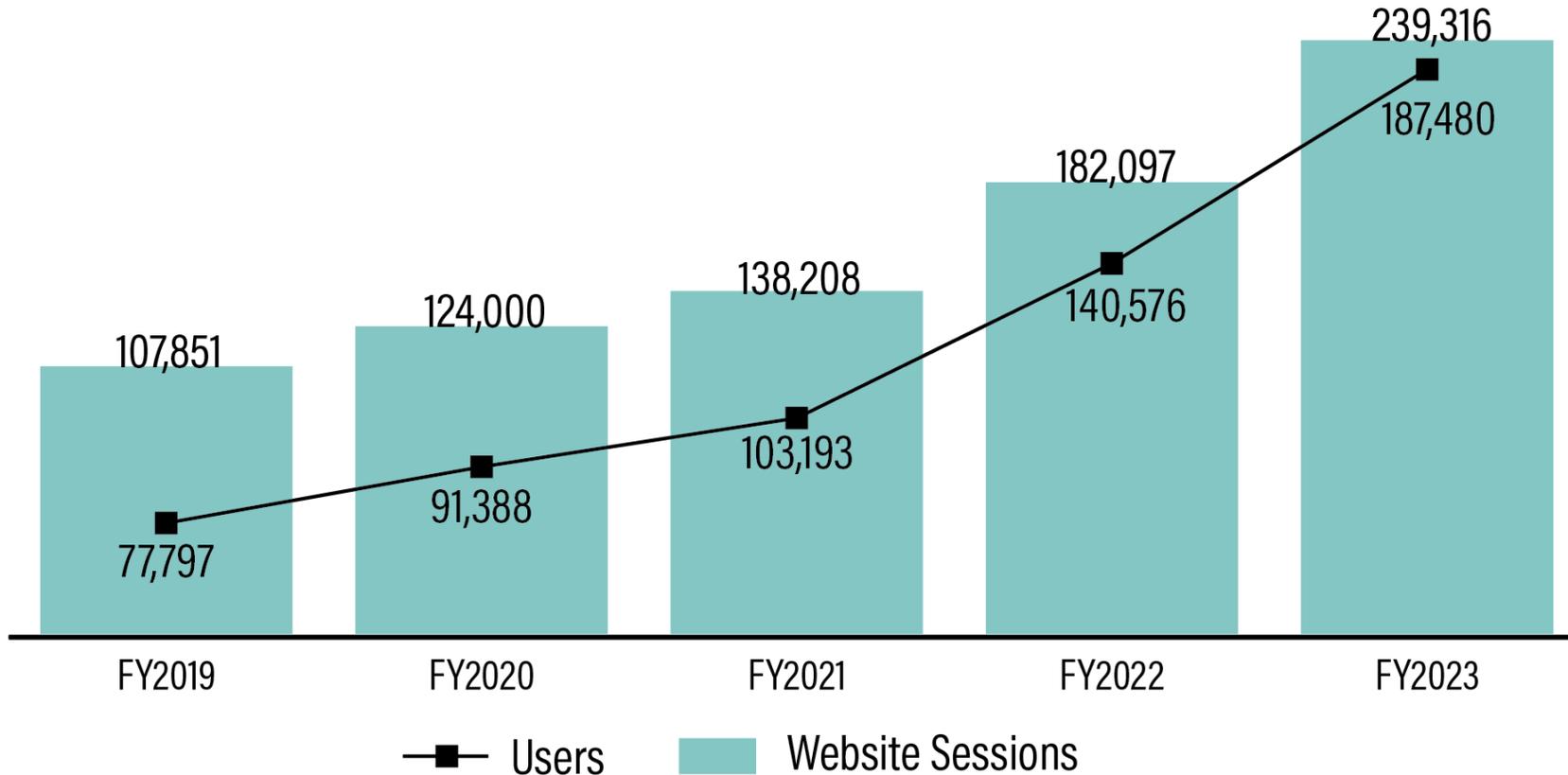
Welcome! We're the Department of Consumer Affairs.

SEARCH FOR COMPLAINTS SIGN-UP FOR EMAIL UPDATES ORDER FREE BROCHURES LICENSEE LOOKUP

The South Carolina Department of Consumer Affairs (SCDCA) Department is the state's consumer protection agency. Established in 1974, SCDCA has more than forty years of experience in protecting South Carolina consumers while recognizing those businesses that act honestly and fairly. If you'd like to learn more about what we do, visit the "[About Us](#)" page.

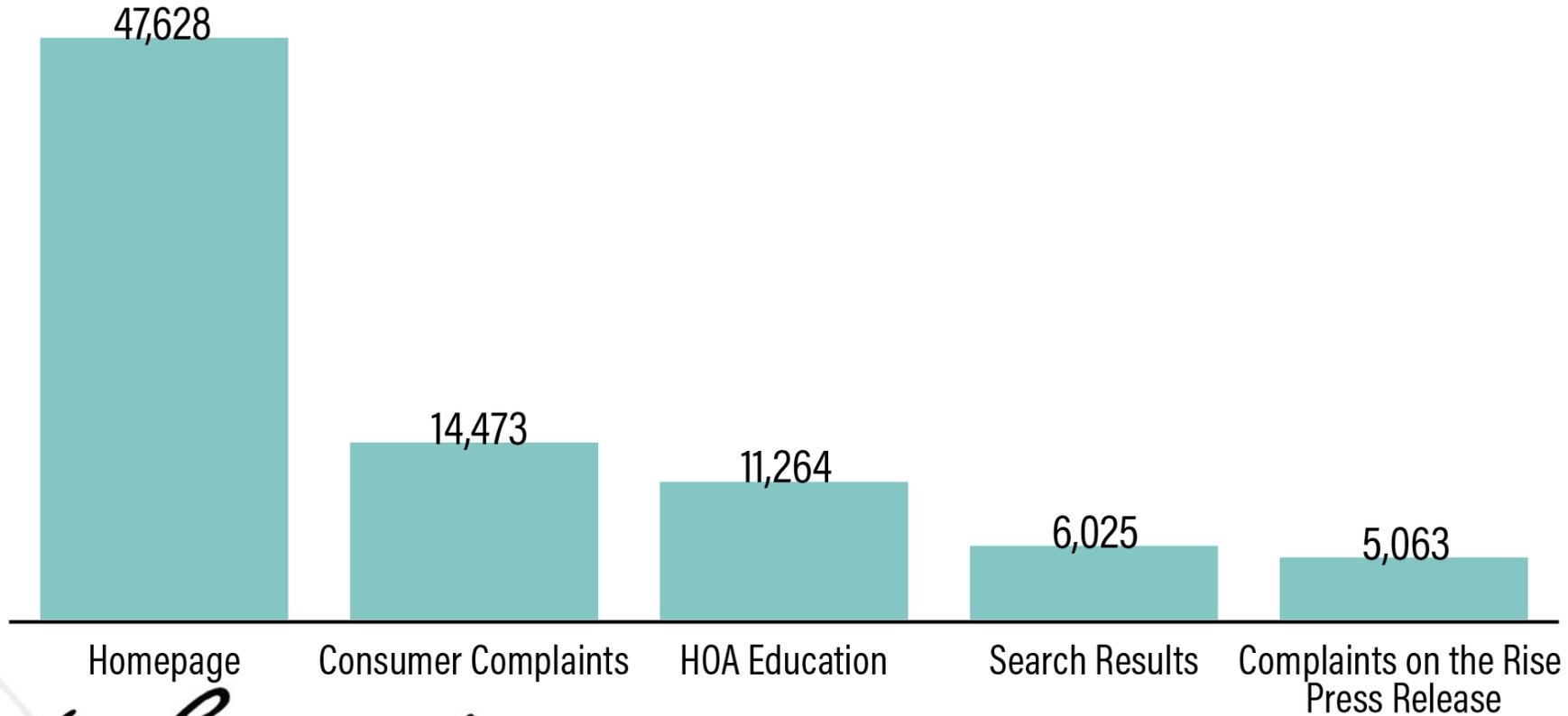


Website



Website

- Top Webpages visited April 13, 2023 - August 17, 2023



Partnerships



Commission on
Minority Affairs

Department on
Aging

Attorney
General's Office

SCEMD

ORS

Department of
Insurance

State Treasure's
Office – SC
Economics

SCDC

FTC

Many more...

Partnerships

What a Partnership Looks Like

- What Happens if a Consumer Clicks on the Ad?



South Carolina DEPARTMENT OF CONSUMER AFFAIRS

Home » Recent News » Solar Scammers Coming into the State

Thu, 07/27/2023

COLUMBIA, S.C. - It's summertime with the South Carolina Department of Consumer Affairs aware of an increase in reports of misdeeds by solar salespersons:

- **No utility company in South Carolina** reported that some solar sales representatives say they need to come inside your home without making an appointment or providing personal information of any type.
- **Real utility companies make appointments** and say they need to come inside your home without making an appointment or providing personal information of any type.
- **Know your rights.** There are state consumer protection laws that require utility companies to provide a consumer with a copy of a consumer protection pamphlet.
- **Know the red flags.** You can spot a scammer by looking for red flags like these and following the rules at <https://solar.sc.gov/consumers>.

Considering solar? Visit solar.sc.gov before signing on the dotted line. Consider going to consumer.sc.gov and click on solar businesses via the website. Click

SOLAR.SC.GOV
South Carolina's source for solar information

Home » Consumer Protections » Solar Scams and Misconceptions

Solar Scams and Misconceptions

Consumers can produce clean energy and save money with solar panels. Adding panels to a home should educate themselves first before signing any papers. Consumers should not sign if they do not feel okay to wait and ask questions before signing.

“The government will pay to put solar on your home.”
Despite claims in the media, no government programs exist that pay for solar on private homes.

“You’ll automatically get a 55% tax rebate from the government.”
Those “rebates” are actually tax credits. Consumers only get a tax credit if they file state or federal tax returns. The South Carolina tax credit is limited to \$3,500 per year and no more than 50% of owed taxes but no more than \$1,000 per year.

“Those trees won’t be a problem- we’ll just add more panels.”

PURCHASE/LEASE OF RENEWABLE ENERGY SYSTEMS STANDARD DISCLOSURE

You are receiving this as required by law. It is **NOT** the complete contract. Read your contract in full before signing. For more information on your rights under the law, contact the South Carolina Department of Consumer Affairs at (803) 734-4200.

This disclosure is prepared for:

Name: _____ Address: _____
 Phone Number: _____ Email: _____
 Make: _____ Model: _____ Estimated size of system in kilowatts (kWdc): _____
 Will you lease or own the system?: Lease Own (Circle all that apply: Cash | Loan | Other)

Individual preparing this disclosure:

Name: _____ Signature: _____
 Title: _____ Company: _____ Date: _____

COST & SAVINGS

Total cost to be paid, including any interest, installation fees, document preparation fees, service fees or other fees. These fees may also be included in the total cost.

System maintenance/upkeep:	System repairs/fees:	Total cost:
<input type="checkbox"/> Included <input type="checkbox"/> Not Included	<input type="checkbox"/> Included <input type="checkbox"/> Not Included	\$ _____

You **HAVE** **HAVE NOT** been provided with a savings estimate based on your contract. If the seller provided you with a savings estimate, the seller: **IS** **IS NOT** guaranteeing these savings. Contact your electric company for more info on rates and potential savings.

You **HAVE** **HAVE NOT** been provided info on tax credits/rebates. You may or may not be eligible for those tax credits/rebates. Talk to a tax professional for more info.

OTHER IMPORTANT DETAILS

- Seller **WILL** **WILL NOT** place a lien on your home as part of entering the contract.
- Seller **WILL** **WILL NOT** file a fixture filing on the system. A fixture filing gives the company the right to take back the system if you fail to pay per the contract.
- System **WILL** **WILL NOT** be connected to the electric grid.
- If you sell your home, you **ARE** **ARE NOT** allowed to transfer the system/contract to a new home or property.
- In terms of your system, the seller is providing you with a: System performance or production guarantee. Other type of system guarantee. No guarantee.
- You **ARE** **ARE NOT** responsible for insuring the system. If so, contact your insurance company to discuss your policy.

You are receiving this as required by law. For more information on your rights under the law, contact the South Carolina Department of Consumer Affairs at (803) 734-4200 or visit consumer.sc.gov.

RENEWABLE ENERGY

What You Need to Know

Buying or leasing solar panels or other renewable energy systems is a big decision. Consumers should do their homework, check prices from several sources and think carefully about which choice is best. South Carolina law gives consumers specific rights in this area, too. Here are some key things to know while thinking about buying or leasing a renewable energy system.

BASIC TERMS TO KNOW

A **renewable energy facility or system** makes electricity through solar, wind, hydroelectric, etc.

A **retailer or seller** is a person or business that sells the system or owns a leased system.

A **lead generator** is a person who finds potential customers for a retailer.

A **lease** is a contract where you pay a monthly amount for a set period of time to use the renewable energy facility and the energy it makes. You will not own the system.

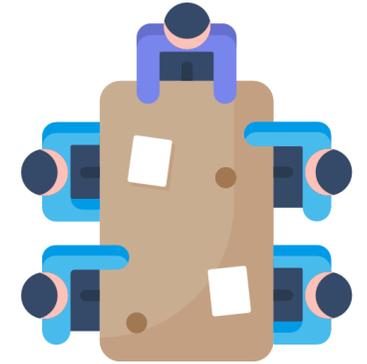
A **purchase** is when you pay for the system up front with cash or with financing (i.e., home equity line, bank loan, use credit card). You will own the system.

QUESTIONS TO ASK BEFORE YOU SIGN

- If you're given a price, what's included?
 - Are maintenance fees, repairs, property taxes or insurance included?
 - If leasing, will monthly fees increase over time?
 - Is there a lease buyout option that would allow you to buy the system?
- Is there a warranty on the system or install? Is there a production guarantee? If yes, what are the details?
- Is the seller or lead generator predicting how much you'll save by switching to a renewable energy system? If they are, how did they calculate the savings?
- Are there any tax credits/rebates that you qualify for? Is the credit/rebate shown in the total price? Who gets the credit/rebate, you or the seller?

For a free copy of a consumer guide to solar, visit solar.sc.gov or call (803) 737-5230.

Boards/Committees/Memberships



SC Cyber
Ecosystem
Initiative

APCC Outreach
Committee

AARP Fraud
Watch Network

SC JumpStart
Board

LifeSmarts State
Coordinators

Richland District
One CATE
Leadership Board

National
Cybersecurity
Alliance

Events



- National Cybersecurity Awareness Month
- National Consumer Protection Week
- ID Theft Awareness Week/Month
- World Elder Abuse Awareness Day



Events



- National Cybersecurity Awareness Month
- National Consumer Protection Week
- ID Theft Awareness Week/Month
- World Elder Abuse Awareness Day



Presentations

General Topics

- ID Theft/Scams
- Financial Literacy
- Consumer Protection
- SCDCA Education
- Business Licensing



**ID Theft & Scams:
How to Stay Safe**

Bailey Parker
Communications Director

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

www.consumer.sc.gov • 800-922-1594

Credit Scores Explained

Bailey Parker
Communications Director

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

www.consumer.sc.gov • 800-922-1594

**South Carolina Residential Landlord Tenant Act:
An Overview**

Zach Passmore
Complaints Attorney

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

www.consumer.sc.gov • 800-922-1594

**Filing a Complaint
with SCDCA**

Bailey Parker
Communications Director

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

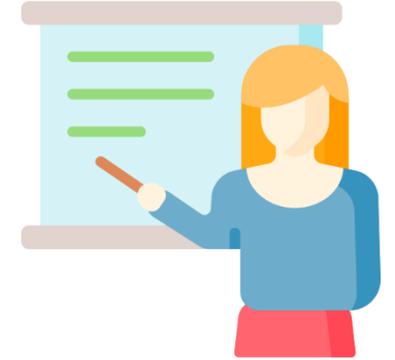
www.consumer.sc.gov • 800-922-1594

Closing Fee Changes

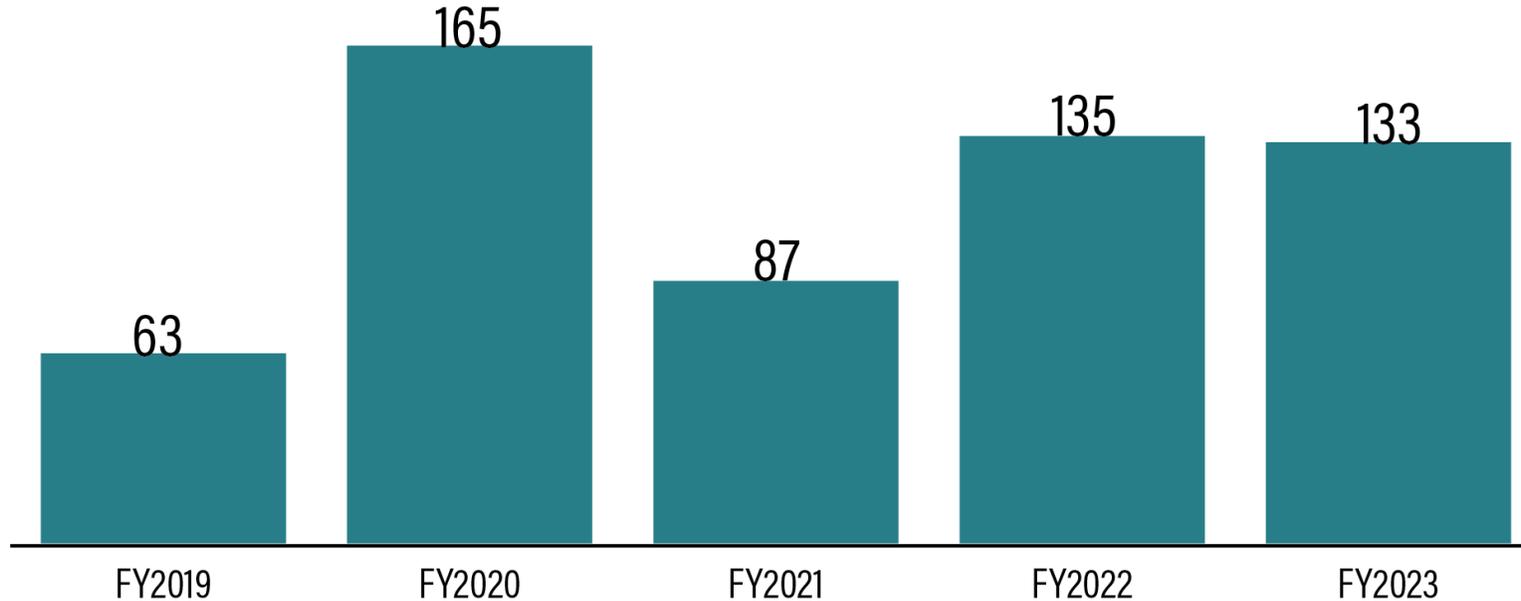
Kelly H. Rainsford
Deputy Administrator/General Counsel

South Carolina

Presentations



Consumer Presentations Given

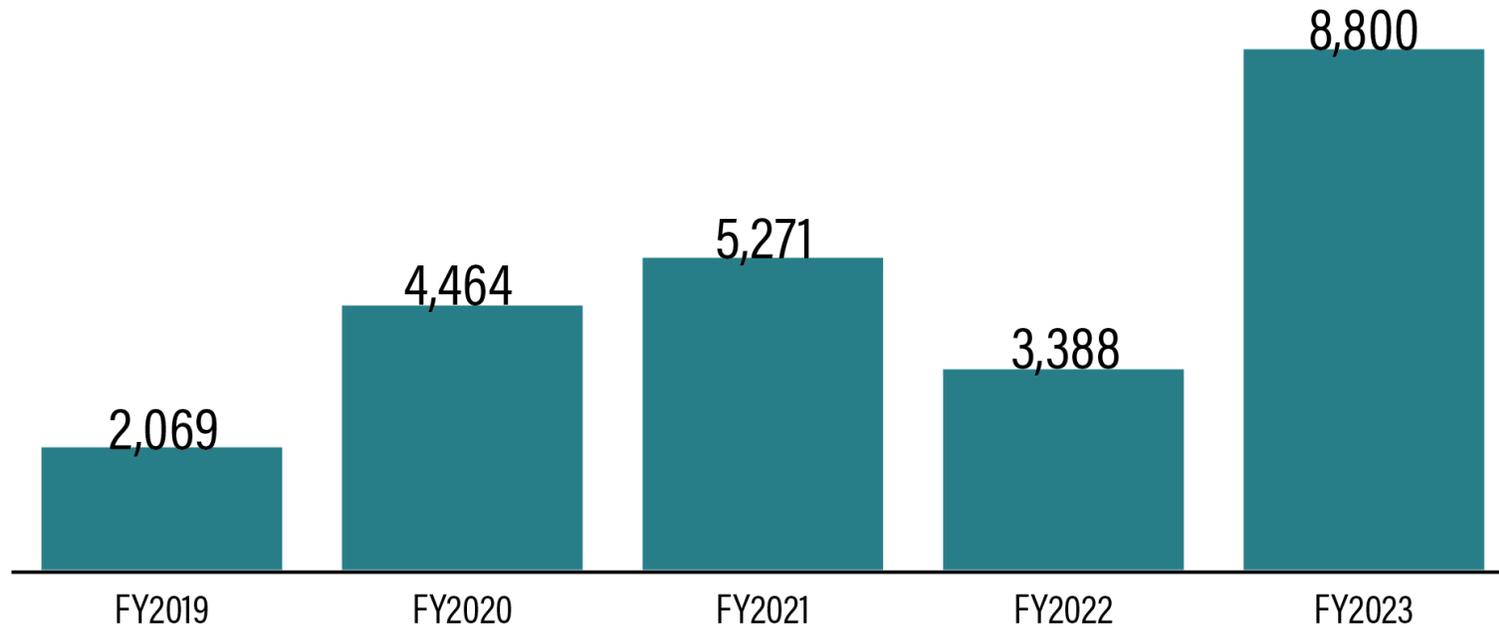


Some Topics Covered with Consumers in FY23:

- Debt Collection Basics
- Get Rich Quick Schemes
- Cybersecurity Basics
- Social Media Safety
- Credit Scores Explained

Presentations

Consumer Presentation Attendees



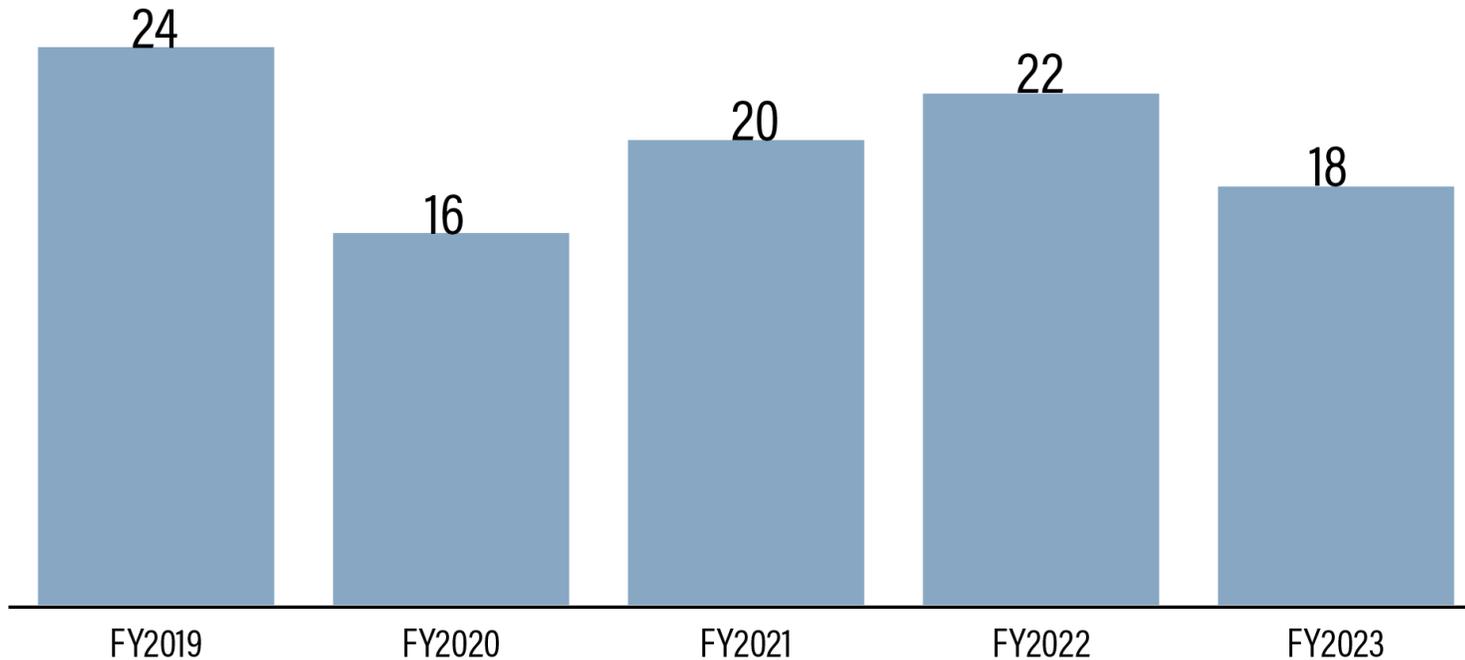
Examples of Groups We Speak To:

- Senior Centers
- Churches
- Libraries
- Teachers/Students
- Conferences

Presentations



Business Presentations Given



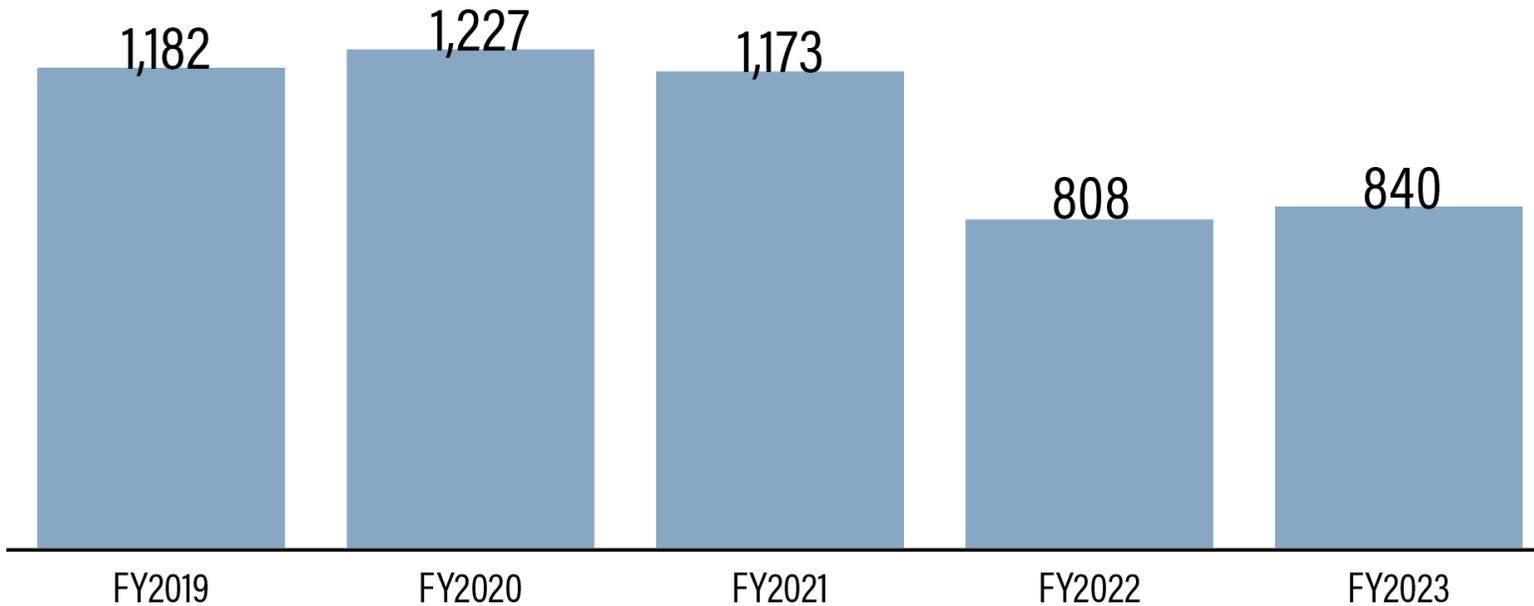
Some Topics Covered with Businesses in FY23:

- Closing Fee Statute Updates
- ID Theft and the Law
- Licensing Renewals for all areas that we License
- Magistrates Training

Presentations



Business Presentation Attendees

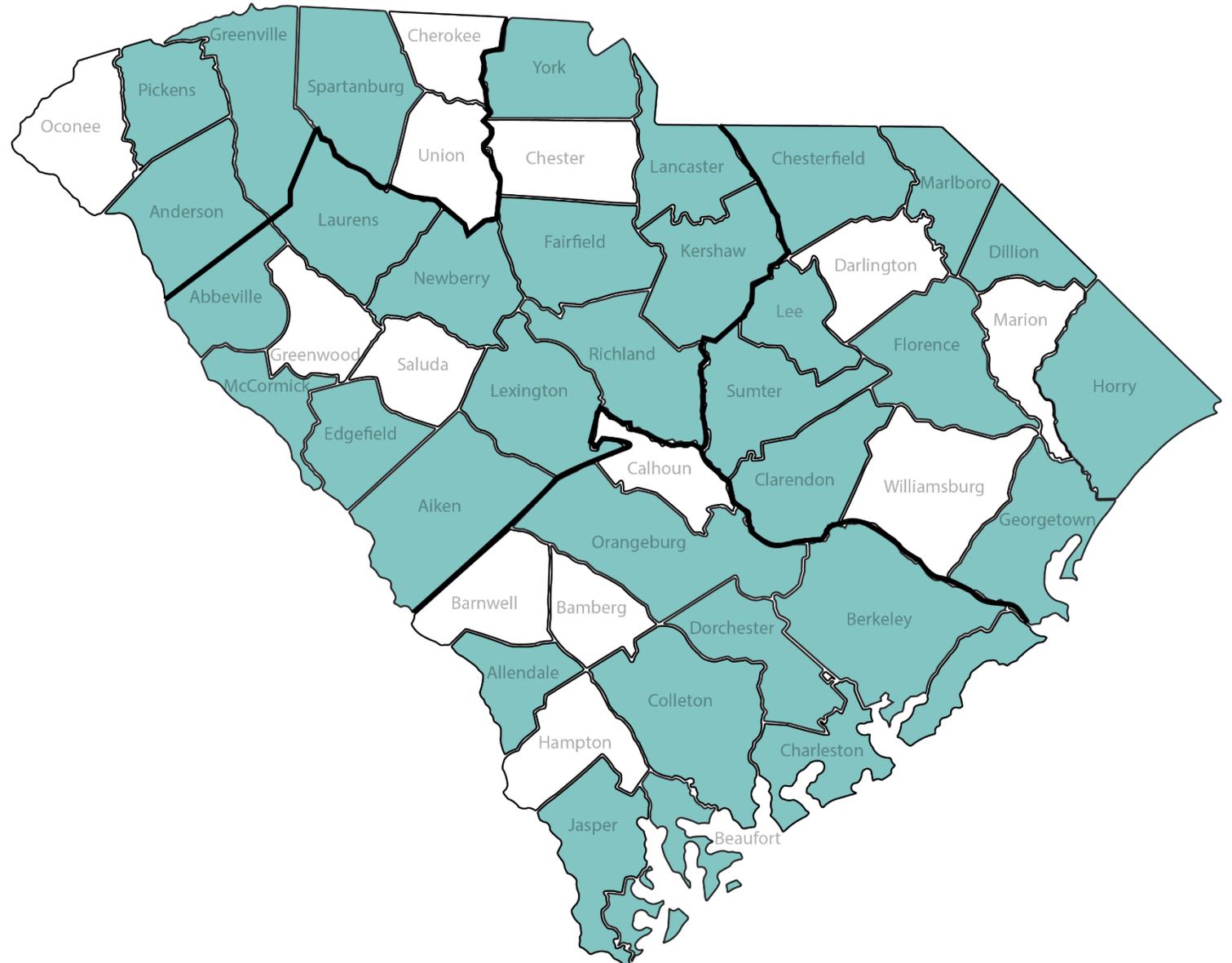


Examples of Groups We Speak To:

- Regulated Industries
- Credit Unions
- Small Business Associations
- Law Enforcement
- Professional Conferences

Presentations

Counties Visited from
FY19-FY23

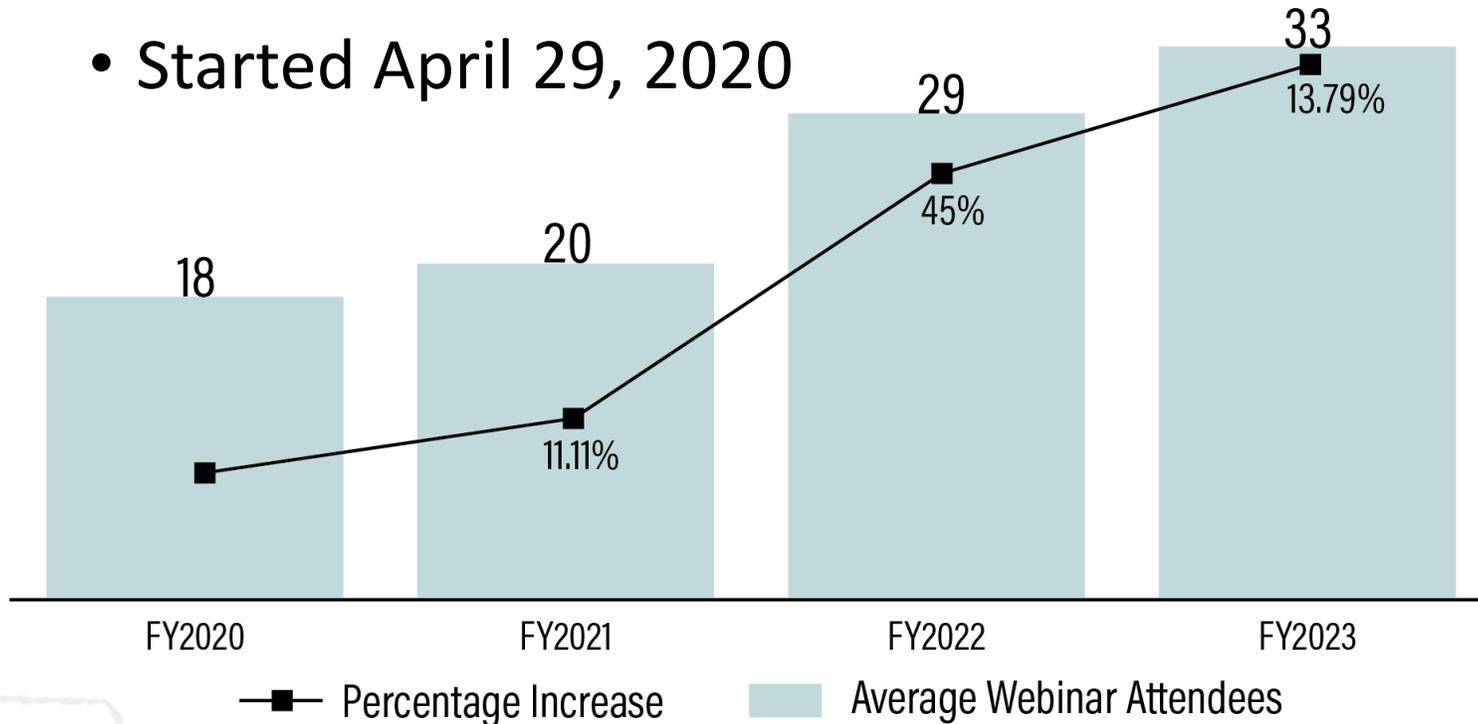


Presentations



Wednesday Webinars

- Started April 29, 2020



Some of our most popular webinars in FY23:

- HOA Complaint Report 2023 – 101 attendees
- Cybersecurity Update with FBI Columbia – 77 Attendees
- Cryptocurrency Basics – 56 attendees
- HOA 5 Year Complaint Report – 52 Attendees

Presentations

CALENDAR

Today ◀ ▶ Wednesday, August 23

- Wednesday, August 23**
 - 10:30am Wednesday Webinar: Job Scams
- Wednesday, August 30**
 - 10:30am Wednesday Webinar: Charity Scams
- Friday, September 1**
 - Credit Counseling Renewal Begins
- Wednesday, September 6**
 - 10:30am Wednesday Webinar: Debt Collection
- Tuesday, September 12**
 - 1:00pm Commission Meeting
- Wednesday, September 13**
 - 10:30am Wednesday Webinar: My Information Has Been Breached... What Now?
- Thursday, September 14**
 - 2:00pm Identity Theft and the Law for Businesses
- Wednesday, September 20**
 - 10:30am Wednesday Webinar: Identity Theft and the Law for Consumers
- Wednesday, September 27**
 - 10:30am Wednesday Webinar: Credit Scores Explained
- Saturday, September 30**
 - Preneed Funeral Renewal Deadline
 - Prepaid Legal Rep. Renewal Deadline
- Wednesday, October 4**
 - Preneed Funeral Renewal Deadline

Events shown in time zone: Eastern Time - New York [Google Calendar](#)

Business Webinar Announcement

Topic: Preneed Funeral Contract Renewals

The Department will discuss the renewal process including how to file online. The renewal period for Preneed Funeral Contracts began on August 1, 2023. All renewal documents and fees must be submitted/postmarked by September 30, 2023.

When: Wednesday, August 16, 2023, 2-3 p.m.

Presenters:

Deborah Friday Lockard,
SCDCA Licensing Supervisor

Kerri Boyer
SCDCA Licensing Attorney

[Register Now!](#)

After registering, you will receive a confirmation email containing information about the webinar. There will be time allotted at the end of the webinar for questions.



NOTICE: RENEWALS FOR PRENEED FUNERAL CONTRACTS

The renewal period for Preneed Funeral Contracts begins on August 1, 2023. All renewal documents and fees **must be submitted/postmarked by September 30, 2023.**

The **fastest and easiest** way to renew is by filing **ONLINE** today using the Department's License Gateway. Go to consumer.sc.gov, click on "How do I... then, "Get a license?" Please provide the email address and password you first registered with to login. When filing online, you can pay your renewal fee using a credit card without paying a convenience fee!

A webinar on the renewal online process will be held on August 16, 2023, at 2 p.m. If you would like to register, please visit consumer.sc.gov/upcoming-presentationswebinar.

NOTE: This is the only renewal notice you will receive by mail. Update your email address in the License Gateway to ensure receipt of future notices.

Questions? Stacy Staley
(803) 734-4251
sstaley@sccconsumer.gov

SC Department of Consumer Affairs
@SCDCA SCDCA TV

[Home](#) > Upcoming Presentations/Webinars

Upcoming Presentations/Webinars

SCDCA provides free presentations to businesses and consumers in the state of South Carolina. The presentations listed below are all open to the public. If you would like to request a private webinar or to learn more about what topics we offer, visit [our presentation page](#).

Click the corresponding topic below to register for a webinar.

Date	Topic
August 30, 2023 at 10:30-11:30 a.m.	Wednesday Webinar: Charity Scams
September 6, 2023 at 10:30-11:30 a.m.	Wednesday Webinar: Debt Collection Basics
September 13, 2023 at 10:30-11:30 a.m.	Wednesday Webinar: My Information Has Been Breached... What Now?
September 14, 2023 at 2:00-3:00 p.m.	Identity Theft and the Law for Businesses
September 20, 2023 at 10:30-11:30 a.m.	Identity Theft and the Law for Consumers
September 27, 2023 at 10:30-11:30 a.m.	Wednesday Webinar: Credit Scores Explained
October 4, 2023 at 10:30-11:30 a.m.	Wednesday Webinar: Cybersecurity Basics
October 11, 2023 at 10:30-11:30 a.m.	Wednesday Webinar: SCDCA ID Theft Unit 10-year Anniversary Report
October 18, 2023 at 10:30-11:30 a.m.	Wednesday Webinar: Security Beyond Passwords
October 25, 2023 at 10:30-11:30 a.m.	Wednesday Webinar: Staying Safe on the Internet

For our full Google Calendar, [click here](#).

Missed one of our webinars?

Here is a selection of webinars that are available for limited-time viewing.

COMMON SOCIAL MEDIA SCAMS

Why Social Media?

- Low-cost.
- Can reach millions of people from anywhere in the world.
- Easy to fake a persona.
- Easy to hack into an existing profile.
- Free way to find out more info about YOU!

HURRICANE PREPAREDNESS AND AVOIDING SCAMS

Common Post-Disaster Scams

COMMON TEXT MESSAGE SCAMS

- What is Identity Theft?
- Common text scams
- How Can You Avoid the scams?
- Protecting your information for free

HOR FIVE-YEAR COMPLAINT REPORT

Top 3 Types of Issues Raised Overall

24.32%	13.54%	11.22%
• Failure to adhere to/enforce	• Concerns regarding maintenance	• Failure to notify residents of

Helpful Links

- [GET LATEST FROM DCA](#)
- [FILE YOUR COMPLAINT](#)
- [REQUEST A PRESENTATION](#)
- [SEARCH COMPLAINTS](#)
- [EMAIL DCA](#)

Questions?

Bailey Parker
Communications Director
(803) 734-4296

(800) 922-1594
Toll Free In SC
(803) 734-4200

293 Greystone Blvd.
Suite 400
Columbia, SC 29210

Mailing Address:
PO Box 5757
Columbia, SC 29250-5757



Presentations

Ditch the Pitch BINGO

- US Attorneys Office introduced us to Pennsylvania Department of Banking and Securities introduced us to their “Investment Fraud BINGO.”

INVESTMENT FRAUD BINGO				
F1 Ask for recommendations in writing.	R16 Don't rely on the testimony of others, regardless of how well you know them.	A31 Understand what your advisor is allowed to sell you.	U46 If the sales person cannot give you detailed answers, hang up!	D61 If you don't understand how the investment works, don't buy it.
F2 Been victimized? Call the Pennsylvania Department of Banking & Securities at 1-800-PA-BANKS (1-800-722-2657) or 1-800-600-0007.	R17 Be wary when a stranger contacts you about an investment.	A32 Be very skeptical of people who promise big profits.**	U47 If in doubt, say "NO!" Trust your instincts.	D62 Nigerian Letter Scam, promising millions for help with foreign business exchange.*
F3 Billions of dollars a year are lost to investment fraud.*	R18 Very few people ever get money back from illegal securities dealers.	A33 Make sure you understand the fees and the way your advisor makes money.*	U48 It is much less risky to hang up.	D63 Ponzi Schemes - Only Ponzi promoters get rich.*


Investor Fraud Bingo



DITCH THE PITCH

BINGO

Bailey Parker
Communications Director

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

consumer.sc.gov • (800) 922-1594

Presentations

Ditch the Pitch BINGO

B	I	N	G	O
1	16	31	46	61
2	17	32	47	62
3	18	33	48	63
4	19	34	49	64
5	20	35	50	65
6	21	36	51	66
7	22	37	52	67
8	23	38	53	68
9	24	39	54	69
10	25	40	55	70
11	26	41	56	71
12	27	42	57	72
13	28	43	58	73
14	29	44	59	74
15	30	45	60	75

N41



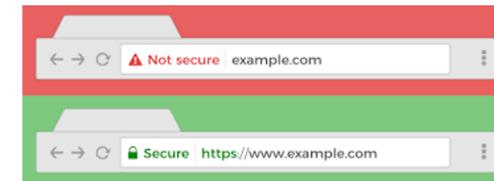
Don't let embarrassment or fear keep you from reporting theft or fraud.



O63



Before you enter your personal information online, be sure the company is reputable and uses encrypted technology. Look for "https" (not just "http").



Presentations

Ditch the Pitch BINGO



Social Media

What Platforms We Use



Facebook



Twitter



YouTube



LinkedIn



NextDoor



Adding:

- Instagram
- Threads

Social Media

How We Decide What to Post

Is there an increase in a certain type of scam report or complaint?

Is there a specific consumer topic that keeps coming up in calls, emails, presentations?

Is there an event coming up that needs to be announced?

Is there a timely topic that needs to be addressed?

Is a report being released?

Social Media

How We Decide What to Post

Public Information Annual Calendar

JULY	AUGUST	SEPTEMBER
<p>Topics of interest: Scholarship scams/ Student Loans Work-at-Home Investment scams Military Consumer Protection Day</p> <p>Materials for Issue: PR ON LEGISLATIVE CHANGES SUPERVISORY HIGHLIGHTS BIANNUAL SCAM REPORT #workfromhome #itsascam</p>	<p>Topics of interest: Contractor fraud Apt./House hunting Tax Free Weekend Vehicles: Lemon Law, flood-damaged, warranties, repossession</p> <p>Materials for Issue: BACK-TO-SCHOOL/TAX-FREE PR BIANNUAL COMPLAINTS REPORT #taxfree #lemonlaw #repo</p>	<p>Topics of interest: Job Hunting Government grant scams LifeSmarts National Preparedness Month</p> <p>Materials for Issue: ACCOUNTABILITY REPORT FY PR #lifesmarts #findajob #itsascam</p>
OCTOBER	NOVEMBER	DECEMBER
<p>Topics of interest: Contact Lenses Discount Medical Plans Cyber Security Awareness Month Domestic Violence Awareness Month International Charity Fraud Awareness Week</p> <p>Materials for Issue: ANNIVERSARY REPORT IDTU (EVERY 5 YEARS) #cyberaware</p>	<p>Topics of interest: Black Friday Budgeting International Fraud Awareness Week Military Financial Literacy Child Safety Protection Month Utility Scam Awareness Day (Usually in the third week)</p> <p>Materials for Issue: #blackfriday #movember</p>	<p>Topics of interest: Cyber Monday/Online shopping Toy Safety (CPSC) Gift Cards National Tax Security Awareness Week (First week of December) ID Theft Awareness Month</p> <p>Materials for Issue: HOLIDAY SHOPPING PR SECURITY BREACH REPORT & PR #cybermonday #IDtheft</p>

JANUARY	FEBRUARY	MARCH
<p>Topics of Interest: Returns/refunds/exchanges Refund Anticipation Loans Tax Scams Tax ID Theft Awareness Week Physical Fitness</p> <p>January 28 – Data Privacy Day</p> <p>Materials for Issue: SUPERVISORY HIGHLIGHTS HOA REPORT #taxes #scamreport</p>	<p>Topics of Interest: Debt collection Credit repair/counseling Vacation Scams America(/Military) Saves Week Vulnerable Adults Month Romance Scams</p> <p>Materials for Issue: STATE OF CREDIT PR #debt #itsascam</p>	<p>Topics of Interest: NCPW Veteran Information Real estate Foreclosure/Bankruptcy Disabilities Awareness Month</p> <p>Materials for Issue: ID THEFT/SCAMS REPORT #NCPW #NCPW2018 #realestate</p>
APRIL	MAY	JUNE
<p>Topics of Interest: Fair Housing Month PAHF Financial Literacy Month Autism Awareness Month</p> <p>Materials for Issue: #finlit #housing</p>	<p>Topics of Interest: Hurricane Preparedness Home safety, Children's Products Fuel efficiency Older American's Month</p> <p>May 5 – World Password Day</p> <p>Materials for Issue: #stormaware #staysafe</p>	<p>Topics of Interest: Home Ownership Month Mortgage fraud Credit report/repair/counseling Weight loss/fitness Alzheimer's/Brain Awareness Month, Elder Abuse Awareness Month Safety Month</p> <p>Materials for Issue: MORTGAGE LOG REPORT & PR #mortgage #home</p>
<p>*Floating PR topics: Enforcement actions resulting in criminal actions or notable refunds for consumers; Certifications/Staff accomplishments; New Directors</p>		

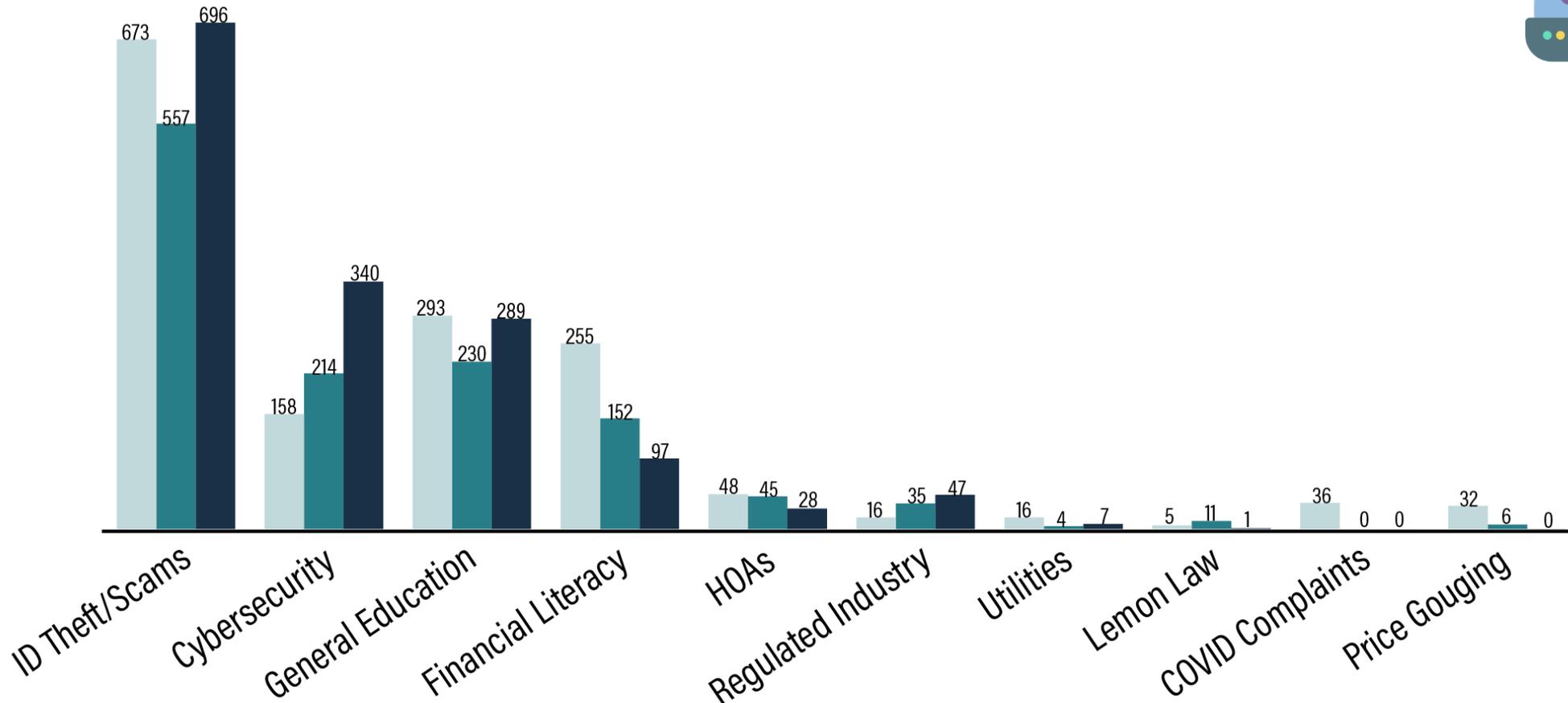
Social Media



How Posts are Reviewed

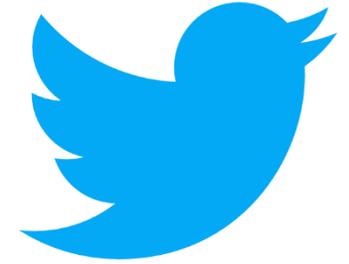
- The social media strategist creates a graphic and send them to the PI director for review.
- PI director reviews for accuracy, understanding, etc. If needs additional review, will consult with the administrator.
- If the post will be used in an ad, the PI director will consult with the administrator and/or legal for review and accuracy.

Social Media



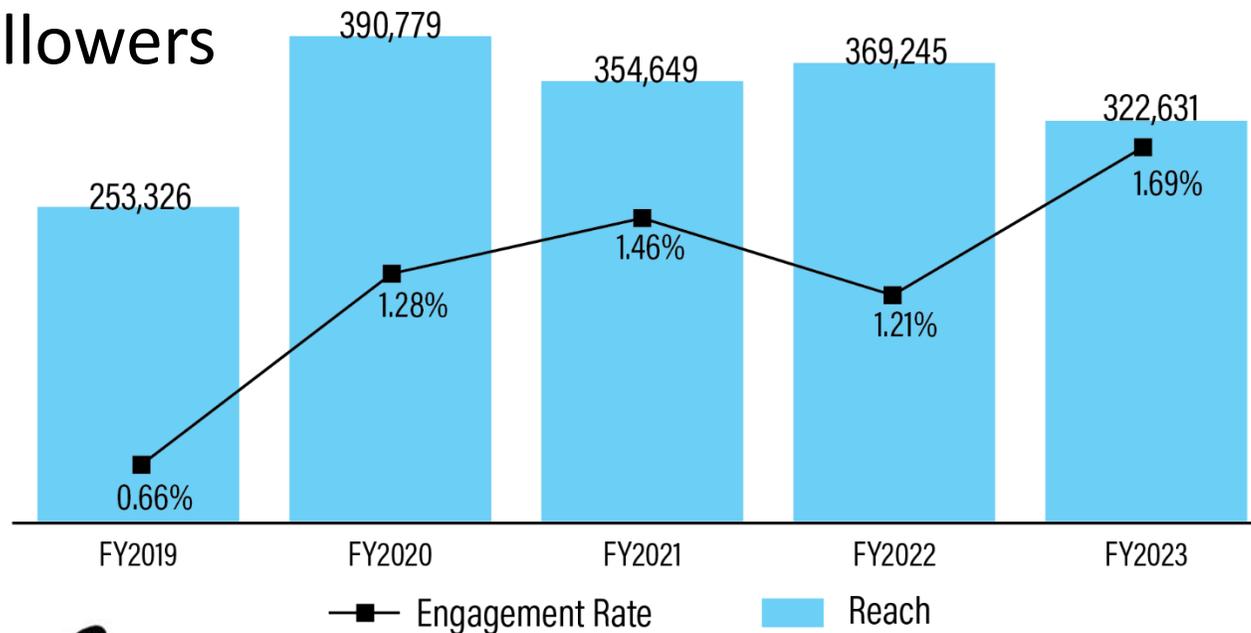
FY2020
 FY2021
 FY2022

Social Media



Twitter

- Created in February 2009
- 3,574 followers

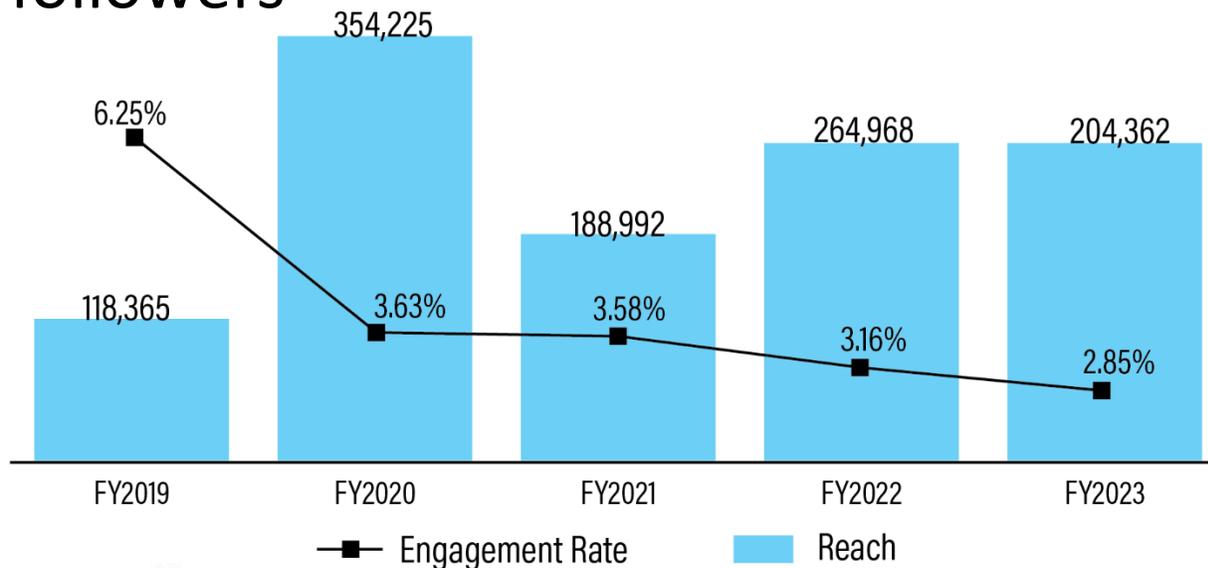


Social Media



Facebook

- Created in February 2009
- 3,132 followers



SC Department of Consumer Affairs
Published by Hootsuite • June 22

Hacked social media account? Report it to the platform. Change your password. Set up two-factor authentication. Block suspicious users. Warn your friends and followers. [National Cybersecurity Alliance](https://staysafeonline.org/online-safety.../hacked-accounts/) has info to help you regain control of your accounts: <https://staysafeonline.org/online-safety.../hacked-accounts/>

HACKED SOCIAL MEDIA ACCOUNT?

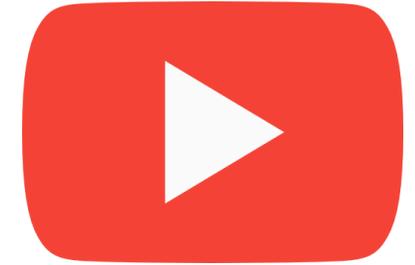
- Report it to the platform.
- Change your password.
- Set up two-factor authentication.
- Block suspicious users.
- Warn your friends, followers.

CONSUMER.SC.GOV | (800) 922-1594 | #TELLDCR

See insights and ads Boost post

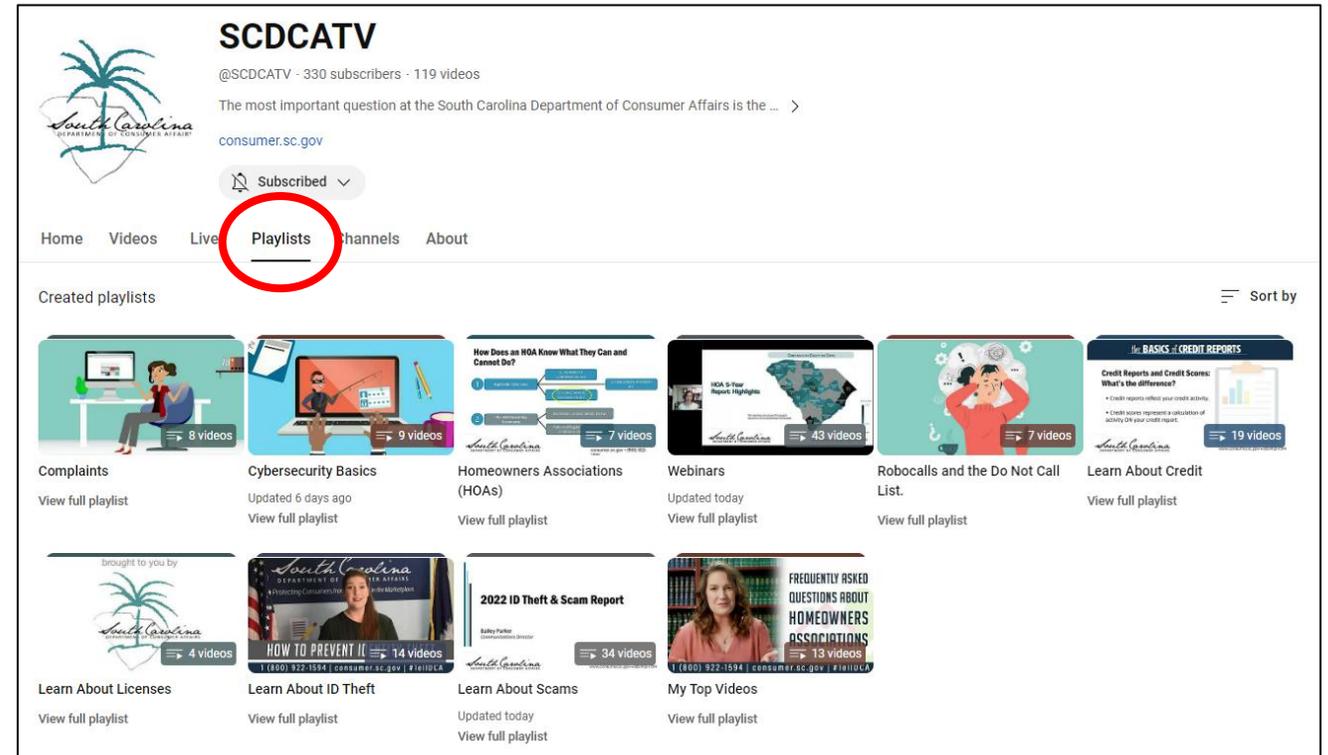
4 1 comment 42 shares

Social Media



YouTube

- Created in May 2008
- 328 subscribers
- 849 hours watched in FY23
- Uploading:
 - Webinars
 - General Education



South Carolina Residential Landlord Tenant Act: An Overview



South Carolina Residential Landlord Tenant Act: An Overview

SCDCATV 330 subscribers Subscribed 10 Share

708 views May 26, 2022
This webinar discusses the South Carolina Residential Landlord Tenant Act and the responsibilities of both the landlord and the tenant. Topics discussed include leases, landlord repairs, nonpayment of rent, and security deposits.

Chapters

0:00	2:54	4:03	5:00	6:03	8:00
Introduction	General Provisions	Leases	Landlord Obligations	Case Law Interpretation	Tenant Obligations

Preneed Funeral Contract Basics



Preneed Funeral Contract Basics

SCDCATV 330 subscribers Subscribed 1 Share Download Clip Save

55 views May 24, 2023
Funerals can be expensive and stressful. A preneed funeral contract is one way people plan and try to ease the stress of their loved ones by covering the costs of their funeral ahead of time. In this webinar hosted by the South Carolina Department of Consumer Affairs, learn about the pros and cons, different types of contracts and other helpful information before you sign the dotted line.

SCDCA resources can be accessed by going to consumer.sc.gov
Additional information on Preneed Funeral Contracts can be found at <https://consumer.sc.gov/business-reso...>

Disclaimer: This presentation is not meant to serve as a substitute for reading the various laws discussed, seeking legal counsel or otherwise requesting Department guidance and/or interpretations on the laws it administers and enforces. The presentation merely serves as an introduction and overview.

Key moments

1:04	2:08	3:19	5:29	8:25	14:04	15:56	17:09
Why purchase a preneed funeral...	Preneed Contract vs Prearrangement	Types of Preneed Contracts	Revocable vs. Irrevocable	Who can sell preneed contracts?	If I purchase an irrevocable,...	What happens if I purchase items on m...	Helpful Tips

Social Media

Next Door

- Created in October 2021
- First state agency to be active on NextDoor.
- July '23 – 293,738 people reached, 1,104 engagements
- FY23 – 4,856,290 reached, 18,743 engagements

State of South Carolina ✓
South Carolina Department of Consumer Affairs Scott Cooke • Edited 7 Jul

Education is a crucial component of our mission. Each month the South Carolina Department of Consumer Affairs holds free webinars on a variety of topics. See more...

FREE WEBINARS IN JULY

- July 12: Legislative Update 2023
- July 19: Hurricane Preparedness and Avoiding Scams Featuring SCEMD
- July 26: Five Most Common Text Message Scams

CONSUMER.SC.GOV | (800) 922-1594 | #TELLDCA

Upcoming Presentations/Webinars | Consumer Affairs
consumer.sc.gov

Posted to Subscribers of State of South Carolina

👎❤️😊 76 · 191,752 Impressions · Like · 11 Comments · Share

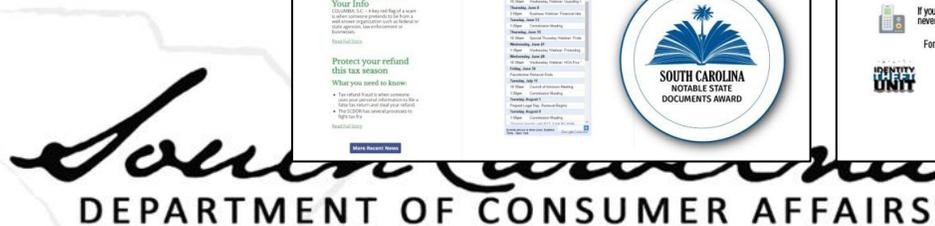
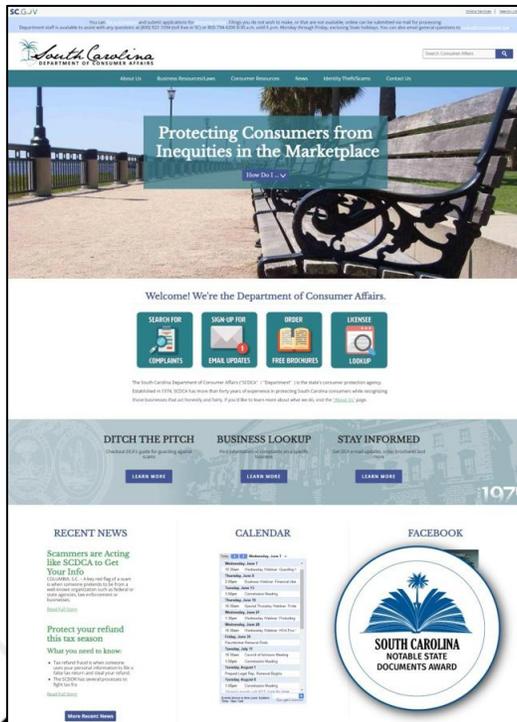
Discussion closed on 11 Jul. Learn more >



Division Successes & Challenges

Successes

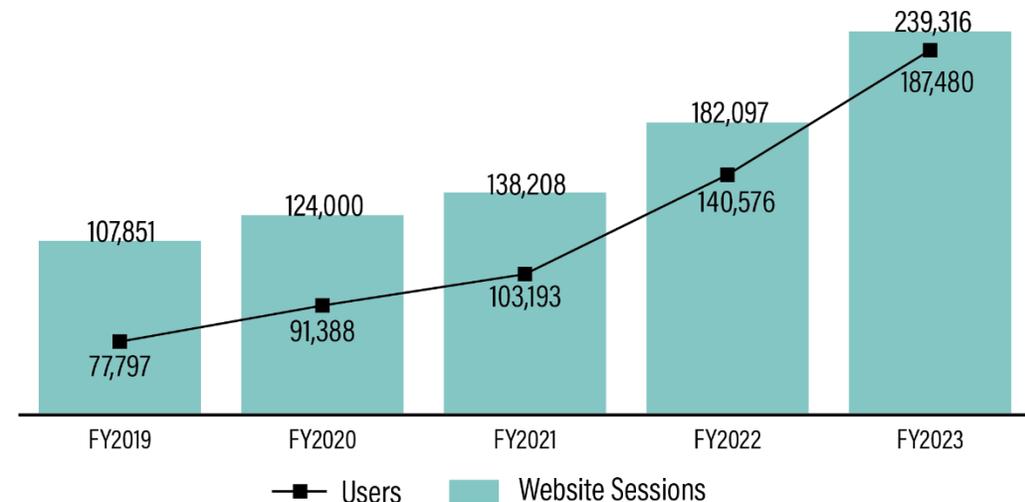
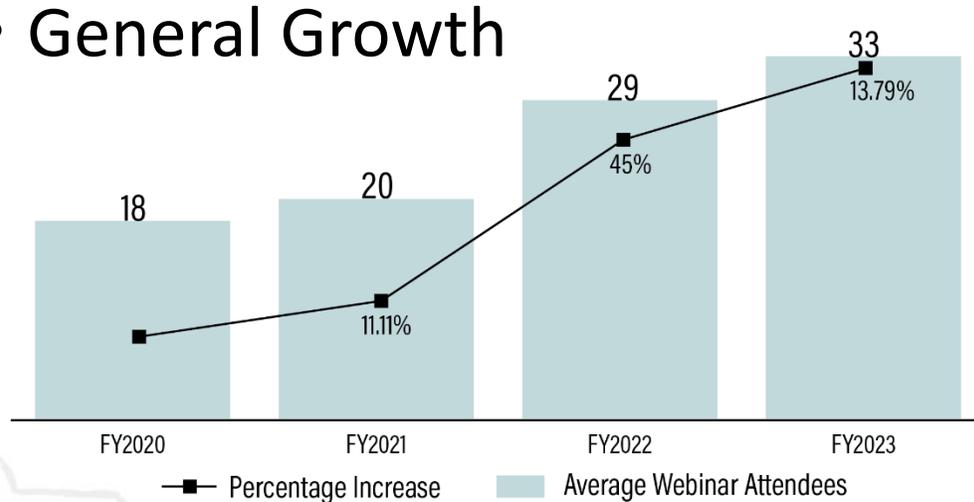
- Notable Document Awards



Division Successes & Challenges

Successes

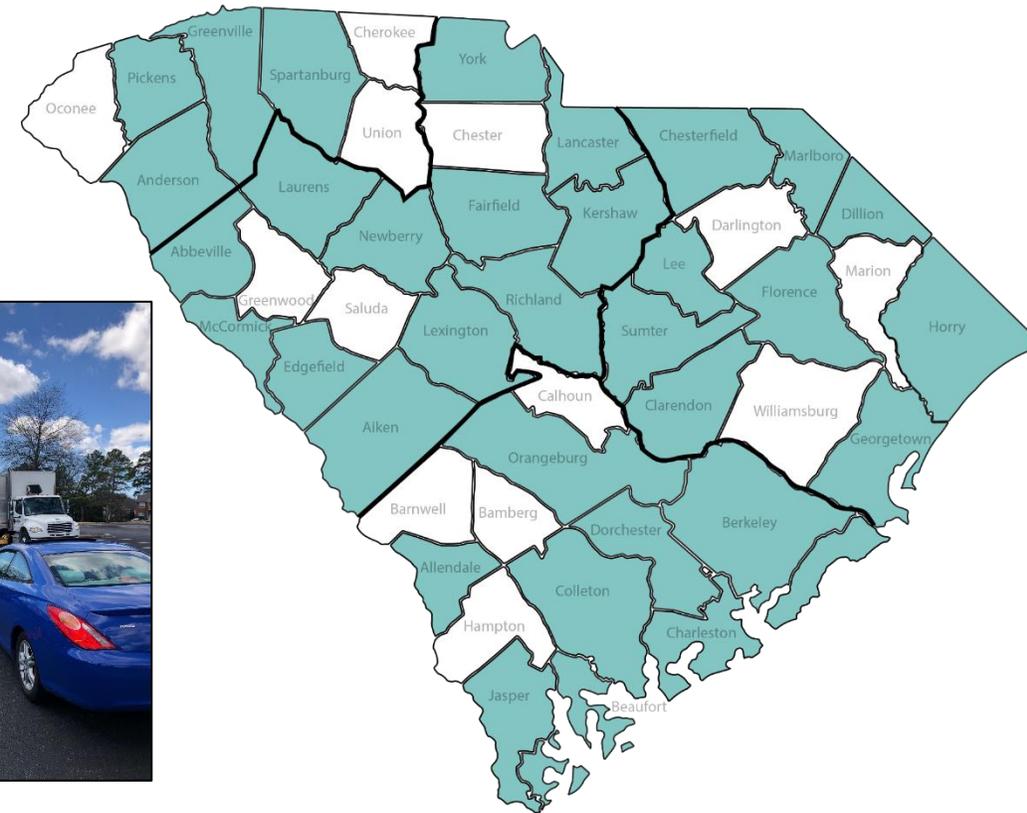
- CATE Richland One “Business Partner of the Year” Award 18-19
- Wednesday Webinar Series
- General Growth



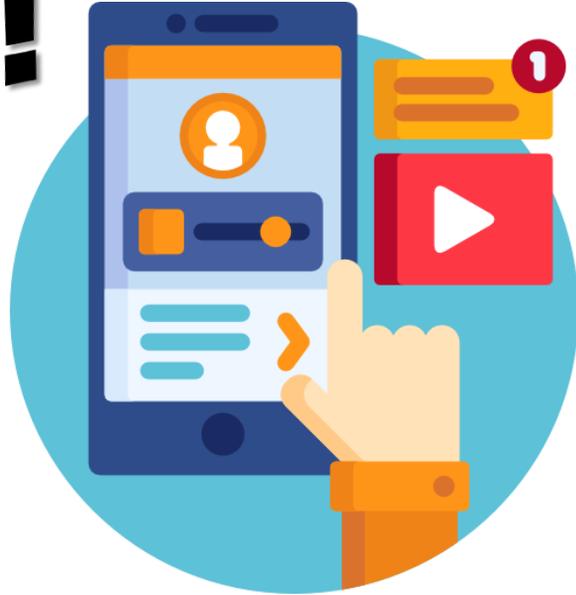
Division Successes & Challenges

Challenges

- Resources



Connect With Us!



Visit Facebook and Twitter for recent scam alerts, the latest consumer news and more educational tools.

Facebook

facebook.com/SCDepartmentofConsumerAffairs

Twitter

[@SCDCA](https://twitter.com/SCDCA)

Check out our YouTube channel for webinars and educational videos.

Youtube.com/scdcatv



Identity Theft Unit

Mandy Self
Identity Theft Unit, Director

SCDCA Identity Theft Unit - Staff

Director

Mandy Self

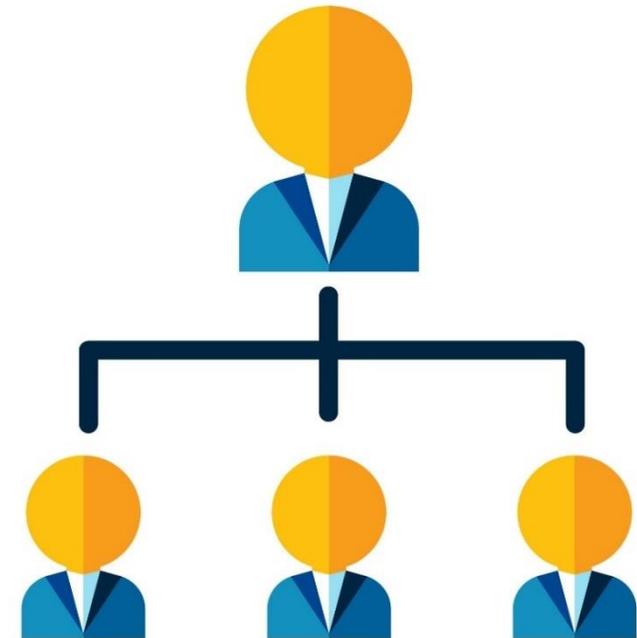
Statistical & Research Analyst

Open Position

Consumer Fraud Specialist

Melanie English

Elliott Hudson



What is Identity Theft?

Identity theft is when:

- **Someone uses your personal or financial information without your permission**
- **Commits fraud with that info.**



Difference Between Data Breach and Identity Theft



A data breach refers to the unauthorized access or release of sensitive data, whereas identity theft involves the misuse of personal information for fraudulent purposes.

SCDCA Identity Theft Unit - History



In 2008, SCDCA was charged with receiving security breach notices.

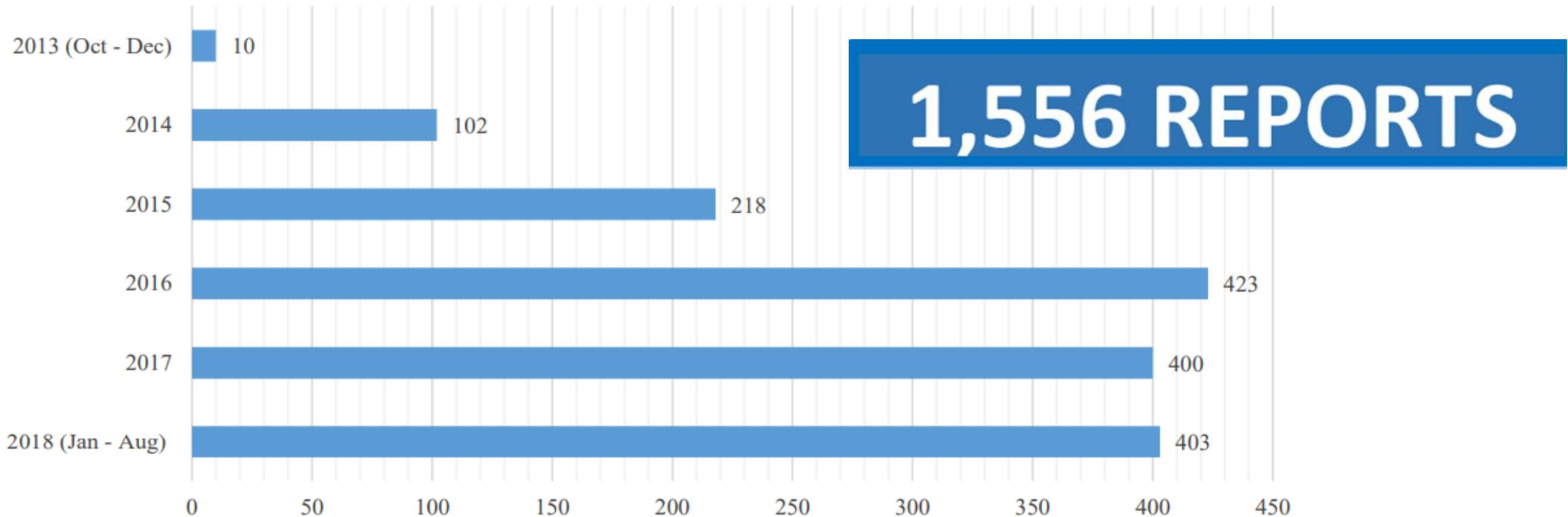
2012 represented the year with the largest number of South Carolina residents being affected by breaches.

In October 2013, SCDCA launched its Identity Theft Unit (“the Unit”/ “IDTU”).

2018 – Five Year Anniversary Special Report

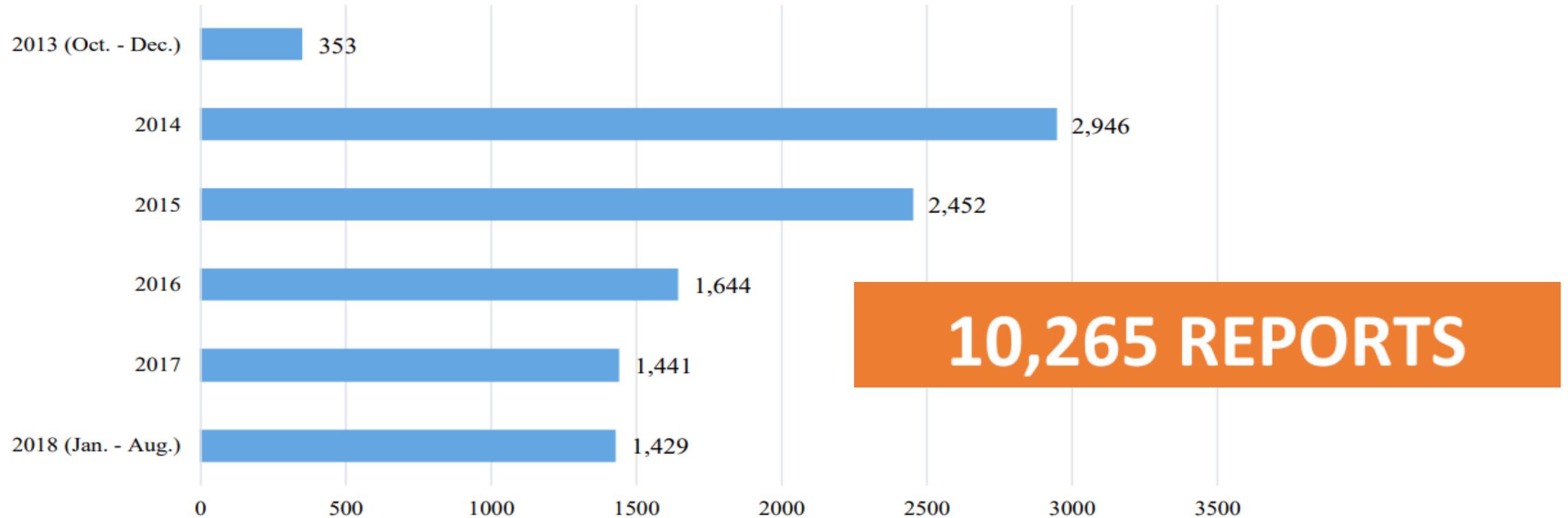
FIFTH ANNIVERSARY REPORT 2013 - 2018

TOTAL ID THEFT REPORTS RECEIVED BY YEAR



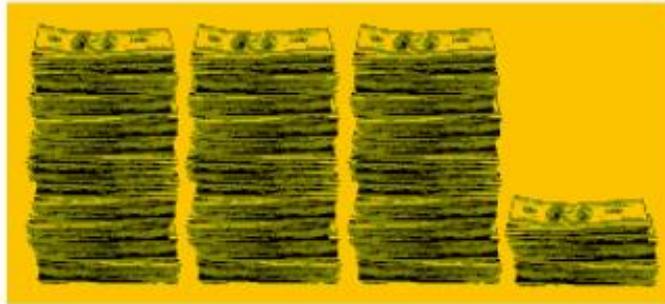
FIFTH ANNIVERSARY REPORT 2013 - 2018

NUMBER OF SCAMS REPORTED BY YEAR



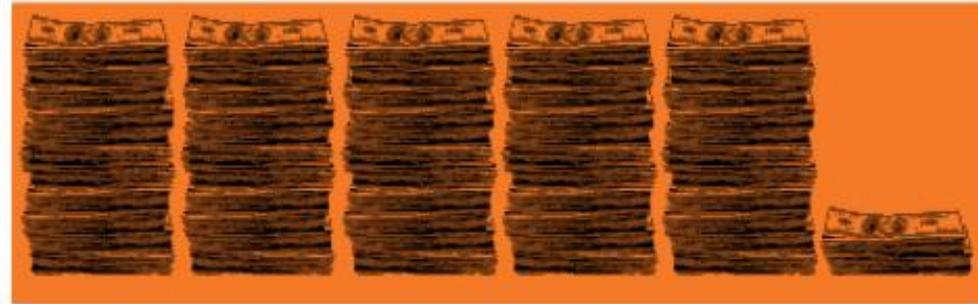
FIFTH ANNIVERSARY REPORT 2013 - 2018

\$3,250,063



**MONEY SCAMMERS
TRIED TO STEAL**

\$5,192,964



**MONEY SCAMMERS
ACTUALLY STOLE**

SCDCA Identity Theft Unit - Purpose

Education: Offer consumer education and outreach programs.

Guidance: Staff provides guidance and direction to consumers regarding identity theft issues as well as scams.



SCDCA Identity Theft Unit – Outreach

Presentations

Partnerships

- **FTC – Sentinel Network**
- **USPIS – JOLT Program**

Consumer Assistance



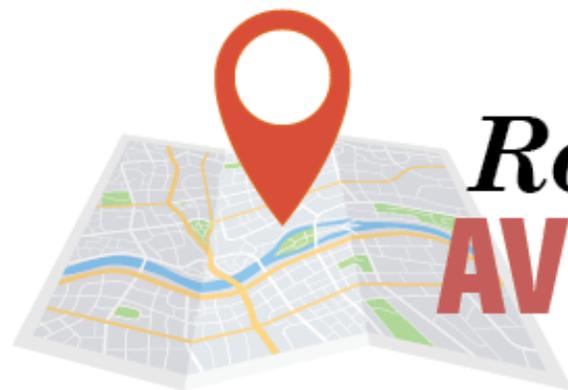
SCDCA Identity Theft Unit – Education

Avoid

Detect

Recover





Roadmap to **AVOID SCAMS**

1

Don't answer calls or respond to text messages from numbers you don't know. Block these numbers as they come in.



Roadmap to **AVOID SCAMS**

2

Don't give personal or financial information for a request that you didn't expect. Legitimate businesses don't do this.



Roadmap to **AVOID SCAMS**

3

Don't fall for high pressure tactics. Anyone who pressures you to make a decision, pay or give over personal info is a scammer.



Roadmap to **AVOID SCAMS**

4

Know the forms of payment scammers like to use. Beware of gift cards, cryptocurrency and wire transfers.



Roadmap to **AVOID SCAMS**

5

Stop and talk to someone you trust. Before you do anything, tell a friend, family member or neighbor what happened.

The Red Flags are the Same



We may not be able to know every scam out there, but if you know the red flags, you can avoid getting scammed.



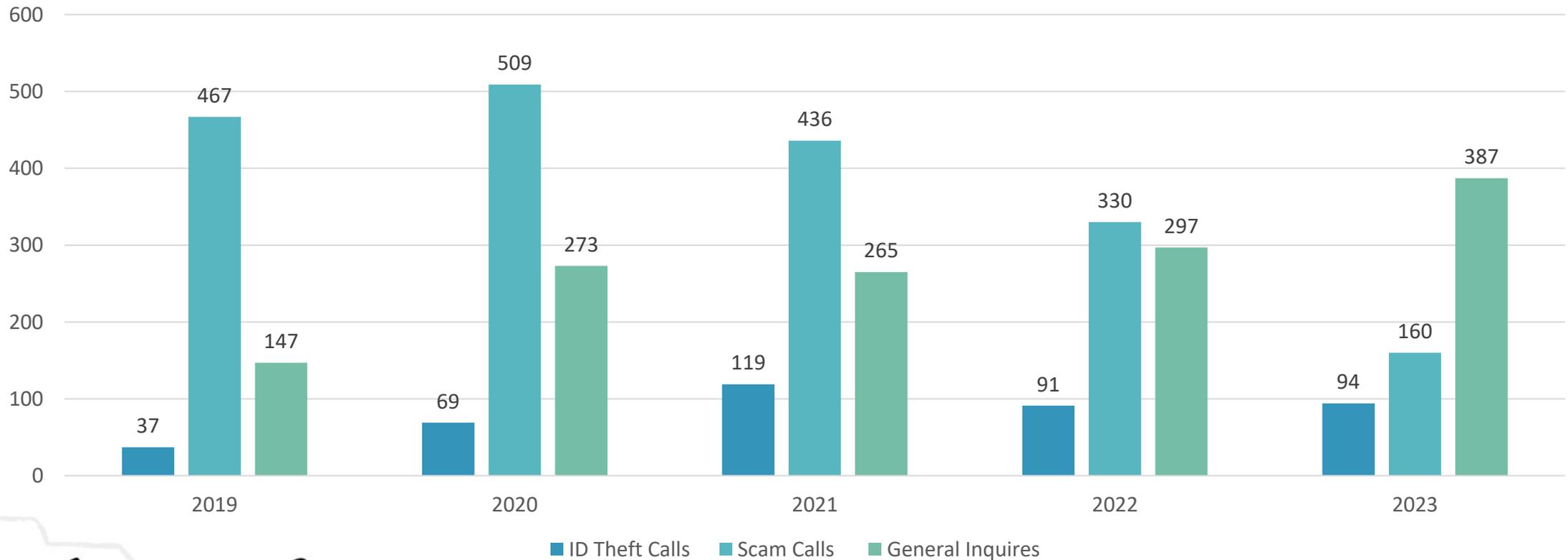
SCDCA Identity Theft Unit – Guidance

- **Scams can also lead to Identity Theft.**
- **No two cases of Identity Theft are the same so specifics are important for providing a remediation plan.**



ID Theft Unit - Phone Calls 2019 - 2023

Phone Calls by Calendar Year



Contacting the SCDCA Identity Theft Unit



Security Breach Notifications

- **ID Theft Unit staff concentrate on working directly with consumers who have received notification.**
- **We maintain the notice information on our website**



Security Breach - How to Prevent Identity Theft

A PUBLICATION OF THE SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS

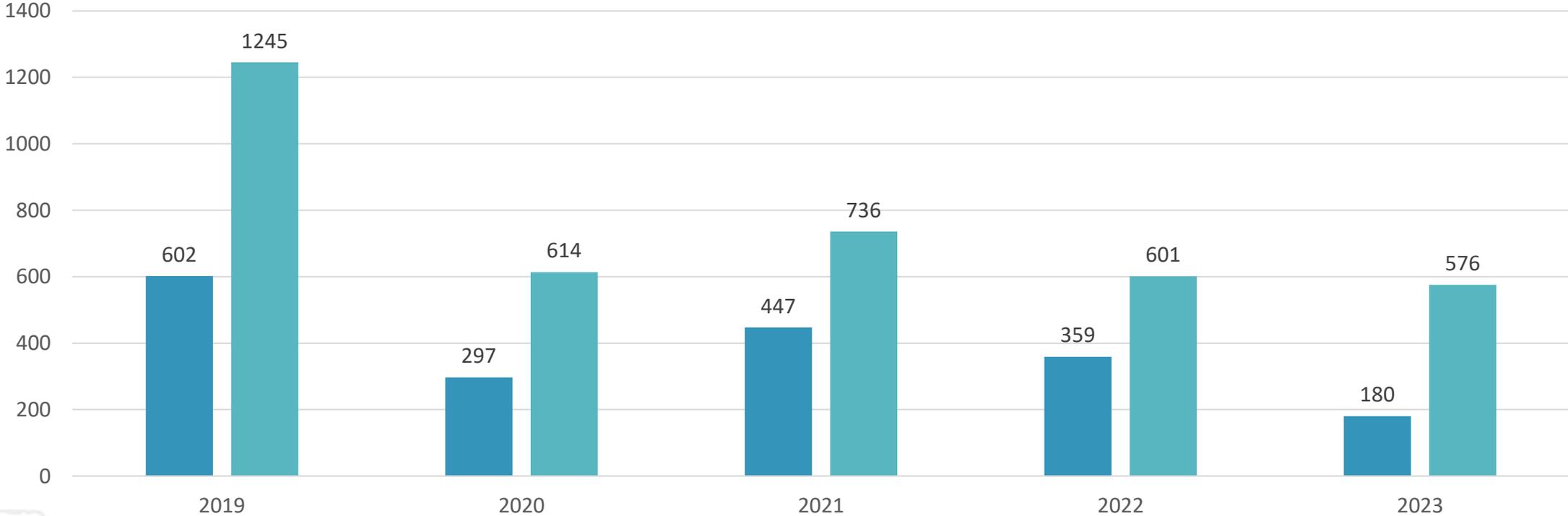
IDENTITY THEFT

WHAT TO DO AFTER A SECURITY BREACH

-  Your Information has been Breached... What Now?
Page 2
-  Fraud Alerts, Freezes and ID Theft Protection Services, Oh My! So, What's the Difference?
Page 3
-  Security Freeze FAQs, Protecting Your Child's Identity and Tools to Consider.
Pages 4-5
-  Get in the Habit: Everyday Practices that Help You Avoid Identity Theft.
Page 6
-  Are YOU a Victim of Identity Theft? What to do.
Page 7

Total ID Theft / Scam Reports 2019 - 2023

ID Theft and Scam Reports by Calendar Year



■ ID Theft Reports ■ Scam Reports

Total ID Theft Reports 1885
Total Scam Reports 3772

Total Scam Losses

Scams Reported July 2019 – June 2023

ACTUAL LOSSES

\$10,017,843

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



POTENTIAL LOSSES

\$4,541,725

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

SCDCA's Scam Form

 SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS
293 Greystone Blvd., Suite 400 | Columbia, SC | 29210
PO Box 5757 | Columbia, SC 29250-5757
www.consumer.sc.gov | 800-922-1594

 IDENTITY THEFT UNIT

SCAM REPORT FORM

You may complete this form and email to IDTheftHelp@sconsumer.gov or print and return by mail or fax.

Name Mr. Mrs. Ms. _____

Mailing Address _____ City _____

ST _____ Zip Code _____ County _____ Daytime Phone _____

Your Age Range: 17 or under 18-24 25-34 35-44 45-54 55-64 65-74 75-84 85+

Preferred Method of Contact: Mail Telephone E-mail _____

Please supply as much information as possible that the scam artist provided.

Name(s) _____

Alleged Company Name _____

Phone Number(s) 1) _____ 2) _____ 3) _____

Address _____ Email _____

City _____ ST _____ Zip Code _____ Website _____

The scammer has contacted you by (choose all that apply). Phone Internet/E-mail Mail Text

Please provide a detailed description of the scam. What did the scammer want from you? How did the scammer want you to pay? What was the scammer offering? You may attach/send additional pages.

Please check if you would to: hear from someone at SCDCA about your report?
 receive educational materials pertaining to your scam?
 receive emails on consumer issues from SCDCA?

The South Carolina Freedom of Information Act may require the Department of Consumer Affairs to release a copy of your scam report as a matter of public record.

Updated Jan. 2021

Scam Report – Example

- **Consumer's mother got involved in a romance scam with someone claiming to be from Nigeria.**
- **Wire transfers in excess of half of a million dollars over a year's time**
- **Not willing to listen to her son or law enforcement that this is a scam.**



Total ID Theft Losses

ID Theft Reported July 2019 – June 2023

ACTUAL LOSSES

\$5,891,042

This is the total amount of money reported lost due to Identity Theft.



POTENTIAL LOSSES

\$2,584,434

This is the total amount of money reported to SCDCA as money recovered through consumers remediation efforts.

SCDCA's ID Theft Form



SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS
 293 Gayles Rd., Suite 400 | Columbia, SC | 29210
 PO Box 5757 | Columbia, SC 29250-5757
www.consumer.sc.gov | 800-922-1594



IDENTITY THEFT INTAKE FORM

Please complete this form to the best of your ability if you think you are an identity theft victim. If you are not a victim but would like information about identity theft, please contact us at the number above or visit our website.

Tell Us About Yourself

Name: Mr. Mrs. Ms.

Mailing Address City

ST Zip Code County Daytime Phone

Age Range: 17 or under 18-24 25-34 35-44 45-54 55-64 65-74 75-84 85+

Preferred Method of Contact Mail Telephone E-mail

Would you like to receive emails on consumer issues from SCDCA? Yes No

Types of Identity Theft

Financial – Misuse of ATM/debit/credit cards, new credit cards, loans opened, utility accounts, misuse of checks/checking account

Tax – Someone filed a tax return with your SSN, IRS withheld part of refund, ID theft notice from the IRS

Benefits – Denied disability, public assistance, social security, unemployment benefits

Medical Care – Received bill for services you have not received, insurance policy you did not sign up for

Criminal – Warrants or citations in your name for crimes/offenses you did not commit

Other – Incorrect information on credit report, someone used your information to get a job, apartment, etc.

Identity Theft Background Questions

How did you learn you were a victim of identity theft? Credit Report Collection Notice IRS Letter Bank Notice Other:

Have you received a data security breach notice from an organization? Yes No
 If so, please list the name of the organization and the type of personal information included in the breach, e.g. name, SSN, bank account number, etc. **(Please do not list your SSN, account numbers or other personal identifying information.)**

Have you filed a police report? Yes No If yes, when?

Filed with:

Have you reported this to the Federal Trade Commission? Yes No If yes, when?

If you lost money as a result of identity theft please list the amount \$

Additional Information
 Briefly describe your identity theft issues. Please include the name(s) of company(ies) and date contacted, if applicable. **Please do not include any sensitive personal or financial information.**

READ THE FOLLOWING BEFORE SUBMITTING YOUR IDENTITY THEFT INTAKE FORM

I understand that the South Carolina Department of Consumer Affairs is not able to provide me with legal representation. I also understand that I may contact a private attorney with questions about my legal rights or responsibilities. **THE SOUTH CAROLINA FREEDOM OF INFORMATION ACT MAY REQUIRE THE DEPARTMENT OF CONSUMER AFFAIRS TO RELEASE A COPY OF YOUR IDENTITY THEFT INTAKE FORM AS A MATTER OF PUBLIC RECORD.**

Signature: Date:

What Happens Now?	Did You Know...
<p>After your form is reviewed by our ID Theft Unit we will contact you with the next steps you should take.</p> <p>Information you provide may be used to identify violations of state and federal law. As a result, the information may also be shared with other agencies or law enforcement.</p> <p>Any statistical information taken from this form (e.g. age range, city, type of identity theft, etc.) may be entered anonymously into a database to be used to educate the public about identity theft and common scams.</p>	<p>You can request a FREE copy of your credit reports annually from each of the three credit reporting agencies by calling 877-322-6228 or visiting www.annualcreditreport.com.</p> <p>Review all three credit reports closely for any information you do not recognize or that may be a result of identity theft.</p> <p style="text-align: center;"> Equifax – 800-525-6285 Experian – 888-397-3742 Transunion – 800-680-7289 </p>

Send a copy of this completed form by...

Mail: Identity Theft Unit, SC Department of Consumer Affairs, P.O. Box 5757, Columbia, SC 29250-5757
 Email: IDTheftUnit@consumer.sc.gov with the subject line: "ID Theft Intake Form"

FY2022 IDTU Accountability Goal

- **Process Identity Theft Reports within two business days of receipt.**

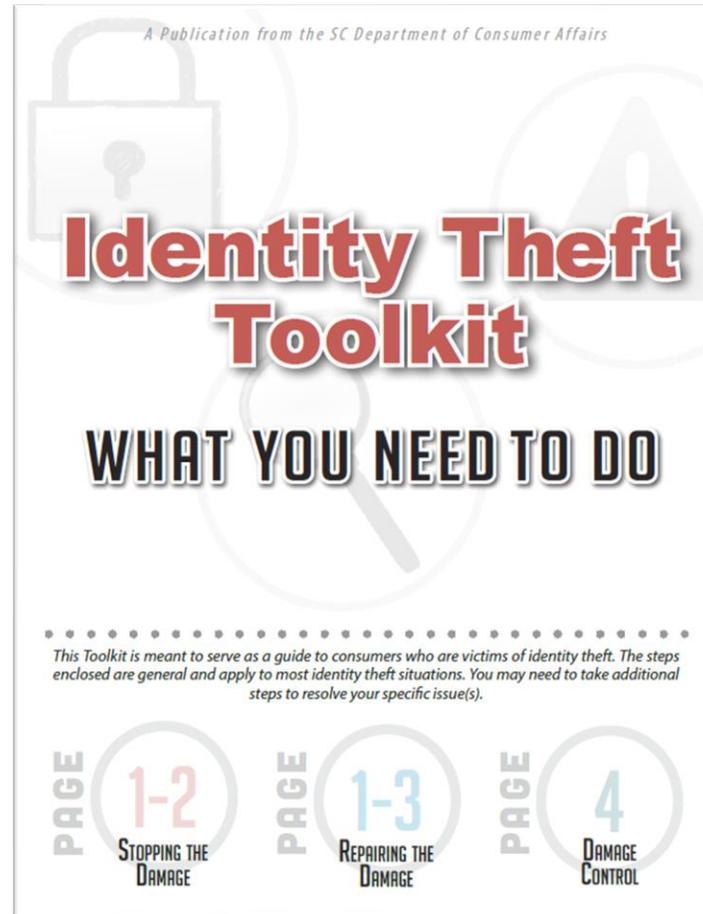
Target	Actual
95%	98%

ID Theft Report – Example

- **Consumer learned of Identity Theft when police showed up at his home with an arrest warrant.**
- **Someone had used his information to create a Driver’s License with his information.**



Identity Theft - What Next?



Identity Theft – Stop the Damage

1

REQUEST YOUR CREDIT REPORT:

AnnualCreditReport.com

The only source for your free credit reports. Authorized by Federal law.

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

Identity Theft – Stop the Damage



PLACE A FRAUD ALERT

Identity Theft – Stop the Damage

3

CONSIDER A SECURITY FREEZE

Identity Theft – Stop the Damage

4

CONSIDER MAKING AN IDENTITY THEFT REPORT

Identity Theft – Stop the Damage

- **SECTION 37-20-130. Initiating law enforcement investigation of identity theft.**
- *A person who learns or reasonably suspects that the person is the victim of identity theft may initiate a law enforcement investigation by reporting to a local law enforcement agency that has jurisdiction over the person's actual legal residence. The law enforcement agency shall take the report, provide the complainant with a copy of the report, and begin an investigation.*

Identity Theft – Repair the Damage

- Review Credit Reports
- Close Affected Fraudulent Accounts
- Correcting Errors



Identity Theft – Damage Control



LONG TERM ALERTS

Extended Fraud Alert

Active-Duty Alert

Identity Theft – Damage Control

- **Advising consumers to set up “my Social Security”**



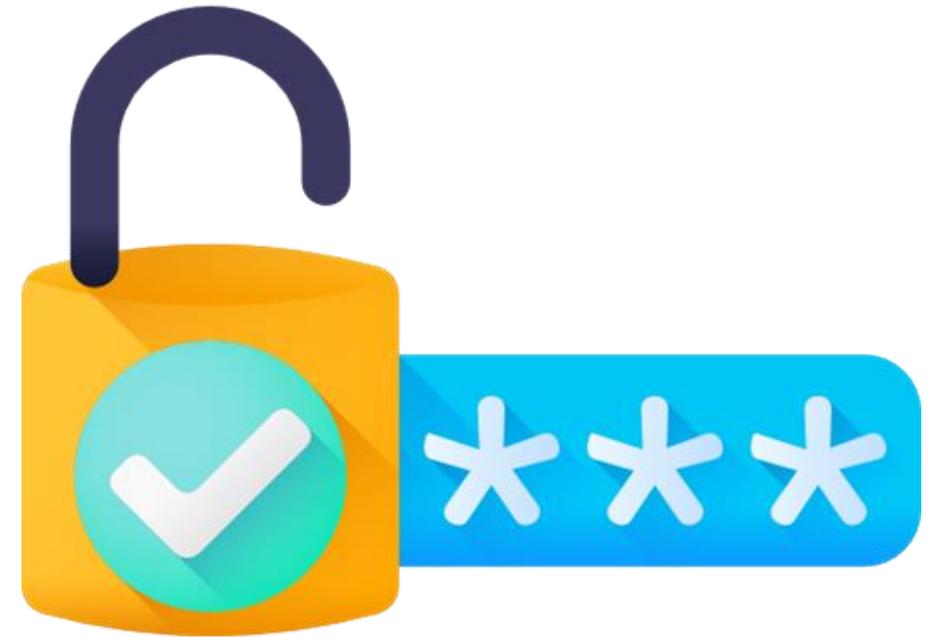
Identity Theft – Damage Control

- **Government Issued ID's**
 - **Passport**
- **State Specific Information**
 - **Driver Licenses**
- **Forms**



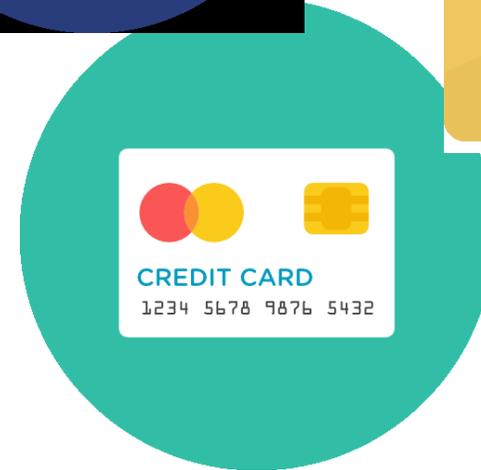
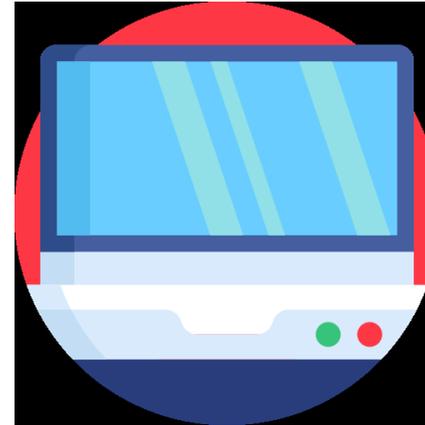
Identity Theft – Damage Control

- **Credit Monitoring Services**



Identity Theft – Damage Control

- **Be Diligent and Monitor**
- **Be Suspicious and Follow-up**



Protecting Consumers from Inequities in the Marketplace

How Do I ... ▾

- [File a complaint?](#)
- [Get a license?](#)
- [Background a business?](#)
- [Report identity theft?](#)
- [Report a scam?](#)
- [Request a presentation?](#)

[Home](#) » [Identity Theft Unit](#) » ID Theft

ID Theft

Avoid. Detect. Recover.

Identity theft can happen to anyone. The South Carolina Department of Consumer Affairs' Identity Theft Unit ("the Unit") aims to inform consumers about the steps they can take to protect themselves from identity theft, how to spot if they are a victim and provide tailored remediation and guidance to identity theft victims. Think someone is using your personal information to commit identity theft, submit an [ID Theft Intake Form \(PDF\)](#). Looking for the Unit to come to your community? [Request a presentation \(PDF\)](#).

Find the most up-to-date resources at your disposal for avoiding, detecting and recovering from identity theft below. Whether you are a victim of identity theft or want to be a savvy consumer, this is the place to be.

▼ How to Report...

▼ Worried about Identity Theft?

▼ Worried about Child Identity Theft?

▼ Elder Fraud

▼ Was Your Information Lost or Stolen?

▼ Sample Letters

Helpful Links



Questions?

(800) 922-1594
Toll Free in SC
(803) 734-4200

293 Greystone Blvd.
Suite 400
Columbia, SC 29210



[Home](#) » [Identity Theft Unit](#) » Scams

Scams

Report Scams to DCA

You can report by calling 1 (844) TELL-DCA (835-5322), and clicking [Report a Scam \(PDF\)](#).

Looking for the Identity Theft Unit to come to your community? [Request a presentation](#).

Why report a scam?

When consumers report scams, it helps stop others from falling victim to the same scams. Education is central to the Department's mission and as such we are committed to educating consumers about the latest scams. Please take a moment to tell DCA if you've gotten a scam call, email, text, etc.-- even if you didn't fall victim to the scam.

Resources for Consumers

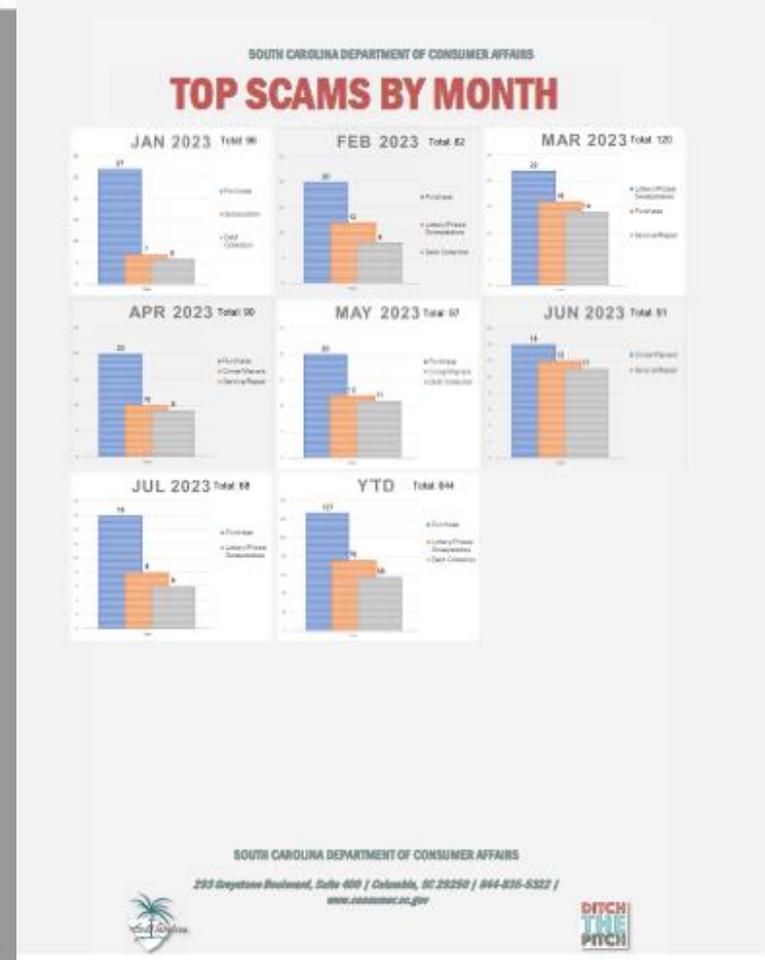
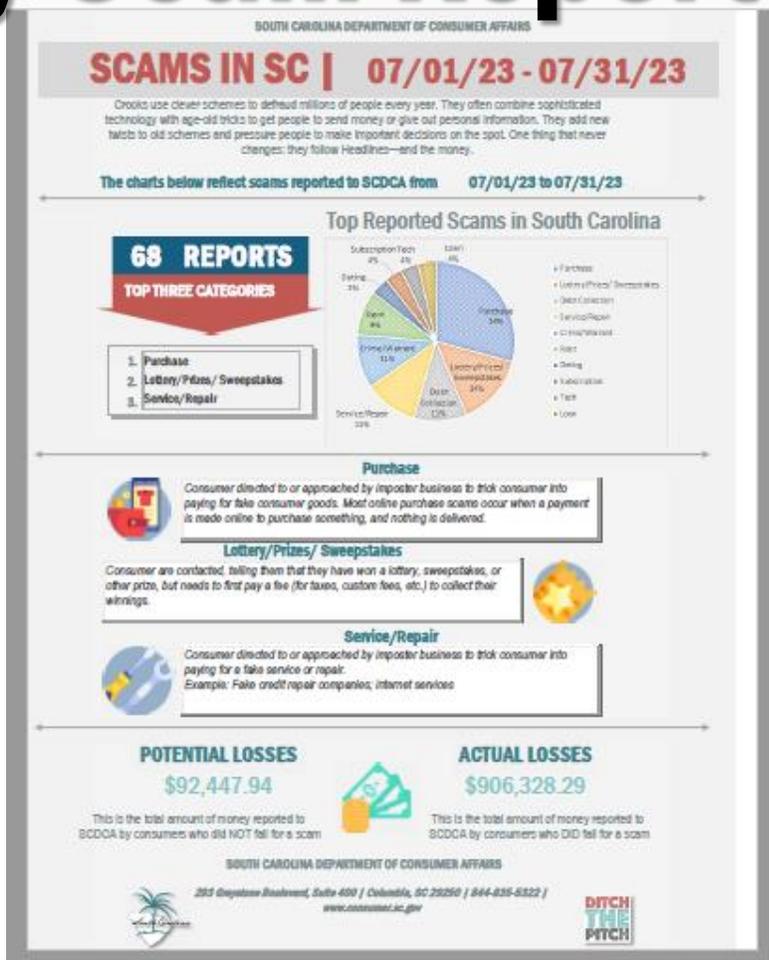
| [Scam Education](#) | [Scam Reports](#) | [Ditch the Pitch Scam Guide \(PDF\)](#)

Helpful Links



Questions?

Monthly Scam Report



Scam Education

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.

DITCH THE PITCH
a guide to guarding against scams

[Click here to download](#)



"Ditch the Pitch: A Guide for Guarding Against Scams" is meant to help you get ahead of the fraudsters. Education has always been a large part of the SCDCA's mission. We get that navigating the ever-changing marketplace can be overwhelming. With the rapid development of technology, scammers are more active (and more successful) than ever. This is why SCDCA created this guide; the best part is all education SCDCA provides is completely free!

Common Scams

- ▼ [Charity Scams](#)
- ▼ [Dating/Romance Scams](#)
- ▼ [Free Prize, Lottery & Sweepstakes Scams](#)
- ▼ [Job Scams](#)
- ▼ [Online Shopping](#)
- ▼ [Phishing](#)
- ▼ [Phone Scams](#)
- ▼ [Property/Real Estate Scams](#)
- ▼ [Repair Scams](#)
- ▼ [Scholarship & Financial Aid Scams](#)
- ▼ [Tax Scams/Fraud](#)
- ▼ [Utility Scams](#)

Helpful Links



Questions?

Bailey Parker
Communications Director
(803) 734-4296

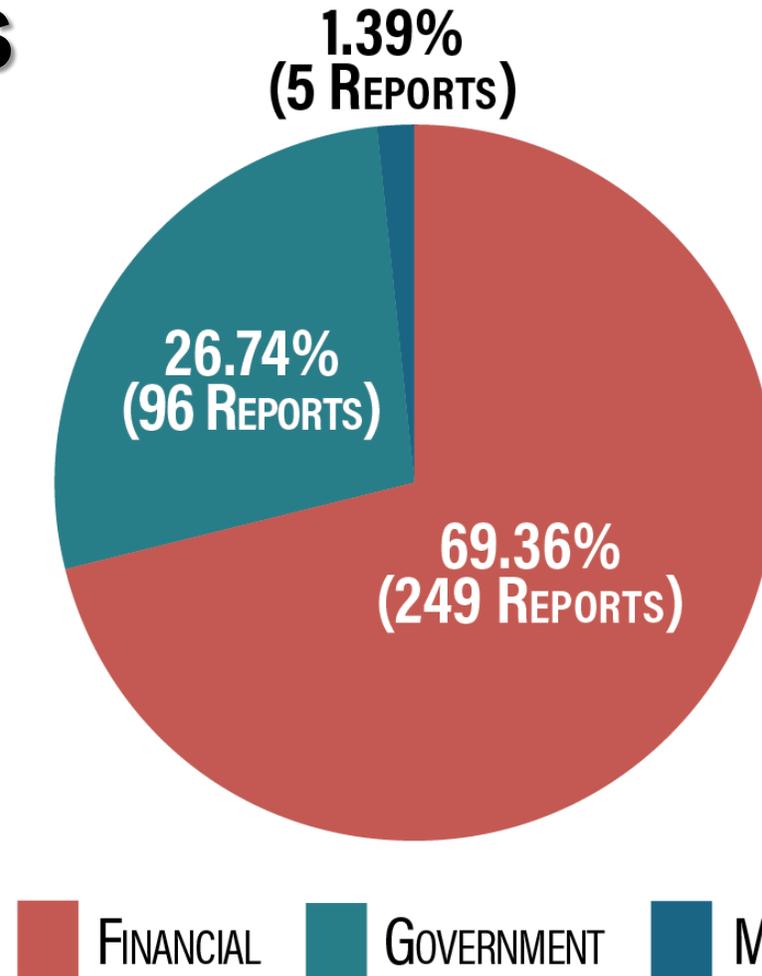
(800) 922-1594
Toll Free in SC
(803) 734-4200

Annual ID Theft and Scams Report

This report shows the data collected in the Identity Theft Unit in the calendar year.



ID Theft Reports



ID Theft Reports

359 REPORTS

TOP THREE CATEGORIES

-19.14%

1 Financial

2 Government

3 Medical



Financial

Financial ID theft includes the misuse of existing ATM/debit/credit cards or checks/checking accounts, or opening new credit cards, loans, or utility accounts using someone else's identifying information.



Government

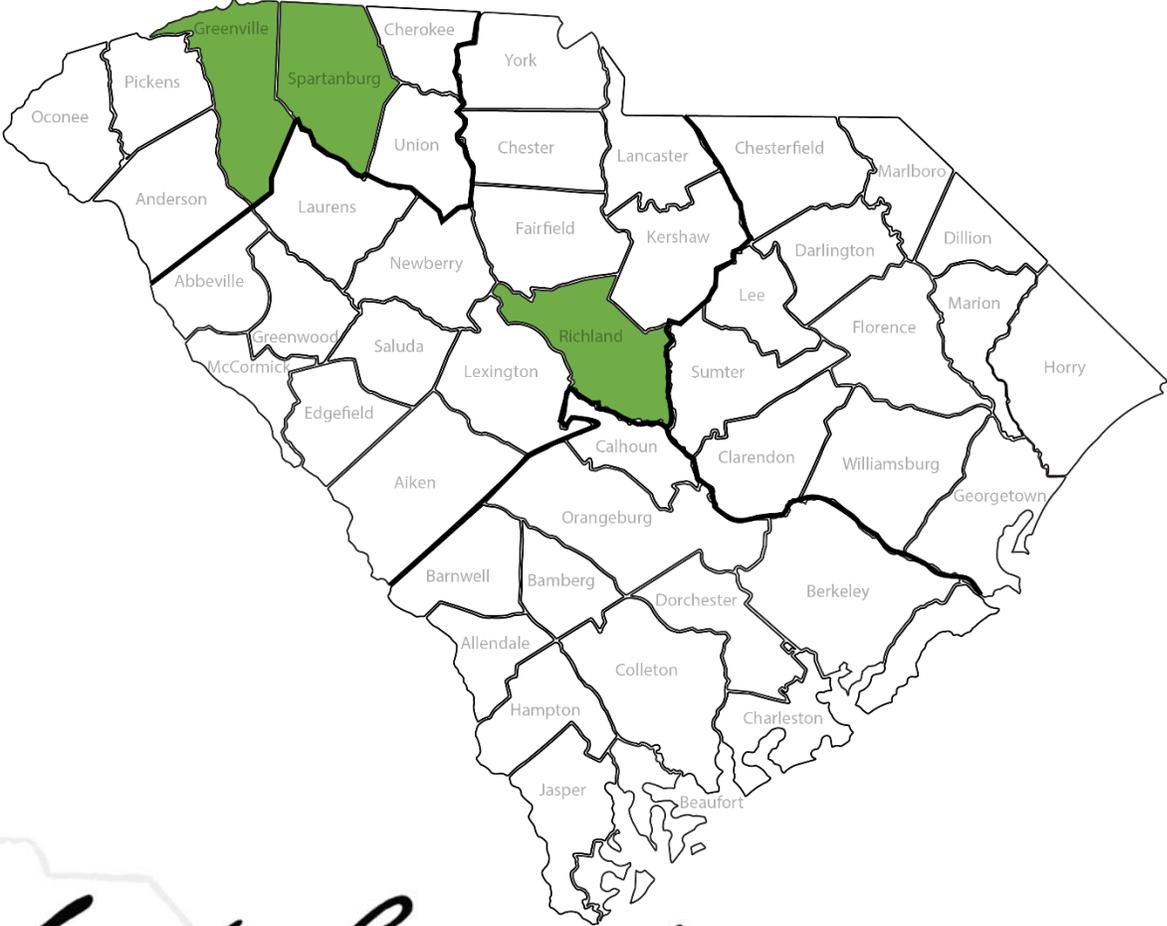
Government ID theft includes tax fraud, being denied disability, public assistance, social security, unemployment benefits and license related fraud.



Medical

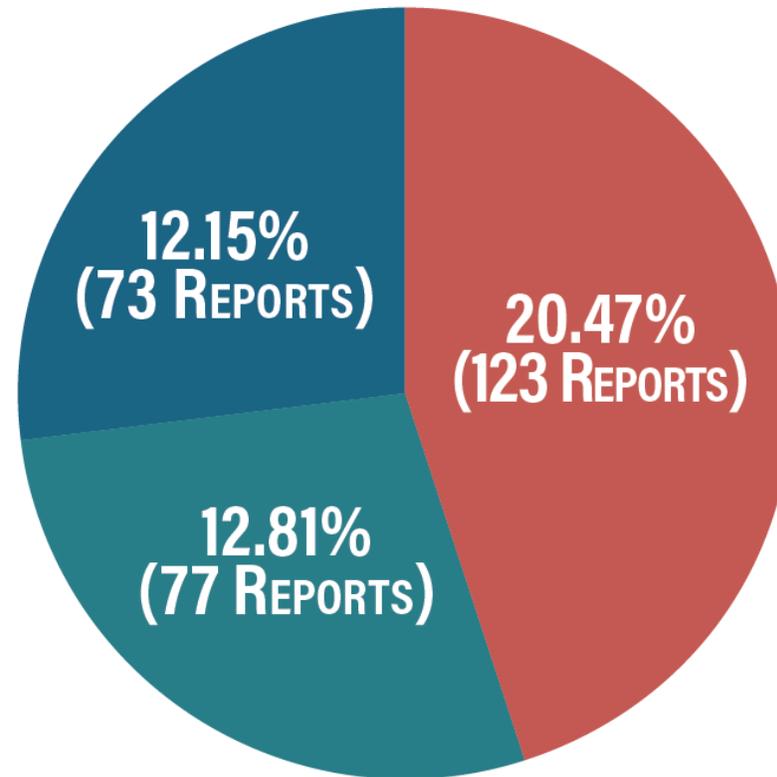
Medical identity theft is when someone steals or uses your personal information (like your name, Social Security number or Medicare number), to submit fraudulent claims to Medicare and other health insurers without your authorization.

Top Three Counties to Report ID Theft



Richland – 41
Greenville – 38
Spartanburg – 32

Scam Reports



Scam Reports

601 REPORTS

TOP THREE CATEGORIES

-18.56%

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



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.

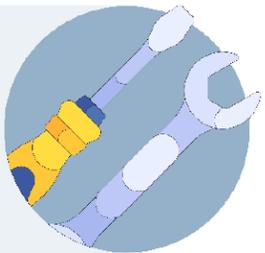


Lottery/Prizes/Sweepstakes

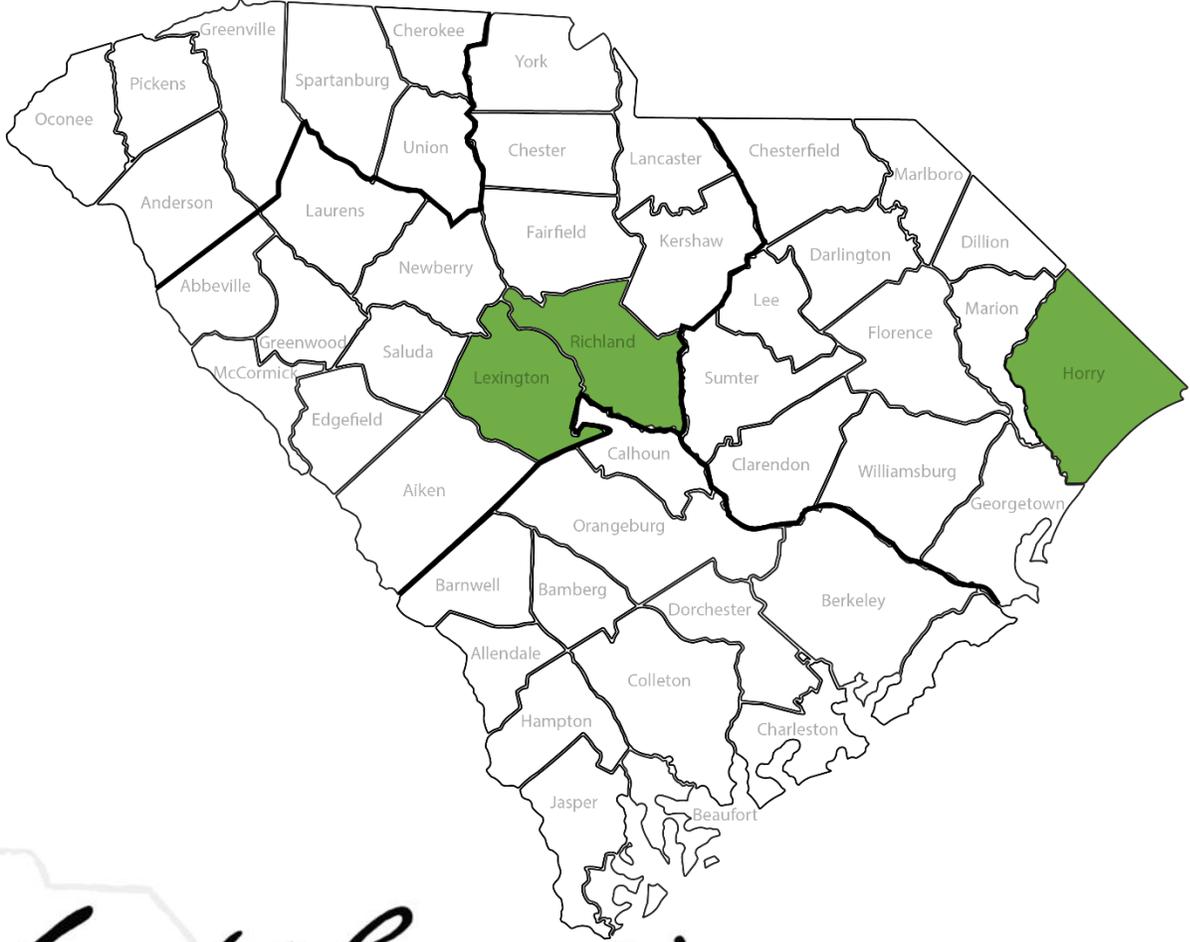
Consumer gets call, email, mail, telling them that they have won a lottery, sweepstakes, or other prize, but needs to first pay a fee (for taxes, custom fees, etc.) to collect their winnings. Examples: Publishers Clearinghouse; foreign lottery.

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.



Top Three Counties to Report Scams



Richland – 61
Lexington – 53
Horry – 53

ID Theft Unit Successes

Existence

Response Times

Agency Relationships

ID Theft Unit Challenges

Data Technology

Staffing

Expectations v. Limitations



AGENCY SUPPLEMENTAL DOCUMENTS



CREDIT REPORTS: What they are and why the matter.



CREDIT REPORTS

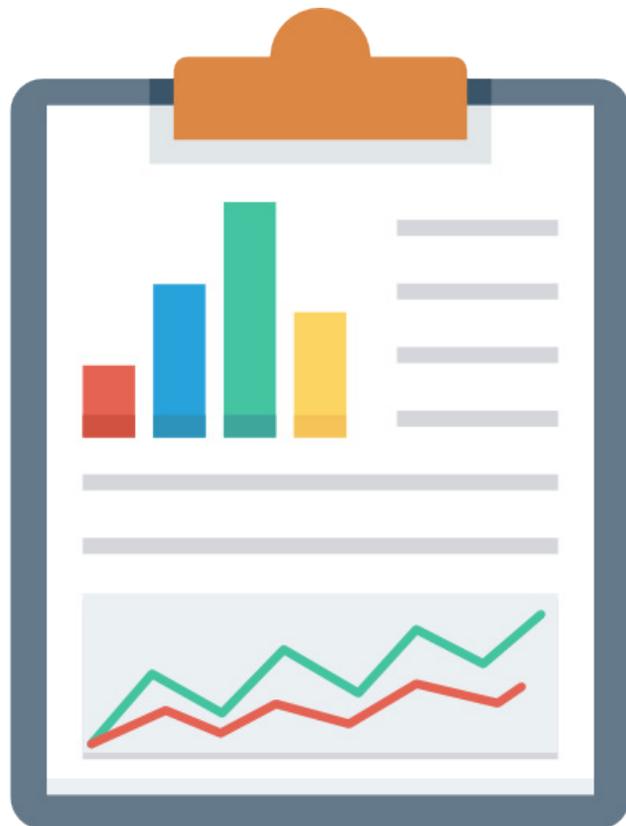
What they are and why they matter.



- [Horizontal bar]
- [Horizontal bar]
- [Horizontal bar]
- [Horizontal bar]

TABLE OF CONTENTS

Credit Report Basics	1-2
Reading Your Credit Report	3
Credit Scores	4-5
Common Credit Myths	6-7
Credit Counseling	8
Watch Out for Scams!	9
Keep Your Information Safe	10-11
Credit Report Checklist	12-13



WHAT IS A CREDIT REPORT?

A credit report is a detailed record of how you've managed your credit over time. The more positive information you have in your credit report, the better your credit options will be.

What is a creditor? A business who gives you money, goods or services that you can pay for over time.

WHAT INFO IS IN MY CREDIT REPORT?

Credit reporting agencies (Experian, TransUnion, Equifax) get information from creditors and public records and compile it into a credit report.

Personal information

- Your name and any name you may have used in the past
- Current and former addresses
- Birth date
- Social Security number
- Phone numbers

Credit accounts

- Current and past credit accounts, including the type of account
- The credit limit or amount
- Account balance
- Account payment history
- The date the account was opened and closed
- The name of the creditor

Public records

- Liens
- Civil suits and judgments
- Bankruptcies

Inquiries

- Hard - You applied for credit, which affects your score.
- Soft - When you or a current creditor check your report. Also, when potential creditors check your report for pre-approval offers. No affect on your credit score.

HOW IS MY CREDIT REPORT USED?

Credit reports are commonly used to determine whether to provide you with credit and how much you will pay for it. Credit is often pulled by creditors and other businesses when you apply to:



- Buy a home
- Set up utility accounts
- Buy a car
- Borrow money
- Get a job
- Rent an apartment
- Buy insurance
- Get a credit card

HOW DO I GET MY CREDIT REPORT?

By law, you're entitled to a free copy of your credit report from each of the three major consumer credit reporting agencies — Equifax, Experian and TransUnion — once every 12 months.

To order, visit
annualcreditreport.com
or call 1 (877) 322-8228.

You can request all three reports at once or you can order one report at a time, spaced throughout the year. There are other times when you may get a free credit report, see page 6 for more details. Already claimed your free reports? A credit reporting company can charge no more than \$12.50 for a credit report.



Tip: Make a habit of pulling your credit report by doing it on the same day every year like your birthday, anniversary, etc.

WHY SHOULD I CHECK MY CREDIT REPORT?



The South Carolina Department of Consumer Affairs suggests that you review your credit report at least once a year. Why?

- **To make sure the information is accurate, complete, and up-to-date.** This way, you know what's on the report and have time to fix errors before you apply for a loan for a major purchase, buy insurance or apply for a job.
- **To help find signs of possible identity theft.** Identity thieves may use your information to open new credit accounts in your name. Then, when they don't pay the bills, the unpaid accounts are reported on your credit report.

WHAT SHOULD I CHECK ON MY CREDIT REPORT?

Go through your credit report with a fine-tooth comb. For a full check-list go to pages 12-13. Here are some areas that have common errors:

Personal Information:

- Make sure all of your personal information is correct including: name, social security number, phone number, previous addresses, marital status and employment history.

Account Information:

- Are the accounts on the list showing the right status? *Examples: open, closed, never late or late in collections.* Are all of the balances and credit limits correct?
- Are the dates listed in each account right? Make sure to look at the date opened, when the last payment was made and the date of the first late payment.
- Are there any accounts you don't recognize or show up more than once?

Find Any Errors?:

- If you found incorrect information, you can dispute it. Your credit report gives directions on how to submit a dispute.
- Do you suspect that you have been the victim of identity theft? Call our Identity Theft Unit at (844) 835-5322 or fill out an [identity theft form](http://www.consumer.sc.gov) at www.consumer.sc.gov.

CREDIT SCORES

WHAT IS A CREDIT SCORE?

A credit score is a three-digit number designed to predict if you will pay your bills on time. Higher credit scores generally result in better credit terms and more options.

HOW DO I BOOST MY CREDIT SCORE?

There is no quick fix to improving your credit score. In order to boost your credit score, you need to improve your credit report. Here's how to start:



CREDIT SCORE RANGES*

300-579 – POOR
580-669 – FAIR
670-739 – GOOD
740-799 – VERYGOOD
800-850 – EXCELLENT

*These ranges are general numbers, not a strict representation of every score range.

BILLS



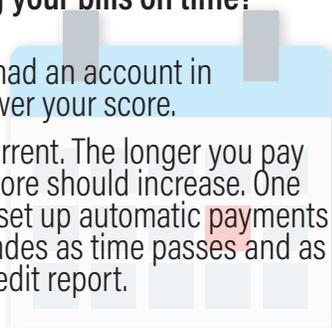
Pay your bills on time.



Not paying your bills on time?

If your credit report shows that you paid bills late, had an account in collections or declared bankruptcy, it is likely to lower your score.

If you've missed payments, get current and stay current. The longer you pay your bills on time after being late, the more your score should increase. One way to make sure your payments are on time is to set up automatic payments or reminders. The impact of past credit problems fades as time passes and as recent good payment patterns show up on your credit report.



CREDIT HISTORY & TYPES OF CREDIT



Long history of good credit.



Haven't had credit for long/no mix.

Lack of credit history may affect your score negatively, but factors like timely payments and low balances can level that out. The more your credit report shows you paying on time, the more info there is to show you know how to handle credit.

A mix of credit types, including long-term loans (A car or mortgage), revolving accounts (Credit cards) and short-term loans (Personal loans) that you pay on-time also show a creditor you are a low-risk.

APPLICATIONS



Few applications.



Applying for a lot of new credit.

If you recently applied for too many new accounts, like credit cards, it could lower your score. It may lead creditors to think you can't pay what you owe or stick to a budget. Take your time and think about whether you can afford another bill to pay, or even if you need the new credit at all. Watch out for store credit card offers. The cost to your credit may outweigh any discounts.

CREDIT LIMITS



No or low balance on cards.



You've maxed out your credit.

Part of your credit score depends on your credit utilization ratio. You can get your ratio by dividing your total credit card balances by your credit limits. You want to keep your credit utilization under 30%.

If the amount you owe is close to your credit limit, it's likely to have a negative effect on your score. Try to keep your balances low compared to your total credit limit. Paying off the balance each month helps get you the best scores.

COMMON CREDIT MYTHS

MYTH: CHECKING MY CREDIT REPORT WILL HURT MY CREDIT SCORE.

Fact: Getting your credit reports will not hurt your credit scores, and can be an important tool to make sure your information is accurate and up-to-date. Reviewing your credit reports regularly gives you an opportunity to quickly identify and fix any errors.



MYTH: GETTING LOAN ESTIMATES FROM MULTIPLE LENDERS WILL HURT MY SCORE.

Fact: Shopping around for credit and comparing offers can help you find the best rates. For auto loans and mortgages, credit scoring models view multiple credit report inquiries made in a certain time frame as just one. For other types of credit applications, it will impact your score. Do your research before you apply to find the best fit for you.



MYTH: I ONLY HAVE ONE CREDIT SCORE.

Fact: You have multiple credit scores. Often, the score you see isn't the same one the creditor sees.

Your score depends on the scoring model, the type of credit you're seeking and even the day when it's calculated. It's normal to see slightly different numbers throughout the year and from different sources.



MYTH: CARRYING A BALANCE ON MY CREDIT CARDS WILL IMPROVE MY CREDIT SCORE.

Fact: Paying off your credit cards in full every month is the best way to improve a credit score or maintain a good one.



MYTH: I HAVE TO PAY TO GET MY CREDIT REPORTS.

Fact: You're entitled to one free copy of your credit report every 12 months from each of the three major credit reporting companies (See page 2).

You're also entitled to a free report if you're unemployed and plan to look for a job; if you're on welfare; are denied employment/credit or if your report is inaccurate because of fraud, including identity theft.

MYTH: CLOSING CREDIT ACCOUNTS WILL IMPROVE MY CREDIT SCORE

Fact: Closing a credit card account can help you manage your spending and protect from identify theft if you're not using the account. It may make sense for your financial situation, but don't assume it will improve your credit scores.

If you close some credit card accounts, but hold the same balance, you'll be using a higher percentage of your total credit limit, which could lower your scores.

MYTH: THERE ARE ONLY THREE CREDIT REPORTING COMPANIES.

Fact: Equifax, Experian, TransUnion are the three nationwide credit bureaus. But, there are also hundreds of other consumer reporting companies.

The other kinds of credit reporting companies compile and provide information used for purposes like employment, tenant screening, insurance, utilities, etc.

All consumer reporting companies offer a free copy of your report every 12 months.

SHOULD I HIRE A CREDIT COUNSELOR?

If you think you need help managing your credit, you may consider hiring a credit counselor. But first:

Are they licensed?

- Credit counseling includes debt management, debt settlement/negotiation and credit repair.
- People offering and providing credit counseling services to South Carolinians must be licensed with SCDCA.
- To see if a counselor is licensed, visit consumer.sc.gov.

Do your research.

- Check online for reviews/complaints on SCDCA's complaint portal or with the Better Business Bureau.
- Research the qualifications of the company and its employees.
- Determine if the services offered fit your budget and needs.
- Find out what the services cost.

Know Your Rights.

- Credit counselors must provide a financial education program and analyze your budget to make sure the program is right for you.
- They must provide you with a completely filled-in contract, no blank spaces.
- If the credit counselor is paying your creditors, they must send you an account statement every three months.

Remember: You can cancel at any time by giving a 10 day written notice and the credit counselor cannot charge you for cancelling.

Credit counselors and organizations CANNOT:

- Charge you more than what the law allows. Call or visit SCDCA's website to find out the current fee caps. For example, credit repair companies cannot charge you more than \$50/month.

If you'd like to file a complaint against a credit counselor, visit consumer.sc.gov, click "How do I..." and then "File a Complaint."

Credit problems? No problem!

We can erase your bad credit — 100% guaranteed.

**WE CAN REMOVE BANKRUPTCIES, JUDGMENTS, LIENS,
AND BAD LOANS FROM YOUR CREDIT FILE FOREVER!**

CREATE A NEW CREDIT IDENTITY — LEGALLY.

Don't believe these claims: they're very likely signs of a scam.

The truth is you can dispute errors in your credit report for free. You don't need to pay a credit repair organization to do it.

RED FLAGS OF A CREDIT REPAIR SCAM

If you choose to get help, watch out for these red flags:

• Pressures you to pay up-front fees.

A simple rule to follow is "Don't pay upfront."

• Promises to remove ALL negative information from your credit report.

No one can do this if the information is accurate and current.

• Tells you to not contact credit reporting companies or creditors.

Again, you can dispute your credit report directly with credit reporting companies and creditors for free. If you just signed up for a credit repair service, you have the right to cancel the contract within three business days at no charge.

KEEP *your* INFORMATION SAFE

Take these four free steps to keep your personal information safe from fraudsters:

1 CONSIDER A SECURITY FREEZE & FRAUD ALERT

Prevent scammers from opening new accounts using your information by placing a **FREE** security freeze on your credit reports. A security freeze puts your credit report on lockdown, limiting access to it without your OK, and lasts until you lift it.

A fraud alert will allow a business to pull your credit report, but only after taking extra steps to verify the applicant is really you.

2 MONITOR YOUR STATEMENTS

Make sure your bills and benefits, medical and financial statements are arriving on time and are correct. Identity thieves can use your info, like a social security number, the same way you do. Including to get:

- Government benefits
- Cell phones/utilities
- Tax refund
- Driver's license/ID
- Medical benefits
- A job

3 DEFEND AGAINST SCAMS

Scam artists use information from breaches to make their requests seem legit. Never reply to calls, texts, pop-ups, or e-mails that ask you for, or to verify, personal information.

Fraudsters may even pose as a monitoring service and send emails with subject lines or content like: "Identity Theft Alert" or "Your Score Has Dropped." Avoid clicking on links or downloading attachments from suspicious emails or texts.

4 INTERESTED IN A MONITORING SERVICE?

Think you might need some help keeping track of everything? Monitoring services often offer to do what you can do yourself for free. Just remember to research the company to ensure they are trustworthy, reliable, legitimate and that their services fit your needs.

Even if you enroll in a service, it doesn't take you out of the picture. You are the best tool for detecting identity theft.

FREE ACCOUNT MONITORING TOOLS

Consider these tools for protecting your accounts.



SET-UP ACCOUNT ALERTS

Most banks and credit unions offer alert programs to help you easily track your accounts. You can setup alerts for purchases, low balances, available credit and more. The options are almost endless because you can tailor them to your liking. You can also choose how you'd like to receive the alert (ie: text/email).



LOGIN PROTECTIONS.

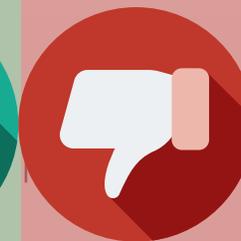
Logging in online? Research any extra security options offered such as: (1) two-factor authentication - requires an extra step to verify it's you attempting to login, and (2) login alerts - give you notice when someone logs into your account from a device you don't normally use.

DO THESE THINGS:

- Shred items that include personal information before getting rid of them.
- Before sharing information at the doctor's office, your child's school or a business ask: why they need it, how it will be protected, and what options you have if you don't want to give the information.
- Take those outgoing bills to a USPS blue mailbox.
- Use anti-virus software and update it often.

DON'T DO THESE THINGS:

- Never release your personal identifying information (PII) to someone you don't know. That means keep your SSN, date of birth and financial account numbers to yourself!
- Don't use your debit card when shopping online.
- Don't use public wi-fi to make purchases or login to your mobile banking site.
- Don't carry around your social security card or birth certificate.



CREDIT REPORT CHECKLIST

Use the following worksheet to review each section of your credit report. Do this for each credit report you get throughout the year. Then, keep the completed checklist with your credit report.

TODAY'S DATE:

1. Is your name correct? YES NO

2. Is your Social Security number correct? YES NO

3. Is your current address correct? Is your current phone number correct? YES NO

4. Are the previous addresses they have listed for you correct? YES NO

5. Is your marital status listed correctly? YES NO

6. Is the employment history they have listed for you accurate? YES NO

7. Is everything listed in the personal information section correct? YES NO

8. Is there anything listed in the public record information? YES NO

Is it correct? YES NO

Highlight the information you think may not be correct.

9. Are the accounts on the list still open? YES NO

Review each item under the credit account (trade account) section.

10. Are all of the current balances correct? YES NO

11. Are accounts where you are an authorized user or joint owner listed? YES NO

12. Are zero balances recorded for debts discharged in bankruptcy? YES NO

For debts paid in full? YES NO

13. Are you listed as a co-signer on a loan? YES NO

Is this correct? YES NO

14. Are accounts that you closed listed as "closed by the consumer"? YES NO

15. Is negative information reported on each credit account correct? YES NO

Look for late or missed payments and other defaults. Highlight items you think are not correct.

16. Are any accounts listed more than once? YES NO

Check to make sure the same account is not listed multiple times in the collections section.

17. Is old negative information still being reported? YES NO

If yes, highlight the information. In most cases, negative info that is more than 7-years-old and bankruptcies more than 10-years-old cannot be reported.

18. Do you suspect that you have been the victim of identity theft after reviewing your credit reports? YES NO

Your credit report contains a lot of personal and financial information. Be sure to keep any hard copies in a safe and secure place. If you do not want to hang on to your credit reports, shred them.

CONTACTS

EXPERIAN

Online:

experian.com/help

Phone: (888) 397-3742

TRANSUNION

Online:

transunion.com/credit-help

Phone: (800) 680-7289

EQUIFAX

Online:

equifax.com/personal/credit-report-services

Phone: (800) 685-1111

REPORT SCAMS TO:

SCDCA: (844) 835-5322 or www.consumer.sc.gov

FTC: (877) 382-4357 or ftccomplaintassistant.gov

FCC: (888) 225-5322 or fcc.gov/complaints (phone)

DO NOT CALL REGISTRY

Add your number to the Do Not Call Registry:

Donotcall.gov or (888) 382-1222

STOP UNSOLICITED OFFERS

Opt out of snail mail marketing:

Dmchoice.org

Opt out of preapproved credit offers:

www.optoutprescreen.com or call (888) 567-8688.

South Carolina

DEPARTMENT OF CONSUMER AFFAIRS

PO Box 5757 • Columbia, SC 29250

(800) 922-1594 • www.consumer.sc.gov

Follow us for the latest.





CYBER SECURITY BASICS

CYBER SECURITY BASICS

Cybersecurity doesn't need to be complicated. Here are the basics of cybersecurity so you can be in control of your information and keep your devices safe.

PROTECT

Your Files & Devices

Update your software.

Outdated software makes it easier for scammers to hack your device. Set automatic updates.



Require passwords.

Use passwords for all of your devices. Don't leave these devices unattended in public places.



Secure your files.

Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.



Use two-factor authentication.

This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.



Encrypt devices.

Encrypt devices, files and other media that contain sensitive personal information. Encryption protects information sent over your network so it can't be read by outsiders.



Your Wireless Network

Secure your home router.

Change the default name and unique password, turn off remote management, and log out as the administrator once the router is set up.



Setup a network firewall.

A firewall is a piece of hardware and/or software that protects and controls traffic coming into your network. If your router has a firewall option, enable it.



Use at least WPA2 encryption.

Make sure your router offers WPA2 or WPA3 encryption, and that it's turned on. Just like on your devices, the encryption will protect your info from being read/accessed by outsiders.



Disconnect old devices.

Disconnect older devices you no longer use from the network. Their security may be out of date, creating a weak point on your network.



Your Identity & Privacy

Own your online identity.

Every time you sign up for a new account, app, or get a new device, immediately set the information sharing privacy/security settings to what you're most comfortable with. Regularly check these settings to make sure nothing has changed.



Share with care.

Think before posting online. Consider what a post reveals, who might see it and how it might affect you or others. ID thieves use the information you post online to try and guess your passwords, security questions and/or steal your identity!



Beware of free Wifi hotspots.

Public Wifi networks are not secure, which means that anyone may see what you are doing while you are connected. Avoid logging into accounts like email and financial services. Consider using a virtual private network (VPN) or a personal/mobile hotspot.



SHOPPING & SURFING ONLINE

We are online all of the time. Protect your info and money by considering these tips when shopping online:



Consider your payment options.

Using a credit card is much better than using a debit card; there are more consumer protections for credit cards if something goes wrong. If your debit card number gets stolen, that's a direct line into your bank account.



Monitor your statements.

Continuously check your accounts for any unauthorized activity. Set up alerts so that if your credit card is used, you will receive an alert with the transaction details.



Do your homework.

Scammers are good at setting up fake websites. Before making a purchase, read reviews. Look for a physical location, any customer service info and call the merchant to confirm that they are real.



Don't give it all away.

If the merchant is requesting more data than you feel comfortable sharing, don't shop there. You only need to fill out required fields at checkout and you should not save your payment information in your profile.

PASSWORD TIPS

There are a lot of ways to create a strong password, but here are the basics:



Make sure your password is at least 12 characters long with uppercase and lowercase letters, numbers and symbols. Avoid using common words, phrases or anything related to your personal life.



Pick security questions only you know the answer to and avoid using questions that answers could be easily found on the internet.



Don't reuse passwords or save your passwords in your internet browsers. Consider a reputable password manager if you struggle to remember your passwords.



Change passwords quickly if there's a breach. Change your passwords every three months to keep your accounts safe.

PHISHING SCAMS

Phishing scammers target consumers by sending them an e-mail, text or direct message that looks like it's from a trusted source. It asks for personal identifying information and then the scammer uses that info to open new accounts or invade the consumer's existing accounts. Some common ways scammers try to phish info from you include:



Claim they've noticed some suspicious activity or log-in attempts.



Say you must confirm personal information.



Claim there is a problem with your account or payment information.



Say you're eligible for a government refund or offer a coupon for free stuff.



Want you to click on a link to confirm login information or make a payment.



Include a fake invoice.

Remember! Never reply to calls, texts, pop-ups, or e-mails that ask for verification of personal information. Avoid clicking on links or downloading attachments from suspicious emails or texts.

To report a scam, visit www.consumer.sc.gov and click "How Do I..."



RECOVERING FROM A DISASTER

RECOVERING from a DISASTER

paying your bills

researching options

finding a place to live

replacing lost or damaged documents

safeguarding personal information



PAYING YOUR BILLS

After a disaster, paying your bills may seem unimportant in comparison to getting food and shelter. But addressing your financial responsibilities sooner, rather than later, can save you a lot of trouble (and possible late fees) in the long run. Taking some or all of the steps below can help you recover even faster:

- **Communication is more important than ever.** Call your creditors and ask for help. Ask about programs in place to defer your loan payments, waive late fees, or raise your credit limit temporarily.
- **Get a copy of your credit report.** If you've lost your financial records and need help identifying your creditors, get your credit report. It's free from annualcreditreport.com, or 1-877-322-8228.
- **Consider a credit counselor.** If you're worried you can't pay your bills, consider a credit counselor. Make sure they are licensed by contacting SCDCa at 800-922-1594 or www.consumer.sc.gov.
- **Don't waste money on utilities you're not using.** Put utility services on hold if you're not able to stay in your home.
- **Ask for help.** Apply for disaster assistance available/offered, even if you aren't sure you will qualify. You can't receive a benefit you don't apply for!



RESEARCHING OPTIONS

Whether you're applying for a loan to get back on your feet, or searching for a repair company to get your home to pre-disaster status, there are a few things you should do:

- **Go with what you know.** Use established businesses that you are familiar with. If you don't have previous experience with the business, take the time to research them. Call us at 1-800-922-1594 or visit www.consumer.sc.gov to see if we have any complaints against the business. Ask to see their state, county or local license(s).
- **Payment.** Avoid advance-fee loan scams and contractors that ask you to pay in full before the work is done.
- **Read the contract.** Make sure you have a written contract, all terms are included and you fully understand them. Ask questions or consult with someone you trust before you sign. Make sure you get a copy of the completed contract.
- **No guarantees.** Be suspicious of promises that sound too good to be true. Make sure you understand the services being offered and the time frame in which they will be provided.
- **Cancellation policies.** Verify the cancellation policy. What would you need to do to opt out? Are there any fees associated with canceling?
- **Take Your Time.** Avoid high pressure sales tactics. If the company is reputable, the deal will be there tomorrow.



FINDING A PLACE TO LIVE

If you've been displaced by a disaster, beware of fake realty/rental listings. Follow these tips to avoid falling victim to a scammer:

- **Talk to the person.** Don't just rely on e-mail correspondence. Be sure that you talk to the person on the phone. If they are unable or unwilling to do so, it could be a scam.
- **Background the property.** Check online for duplicate listings or negative information related to the listing/owner. Legitimate rental or realty listings can easily be hijacked by fraudsters.
- **Tour the property.** Look at the whole property inside and out before signing a contract or paying any money.
- **Ask for references.** Request that the owner give you references from other tenants. What was their rental experience like?
- **Get it in writing.** It is very important to get any verbal promises in writing. Review the contract carefully before handing over any cash.
- **Don't pay by wire transfer.** Don't make any payments by wire transfer. It immediately puts the money in the scammer's hands, making it difficult to recover.
- **Look up the owner.** If you're looking to rent a house, you can find the real owner and their contact information by looking up the property on the register of deeds website. Be sure you are looking in the county in which the house is located.
- **Be suspicious.** If the deal sounds too good to be true, walk away.

REPLACING LOST OR DAMAGED DOCUMENTS

It's important to replace damaged or lost legal and personal documents.

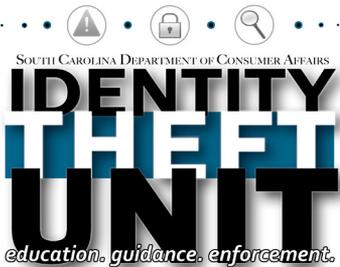
<i>Document(s)</i>	<i>Who to Contact</i>
Deeds and recorded real estate documents	County's Register of Deeds (800) 922-6081 • www.sccounties.org
Mortgages and other credit documents	Lender or financial company
Leases	Landlord or financial company
Insurance policies	Insurance company/agent (803) 737-6160 • www.doi.sc.gov
Wills	The attorney (<i>If the will is destroyed, you'll need another</i>) (803) 779-4579 • www.sctbar.org
Checks/Savings documents/ Investment material	Bank, investment company, or your broker
Auto Title/Driver's License	Department of Motor Vehicles (803) 896-5000 • www.scdmsonline.com
Birth Certificate	Department of Health and Environmental Control (803) 898-3432 • www.scdhec.gov
Social Security Card	Local Social Security Administration Office (866) 964-7594 • www.socialsecurity.gov
Tax Returns	Internal Revenue Service (800) 829-1040 • www.irs.gov
Documents like contracts or divorce judgments	The attorney or the court (see Wills above) sccourts.org



SAFEGUARDING PERSONAL INFORMATION

As you recover from the disaster, you will share personal information to get relief benefits, loans, replacement documents, etc. Scammers may pose as government officials, insurance agents, financial institutions and other professionals asking for personal financial information or money to help you.

- **Stay on guard.** Ask for identification and don't be afraid to contact the organization the person represents to verify their identity.
- **Hang up.** Don't give any personal or financial information to a cold caller.
- **Send information securely.** If you're mailing any sensitive personal documents, be sure to send them certified mail, return receipt requested. Place outgoing mail in USPS mailbox.



If you gave your information to someone suspicious, contact the South Carolina Department of Consumer Affairs' Identity Theft Unit at 800-922-1594. Also consider taking some or all of the following steps:

STEP #1: FRAUD ALERT

Place a Fraud Alert: Its FREE, stays in place for 90 days and requires a business to take steps to verify that it is in fact you that is applying for the good or service. Call one of the credit bureaus and they'll notify the other two.

STEP #2: SECURITY FREEZE

Consider a Security Freeze: Its FREE and will prevent a business from accessing your credit report for new products or services, unless you temporarily lift the freeze. You must call each of the credit bureaus to do this.

Equifax: 800-685-1111

TransUnion: 800-680-7289

Experian: 888-397-3792

You can use these numbers for both the fraud alert and the security freeze.

STEP #3: MONITOR

Monitor Financial and Personal Statements: Be sure that your bills and statements are arriving on time and are correct. ID Thieves don't just use your information to get money. Your SSN can be used to receive:

- Government benefits
- Driver's License/ID
- Tax refund
- Medical benefits

So, be sure to monitor ALL of your statements, and always be on alert for any suspicious or unexpected letters or phone calls!



For more information on financial literacy, scams, identity theft and being a savvy consumer, contact the South Carolina Department of Consumer Affairs at **800-922-1594** or **www.consumer.sc.gov**



Check out our
YouTube channel.
youtube.com/scdcatv



Find the latest scam
alerts and news here.
twitter.com/scdca



Look here for updates &
educational materials.
facebook.com/scdca



DITCH THE PITCH: A guide for guarding against scams.



01/20/46

DITCH THE PITCH

a guide for guarding against scams



The State of South Carolina
Department of Consumer Affairs

2221 DEVINE STREET, STE 200
P. O. BOX 5757
COLUMBIA, S.C. 29250-5757

Commissioners
David Campbell
Chair
Columbia
Mark Hammond
Secretary of State
Columbia
Caroline Ballington
Conway
Carlisle Kennedy
Leesville
W. Fred Pennington, Jr.
Taylors

Carri Grube Lybarker
Administrator/
Consumer Advocate

Celebrating Over 40 Years of Public Service

TABLE OF CONTENTS

Dear Fellow South Carolinian,

Thank you for taking this step to arm yourself with the tips you need to spot and avoid scams. Education is, and always has been, a large part of the South Carolina Department of Consumer Affairs' mission. We understand navigating the ever-changing marketplace can be a daunting task. And with the rapid development of technology, scammers are more active (and more successful) than ever. It is with that fact in mind that SCDCA created this guide to avoiding scams.

“Ditch the Pitch” is meant to help you get ahead of the fraudsters. It also serves as a call to action; encouraging you to “beware and share” this information with your friends and family. You play an invaluable role in helping us warn more of our citizens about scammers. Thank you!

With Warm Regards,

Carri Grube Lybarker, Esq.
Administrator



- scam red flags.....2
- defend against phone scams.....3
- common digital scams.....4
- common scams.....9
- defend against other popular scams.....12
- does a scammer have your information?.....14
- important contact information.....16
- help us spread the word.....17

If it sounds too good to be true...
SCAM RED FLAGS

Below you will find a list of the most common signs of a scam. Be wary if someone:

- Asks you to verify personal identifying information.
- Asks you to wire transfer money or purchase a prepaid/reloadable debit card or iTunes gift card and give them the number off the card.
- Sends you a check, asking you to cash it and wire or send money somewhere.
- Poses as a local, state, or federal law enforcement officer. They may also pose as other government officials.
- Scares you with threats of arrest or garnishment.
- Makes you think their “offer” is time sensitive. **“Act NOW, or you won’t get this great deal!”**



Bottom Line: If you are fielding a cold call (email, text message, etc.) never give information to the person and when in doubt, **hang up and follow up!**

3 **WAYS** **TO DEFEND**
against phone
scams

1. Don't fall for high pressure tactics

2. Be suspicious of wire transfer or reloadable debit card payment requests

3. When in doubt, hang up and follow up

 **RED FLAG:** Scammers have also been asking consumers to make payments with iTunes gift cards. Businesses and government organizations will not ask for payment this way.

COMMON DIGITAL SCAMS

PHISHING

Phishing is a scam where an Internet fraudster sends an e-mail that claims to be from a business you may have a relationship with. The message asks you to “confirm,” “update” or “verify” your personal information - for example your account number or social security number - or your online account user name or password. A website link for you to visit or telephone number for you to call may be included in the e-mail.



RED FLAG: Legitimate companies don't ask for personal information via e-mail and text message.

NOTE: Watch out for “spear” phishing attempts too. This is a spin on traditional phishing where scam artists have some inside information, such as your name or knowledge of who you do business with, which they use to seem more legitimate in their request for personal data.

SMiShing

SMiShing, similar to phishing, is an attempt to get personal information from you. The only difference is that SMiShing attempts come in the form of text messages instead of emails.

The message may ask that you verify or update information, or it could contain a link with a virus or other malware that the scammer wants you to download onto your mobile device.

You've won a free \$100 gift card, just click [here](#) to claim!

the defense

- Do not reply to an e-mail, text or pop-up message that asks for personal or financial information.
- Do not click on any links in an email or text message or cut and paste the link into your browser.
- Do not open any attachments or download any files from an email or text message.
- Do not call a phone number contained in the e-mail or text.
- Use antivirus or antispyware software and a firewall. Make sure to update them regularly.
- Always review your personal and financial statements carefully. Also review your credit report at least once a year. You can get your report by visiting www.annualcreditreport.com or calling (877) 322-8228. Dispute unauthorized purchases/accounts and incorrect information.

TECH SUPPORT SCAMS

Scammers call claiming to be computer techs associated with well-known companies like Microsoft. They say viruses or other malware have been detected to trick you into giving them remote access to your computer or paying for software you don't need.



These scammers take advantage of your reasonable concerns about viruses and other threats. They

know that computer users have heard it's important to install security software. **But their goal is to take your money or personal information, not protect it.**

the defense

- Don't give control of your computer to a third party who calls you out of the blue.
- Do not rely on caller ID alone to authenticate a caller. Criminals spoof caller ID numbers.
- Don't rely on online search results. Scammers sometimes place online ads to convince you to call them. They pay to boost their ranking in search results so their information appears above that of legitimate companies. **If you want tech support, look for a company's contact information on their software package or on your receipt.**
- Never provide your credit card or financial information to someone who calls and claims to be from tech support.
- Never give your password to a cold caller.

CALLER ID SPOOFING



Scammers use fake caller ID information to trick you into thinking they are someone local, someone you trust – a company you do business with, maybe even a government agency or police department. The practice is called caller ID spoofing, and scammers don't care whose phone number they use.

While caller ID can be a great tool, it's not fool proof. Don't rely on caller ID to verify who's calling.

the defense

- Do not give a cold caller your personal information.
- If you're suspicious, hang up and call the organization directly. Find a legitimate phone number by searching the phone book, the back of any mail you might receive from the organization or their website. If you're still unsure, call SCDCA at (844) 835-5322 and we can help you find a phone number.
- Consider blocking the phone number. Contact your phone company to see if they provide this service and how much it might cost. Many smart phones feature blocking functions that can also be helpful.

-  **RED FLAG:** The caller ID contains all zeros, too many numbers, or is blank.
-  **RED FLAG:** Feeling pressured to act immediately? Hang up. That's a sure sign of a scam.

AUCTION/AD SITES

Auction/Ad sites like eBay and Craigslist can be great tools for buying and selling. They are also hotbeds for scam activity. Scammers may offer to buy an item you've posted, but when you get the check you realize it's for a much larger amount than you asked. The scammer will tell you to cash the check, pay yourself and send the rest back to them.



the defense

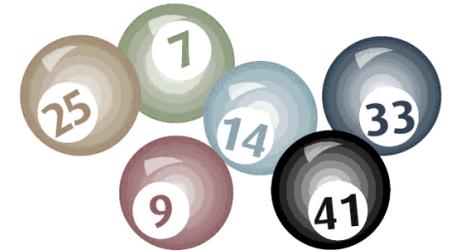
- There is never a valid reason to cash a check for someone and send the money back.
- Try selling to someone in your area. If you can't, talk to the buyer via phone.
- Be wary of a check for a larger amount than expected.
- Report the person to the site you are using.
- Request a check drawn on a local bank so you can make sure it is valid.

RED FLAG: Look out for spelling and grammar errors in e-mails.

COMMON SCAMS

LOTTERY/SWEEPSTAKES

The Pitch: Scam artists will call or write saying you've won a lottery out of Australia, England or another foreign country. Some scammers use the names of well-known home improvement stores or super stores and allege you were entered into a drawing each time you shopped at the store and... you are a winner! In these scenarios, the scammer will ask you to wire or send money to get your prize.



the defense

- Never send money to claim a prize, especially through a wire transfer. Wiring money to a location is like sending cash.
- Don't play along or engage with the scammer. It will only make them more likely to call you again.

RED FLAG: Legitimate lotteries and sweepstakes will not ask you to pay a fee to collect your winnings.

RED FLAG: Scam artists often say the up front fee is for "insurance," "taxes," "shipping and handling charges."

FAKE DEBT COLLECTORS



The Pitch: The scammer, sometimes pretending to be from a state, federal or law enforcement agency, will try to get you to settle a debt you supposedly “owe.” The fraudster may ask you to pay a fraction of the amount, immediately, over the phone. In exchange, the debt will be forgiven. Some consumers have reported that the scammer had their

personal information, making the call seem more legitimate. If you don’t make the payment right then, you will have to pay it all.

the defense

- Never give your credit card number or banking information to someone you do not know.
- Call the organization the scammer posed as to let them know about the scam.
- Ask for something in writing from the “debt collector” so you can verify their claim. Federal law requires debt collectors to send you a letter about the debt.
- Check your credit report to see if the debt you “owe” is there. Get a free copy of your credit report at www.annualcreditreport.com or by calling (877) 322-8228.

RED FLAG: The scammer threatens that you’ll be arrested if you don’t pay.

IMPOSTERS

The Pitch: Fraudsters will pose as your bank and ask for personal or banking information needed to supposedly “verify” or “reactivate” your credit or debit account. The caller may claim that the information is needed to reverse a fraudulent charge or an error resulting in your card being blocked. Scammers also pose as government agencies like the IRS.

A different spin on the imposter scam has the scammer posing as a friend or a family member who is in trouble and needs money. The “trouble” often ranges from car problems to being in jail. Instead of your personal banking information, this time the caller wants you to wire money to assist your loved one.



the defense

- Do not give your personal information or otherwise ‘verify’ your bank/credit card information over the phone.
- Hang up and dial your bank or credit card company directly and tell them about the call.
- Before you send money to a caller insisting your family member or friend needs it, contact someone who could verify or debunk the story.

RED FLAG: The fraudster tells you not to tell anyone about the call/situation.

DEFEND AGAINST OTHER POPULAR SCAMS

SECRET SHOPPER

- Steer clear of offers that come through the mail with a check included.
- Look for a legitimate secret shopper job through the Mystery Shopper Providers Organization of North America by visiting mspa-na.org.
- Never cash a check from someone you don't know and wire the money.

JURY DUTY

- Information about jury duty will come through the mail, not a phone call.
- Courts and law enforcement officers will not call or email you asking for personal information or money.
- Don't trust your caller ID; scammers can easily spoof their phone number to look like it is a local call.

HEALTH FRAUD

- Be aware of false ads for free medical services or products.
- Medicare and Medicaid will never call and request your personal information over the phone.
- If called, do not agree to enroll in health insurance plans over the phone. Ask for information in writing.

FAKE CHARITIES

- The Secretary of State's Office has a list of good and bad charities. For a copy visit www.scsos.com or call (888) CHARITI (242-7484) or (803) 734-1790.
- Avoid charities soliciting door-to-door.
- Stick with recognized charities that are well-established.
- Ask any cold caller to send you information about the charity through the mail.

HOME REPAIR

- Do not pay in full upfront.
- Make sure all details are in a written contract and you get a completed copy.
- Check with the SC Department of Labor Licensing and Regulation at www.llr.sc.gov to verify licensure.
- Ask friends or family for references.

SHAM INVESTMENTS

- Legitimate offers will not disappear overnight. Do not feel pressured to make a quick decision.
- Involve a family member or professional when a stranger promises a large profit on an investment.
- Think twice if you are told "your profit is guaranteed" or "there is no risk."

DOES A SCAMMER HAVE YOUR INFORMATION?

If you have shared your information with a scammer, there are some steps you should take to minimize the damage!

STEP #1: FRAUD ALERT

Place a Fraud Alert: It's FREE, stays in place for one year and requires a business to take steps to verify that it is in fact you that is applying for the good or service. Call one of the credit bureaus and they'll notify the other two.

STEP #2: SECURITY FREEZE

Consider a Security Freeze: It's FREE and will prevent a business from accessing your credit report for new products or services, unless you temporarily lift the freeze. You must call each of the credit bureaus to do this.

Equifax: (800) 685-1111

TransUnion: (800) 680-7289

Experian: (888) 397-3742

You can use these numbers for both the fraud alert and the security freeze.

STEP #3: MONITOR

Monitor Financial and Personal Statements:

Be sure that your bills and statements are arriving on time and are correct. ID Thieves don't just use your information to get money. Your SSN can be used to receive:

- Government benefits
- Driver's License/ID
- Tax refund
- Medical benefits

So, be sure to monitor ALL of your statements, and always be on alert for any suspicious or unexpected letters or phone calls!

FOR ADDITIONAL HELP:

Contact the South Carolina Department of Consumer Affairs' ID Theft Unit for more tips on dealing with identity theft and scams.

(844) 835-5322 • www.consumer.sc.gov



Check out our YouTube channel.
youtube.com/scdcatv



Find the latest scam alerts and news here.
twitter.com/scdca



Look here for updates & educational materials.
facebook.com/SCDepartmentofConsumerAffairs

IMPORTANT CONTACT INFORMATION

REPORT SCAMS TO:

SCDCA: (844) 835-5322 or www.consumer.sc.gov
FTC: (877) 382-4357 or ftccomplaintassistant.gov
FCC: (888) 225-5322 or fcc.gov/complaints (phone)

DO NOT CALL REGISTRY

Add your number to the Do Not Call Registry:
Donotcall.gov or (888) 382-1222

STOP UNSOLICITED OFFERS

Opt out of snail mail marketing:
Dmchoice.org

Opt out of preapproved credit offers:
www.optoutprescreen.com or call (888) 567-8688.

FREE CREDIT REPORT

Get a copy of your **FREE** credit report:
www.annualcreditreport.com or call (877) 322-8228.

HELP US SPREAD THE WORD

Use this magnet as a reminder to warn your friends, family and others about the dangers of scams.



Scam reports help SCDCA identify fraud trends and get the word out to consumers on what to avoid. There is no report too small!



Find the latest scam alerts and news here. twitter.com/scdca



Check out our YouTube channel. youtube.com/scdcatv



Look here for updates & educational materials. facebook.com/SCDepartmentofConsumerAffairs



South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

PO Box 5757 • Columbia, SC 29250
(800) 922-1594 • www.consumer.sc.gov



HOW TO PREVENT IDENTITY THEFT

HOW TO PREVENT IDENTITY THEFT



Your Information has been Breached... What Now?

Page 1



Fraud Alerts, Freezes and ID Theft Protection Services, Oh My! So, What's the Difference?

Page 2



Security Freeze FAQs, Protecting Your Child's Identity and Tools to Consider.

Pages 3-4



Get in the Habit: Everyday Practices that Help You Avoid Identity Theft.

Page 5



Are YOU a Victim of Identity Theft? What to do.

Page 6

YOUR INFORMATION HAS BEEN BREACHED...

WHAT NOW?

1 CONSIDER A SECURITY FREEZE AND FRAUD ALERT

Prevent scammers from opening new accounts using your information by placing a **FREE** security freeze on your credit reports. A security freeze puts your credit report on lockdown, limiting access to it without your OK, and lasts until you lift it.

A fraud alert will allow a business to pull your credit report, but only after taking extra steps to verify the applicant is really you.

3 DEFEND AGAINST SCAMS

Scam artists use information from breaches to make their requests seem legit. Never reply to calls, texts, pop-ups, or e-mails that ask you for, or to verify, personal information.

Fraudsters may even pose as a monitoring service and send emails with subject lines or content like: "Identity Theft Alert" or "Your Score Has Dropped." Avoid clicking on links or downloading attachments from suspicious emails or texts.

2 MONITOR YOUR STATEMENTS

Make sure your bills and benefits, medical and financial statements are arriving on time and are correct. Identity thieves can use your info, like a social security number, the same way you do. Including to get:

- Government benefits
- Driver's License/ID
- Cell phones/utilities
- Medical benefits
- Tax Refund
- A Job

Find signs of identity theft? Flip to page six for the next steps.

4 INTERESTED IN A MONITORING SERVICE?

Think you might need some help keeping track of everything? Monitoring services (also called ID theft protection services) often offer to do what you can do yourself for free (see steps 1-3 above).

Just remember to research the company to ensure they are:

1. TRUSTWORTHY, RELIABLE, and LEGITIMATE.
2. Their services fit your needs.

Even if you enroll in a service, it doesn't take you out of the picture. You are the best tool you have for detecting identity theft.

WHO TO CONTACT:

SECURITY FREEZE: You MUST contact EACH credit reporting agency to place, thaw or lift the freeze.

FRAUD ALERT: You only need to contact one of the credit reporting agencies to place a fraud alert and they will notify the other two.

EQUIFAX

Online:
equifax.com/personal/credit-report-services

Phone: (800) 685-1111

EXPERIAN

Online:
experian.com/help

Phone: (888) 397-3742

TRANSUNION

Online:
transunion.com/credit-help

Phone: (800) 680-7289

Having trouble finding what you need? Call us at (844) 835-5322.

FRAUD ALERTS, FREEZES AND ID THEFT PROTECTION SERVICES, OH MY! SO, WHAT'S THE DIFFERENCE?

FRAUD ALERT:

WHAT IS IT? Federal law gives consumers the right to place a fraud alert on credit reports for **FREE**. It alerts potential creditors pulling your report to take extra steps to verify your identity before issuing credit or services in your name.

HOW LONG WILL IT LAST? Lasting one year, the alert entitles you to a free credit report from each of the three credit reporting agencies. A fraud alert can be renewed. But if you have proof you are a victim of identity theft, you can place an extended fraud alert that lasts 7 years.

WHO DO I CONTACT? You only have to contact one of the credit reporting agencies, Equifax, TransUnion or Experian, and they'll notify the other two. See page one for contact info.

SECURITY FREEZE:

WHAT IS IT? When a freeze is in place, a business that receives an application for products or services cannot access your credit report without your permission. Utilities, credit cards and insurance companies all commonly require a credit check. A freeze doesn't affect your existing lines of credit and will need to be thawed if you decide to apply for new credit or services.

HOW LONG DOES IT LAST? The freeze lasts until **YOU** lift it. You can lift for a specified amount of time. After the time has elapsed, the freeze will go back into place. It can also be lifted permanently. When you place the freeze, you will receive a PIN number or password to use when you want to temporarily lift ("thaw") or permanently remove the freeze. Make sure to keep it in a safe place.

WHO DO I CONTACT? Each of the three major credit reporting agencies. See page one for contact info. *If you are the caregiver for a minor or incapacitated adult, consider the protected consumer freeze. See page four for more information on how it works.*

FREE ID THEFT PROTECTION SERVICES:

WHAT IS IT? Identity theft protection services often include either credit report monitoring, identity monitoring, or resolution services...or a combination of those.

- Credit monitoring is when a third party monitors your credit reports for identity theft red flags.
- Identity monitoring is when a third party searches databases, chatrooms or "underground" websites for signs your information is in the hands of fraudsters.
- Resolution or recovery services are meant to assist you in the process of remedying an identity theft event.

HOW LONG WILL IT LAST AND WHO DO I CONTACT? Check the security breach notice you receive for more information on opting in and the duration of the service. If a service is not offered and you would like to have one, be sure to do your research and find the best fit for you.

***REMEMBER:** All of these tools are independent of one another. That means you **MUST** opt into them separately. The freeze and fraud alert only mitigate the effects of identity theft related to products or services where your credit report is viewed as part of the application process. Not all companies check credit reports.

SECURITY FREEZE FAQs

COMMON QUESTIONS ABOUT THIS FREE ID THEFT PROTECTION TOOL.

DOES A SECURITY FREEZE ON MY CREDIT REPORT AFFECT MY CREDIT SCORE?

No. A security freeze does not affect your credit score. Lifting or removing the freeze does not affect your score either.

DOES PLACING A SECURITY FREEZE ON MY CREDIT REPORT STOP PRESCREENED CREDIT OFFERS?

No. Prescreened/ "preapproved" offers for credit and insurance can be stopped by calling 1-888-5-OPT-OUT (1-888-567-8688) or visiting www.optoutprescreen.com.

DOES A SECURITY FREEZE PREVENT ME FROM USING MY CREDIT CARDS?

No. A security freeze restricts access to your credit report to prevent new accounts or services from being opened in your name. It does not prevent you, or an identity thief, from using existing accounts/ cards.

WILL A SECURITY FREEZE PREVENT ME FROM PULLING MY OWN CREDIT REPORT OR ENROLLING IN CREDIT REPORT MONITORING SERVICES?

No. The freeze will not affect your ability to pull your own credit report or receive credit monitoring services. Businesses you currently have a relationship with can still access your report as well.

IS A SECURITY FREEZE THE SAME AS A CREDIT LOCK?

No. A security freeze is a free identity theft protection tool provided by law. A credit lock is a product offered by consumer reporting agencies that consumers can contract for, sometimes for a fee, and provides a similar effect of limiting access to a credit report. Because the lock is not provided for by law, who can access your credit report when a lock is in place may change as can other terms of the product, including fees. Legal protections for consumers when a lock goes awry are also unclear.

PROTECTING YOUR CHILD'S IDENTITY

STAY ON GUARD.



CHECK FOR A CREDIT REPORT.

Generally, children will not have a credit report unless an identity thief uses their information. A thief may use it for many years before the crime is discovered. Parents are encouraged to check to see whether their child has a credit report. Contact each of the three credit reporting agencies for information on how to request a search.



CONSIDER THE PROTECTED CONSUMER FREEZE.

A protected consumer freeze is **FREE** and available for children under the age of 16 and incapacitated adults. The freeze allows a parent, guardian or representative of the consumer to create a credit file in the person's name and place a freeze on it, helping to deter identity theft. Remember to place your request with **EACH** of the three credit reporting agencies. You will be asked to give proof of the protected consumer's identity, your identity, and proof of authority to act on behalf of the protected consumer.



To request a credit report search or place a freeze, see page one for credit reporting agency contact information. *Having trouble finding what you need? Call us at (844) 835-5322.*

ACCOUNT MONITORING TOOLS

CONSIDER THESE TOOLS FOR PROTECTING YOUR ACCOUNTS.



ACCOUNT ALERTS.

Most banks and credit unions offer alert programs to help you easily track your accounts. You can setup alerts for purchases, low balances, available credit and more. The options are almost endless because you can tailor them to your liking. You can also choose how you'd like to receive the alert (ie: text/email)



SIGN UP FOR MY SOCIAL SECURITY.

This online tool lets anyone still working view estimates of future retirement, disability and survivor benefits, earnings and Social Security and Medicare taxes you've paid. If an identity thief is using your SSN to work, their earnings may show up in your account. Once you create an account, it prevents others from creating an account in your name. Visit www.ssa.gov/myaccount.



LOGIN PROTECTIONS.

Logging in online? Research any extra security options offered such as: **(1) two-factor authentication** - requires an extra step to verify it's you attempting to login, and **(2) login alerts** - give you notice when someone logs into your account from a device you don't normally use.

GET IN THE HABIT

EVERYDAY PRACTICES THAT HELP YOU AVOID IDENTITY THEFT.

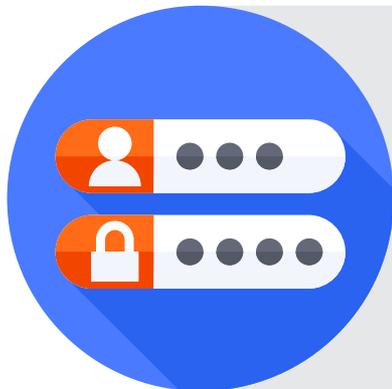
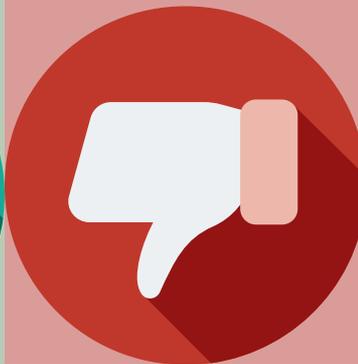
DO THESE THINGS:

- Shred items that include personal information before getting rid of them.
- Before sharing information at the doctor's office, your child's school or a business ask: why they need it, how it will be protected, and what options you have if you don't want to give the information.
- Take those outgoing bills to a USPS blue mailbox.
- Use anti-virus software and update it often.



DON'T DO THESE THINGS:

- Never release your personal identifying information (PII) to someone you don't know. That means keep your SSN, date of birth and financial account numbers to yourself!
- Don't use your debit card when shopping online.
- Don't use public wi-fi to make purchases or login to your mobile banking site.
- Don't carry around your social security card or birth certificate.



PASSWORDS AND SECURITY QUESTIONS

Make sure security questions cannot be answered with information found on your social media accounts. Use strong, creative passwords (uppercase, lowercase and special characters) and don't share them with anyone. Don't use the same passwords or security questions for multiple accounts.



REQUEST YOUR **FREE** ANNUAL CREDIT REPORT

It's easy, FREE and you get three each year: one from Equifax, Experian and TransUnion. Just call: (877) 322-8228 or visit www.annualcreditreport.com



LIKE TO SURF THE WEB, SHOP, BANK OR CONNECT ONLINE?

Take stock of the personal information you share online. Once it's shared, it is difficult—or near impossible—to erase. Review privacy settings to see who can see your information and make any needed changes. Read privacy policies before signing up to see what the business does with your info.

STAY ON GUARD ONLINE!

ARE YOU A VICTIM OF IDENTITY THEFT?

AFTER PLACING A FRAUD ALERT AND A SECURITY FREEZE ON YOUR CREDIT REPORTS:

1 CLOSE AFFECTED/FRAUDULENT ACCOUNTS AND DISPUTE THEM

- Notify the company ASAP and request a dispute form.
- Send the form certified mail, return-receipt requested.
- Once the dispute process is complete, ask for a letter that confirms the accounts and fraudulent debts are resolved.
- Keep copies of ALL correspondence.
- Are signs of fraud showing up on your credit report? Send a letter explaining the errors/mistakes to the 3 credit reporting agencies, too.

2 CONTACT SCDCR'S ID THEFT UNIT

The Identity Theft Unit offers specific tips for the type(s) of ID theft you are experiencing. If you're feeling overwhelmed, contact the Unit and fill out an intake form. Call (844) 835-5322 or visit www.consumer.sc.gov.



3 FILE A COMPLAINT WITH THE FTC

The Federal Trade Commission shares complaint data with law enforcement officials nationwide. You need the complaint affidavit to serve as part of your official "ID Theft Report" for disputing any further fraudulent activity. Report to (877) 438-4338 or identitytheft.gov.

4 FILE A POLICE REPORT

Take your FTC affidavit with you. If the officer is hesitant to fill out the report, request an information only report. You need the police report to complete your ID Theft Report.

WHEN RESOLVING IDENTITY THEFT, KEEP DETAILED RECORDS



Create a phone log and note who you talked to and when.



When sending supporting documents, send copies, not originals.



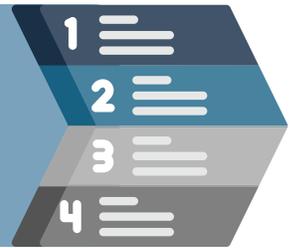
Send letters by certified mail, return-receipt requested.



Be aware of deadlines or time constraints.



Step by Step: INCOME TAX FRAUD



If you think someone has misused your Social Security number to get a job or tax refund - or the IRS sends you a notice indicating a problem - contact the IRS and/or the SC Department of Revenue immediately.

HOW TO REPORT LOST, STOLEN OR MISSING ID

STEP BY STEP:

NOTES:

For **federal tax fraud**, contact the Internal Revenue Service (IRS).

Report the fraud and ask for IRS ID Theft Affidavit Form 14039.
 Send the IRS Identity Theft Affidavit Form 14039, proof of your identity, such as a copy of your Social Security card, driver's license or passport and a copy of your police report, if you filed one.

IRS Identity Protection Specialized Unit
 1 (800) 908-4490
www.irs.gov/identitytheft

Request a FREE federal tax return transcript and/or a tax account transcript.

Review these documents for red flags such as wages you didn't earn.
 1 (800) 908-9946
www.irs.gov, under "Tools" click "Order a Return or Account Transcript."

Report your lost or stolen **passport** to the U.S. Department of State.

This office will help you navigate through the process of resolving issues with your tax records.
 1 (877) 487-2778
www.irs.gov
 Click "Help & Resources" then click "Contact Your Taxpayer Advocate," pick "SC."

For **state tax fraud**, contact the SC Department of Revenue.

Remember: See step 2 above about getting your federal return/account transcripts. You should check them for signs of fraud.

Complete tax fraud form CID-27: Tax Violation Complaint Form.

1 (803) 898-5953
www.sctax.org/tax+information/reporttaxfraud
 SC Department of Revenue
 Attn: Tax Fraud Divison
 Market Pointe Service Center
 300-B Outlet Pointe Blvd.
 P.O. Box 21587
 Columbia, SC 29221



IDENTITY THEFT TOOLKIT

Identity Theft Toolkit

WHAT YOU NEED TO DO

.....

This Toolkit is meant to serve as a guide to consumers who are victims of identity theft. The steps enclosed are general and apply to most identity theft situations. You may need to take additional steps to resolve your specific issue(s).

PAGE

1-2

STOPPING THE
DAMAGE

PAGE

1-3

REPAIRING THE
DAMAGE

PAGE

4

DAMAGE
CONTROL

STOP THE DAMAGE

Struggling with an identity theft event? Start here to minimize the damage.

1 REQUEST YOUR CREDIT REPORT:

WHAT IS IT? You are entitled to a **FREE** credit report from each credit reporting agency annually. Review them carefully for signs of identity theft. (i.e. accounts you didn't open, names/addresses that are not yours, etc.)

WHO DO I CONTACT? Call (877) 322-8228 or visit annualcreditreport.com to request your free credit reports.

WARNING! Beware of impostor websites or phone numbers. If you are asked for a credit card number, hang up or close the browser and try again.

2 PLACE A FRAUD ALERT

2 PLACE A FRAUD ALERT

WHAT IS IT? Federal law gives consumers the right to place a fraud alert on credit reports for **FREE**. It alerts potential creditors pulling your report to take extra steps to verify your identity before issuing credit or services in your name.

HOW LONG WILL IT LAST? One year. The alert allows you another free credit report from each of the three credit reporting agencies. While an initial fraud alert can be renewed, if you have proof you are a victim of identity theft, you can place an extended fraud alert that lasts seven years. *See page 4 for more information on the extended fraud alert.

WHO DO I CONTACT? You only have to contact one of the agencies and they'll notify the other two.
Equifax • (800) 685-1111 or equifax.com/personal/credit-report-services
Experian • (888) 397-3742 or experian.com/help
TransUnion • (800) 680-7289 or transunion.com/credit-help

3 CONSIDER A SECURITY FREEZE

WHAT IS IT? When a freeze is in place, a business that receives an application for products or services cannot access your credit report without your permission. Utilities, credit cards and insurance all commonly require a credit check. A freeze doesn't affect your existing lines of credit but will need to be thawed if you decide to apply for new credit or services. It is **FREE** to place, thaw or lift the freeze.

HOW LONG DOES IT LAST? The freeze lasts until **YOU** lift it. You can lift for a specified amount of time. After the time has elapsed, the freeze will go back into place. It can also be lifted permanently.

WHO DO I CONTACT? Contact ALL three to place the freeze.
Equifax • (800) 685-1111 or equifax.com/personal/credit-report-services
Experian • (888) 397-3742 or experian.com/help
TransUnion • (800) 680-7289 or transunion.com/credit-help

4 CONSIDER MAKING AN IDENTITY THEFT REPORT

4 CONSIDER MAKING AN IDENTITY THEFT REPORT

WHAT IS IT? An Identity Theft Report is made up of an affidavit from the Federal Trade Commission (FTC) and a police report. Together these items help you to dispute any accounts the identity thief opened using your information. See pages 3-4 for information on the value of an Identity Theft Report.

HOW DO I MAKE ONE? Contact the FTC to complete an Identity Theft Affidavit. Then, print out a copy of the affidavit for use in your Identity Theft Report. Take the affidavit with you to the police station to file your police report. If the officer is hesitant to give you a report, tell them you need an "information only" report. Attach your Identity Theft Affidavit to the police report.

WHO DO I CONTACT? Call the FTC (877) 438-4338 or visit IdentityTheft.gov.

REPAIR THE DAMAGE

There are different options for repairing the damage caused by identity theft. Choose the path that is right for you.

1 REVIEW YOUR CREDIT REPORTS

Go through each section with a fine tooth comb. Look for items you don't recognize. This could be anything from a misspelled name, an address where you've never lived, an account you didn't open or a judgment or lien you weren't aware of. Be sure to check your credit reports regularly.

2 CLOSE AFFECTED/FRAUDULENT ACCOUNTS

Contact the security or fraud department of each company. If the identity thief has made charges or debits on your accounts, or has fraudulently opened accounts, request the forms needed to dispute those transactions. Send the forms certified mail, return receipt requested and keep a copy for your records.

3 CORRECTING ERRORS

If you find mistakes resulting from identity theft on your credit reports, you can dispute or block the information, but depends on if you've created an ID theft report. Head to page 3 for your next step.

CORRECTING ERRORS

If you find mistakes resulting from identity theft on your credit reports, you can dispute or block the information. Blocking requires an Identity Theft Report. See page 2 for the steps to make a report.

What is Disputing?

Federal law allows you to dispute inaccuracies on your credit report. To do this, contact the credit reporting agencies and the business that provided the inaccurate information. You can dispute inaccuracies whether they are the result of identity theft or not. **You will not need an Identity Theft Report to dispute information.**

***REMEMBER:** Send all letters **certified mail with return receipt requested.**

I DON'T have an Identity Theft Report



Disputing Fraudulent Accounts

With Credit Reporting Agencies:

- Write to the credit reporting agency explaining that you are a victim of identity theft.
- List any errors found on your credit report and include **copies** of supporting documents.

With Businesses:

- Request dispute forms from the business. Fill them out, detailing what information is inaccurate.
- In some cases, you can send a letter outlining what is incorrect.
- Send **copies** of any supporting documents along with your completed form/letter.

DID YOU KNOW? You can dispute online, too!

www.transunion.com
(click on Credit Help)

www.equifax.com
(click on Credit Report Assistance)

www.experian.com
(click on Credit Report Assistance)

What is Blocking?

By law, credit reporting agencies must block identity theft-related information from appearing on a victim's credit report. They must block unauthorized transactions, accounts, and inquiries. To get unauthorized information blocked, you must give certain information to the credit reporting agencies. **You will need an Identity Theft Report.**

I DO have an Identity Theft Report



Blocking Fraudulent Accounts

With Credit Reporting Agencies:

- Write to each credit reporting agency. Send a copy of your Identity Theft Report.
- Include proof of your identity: your name, address, and Social Security number.
- Explain which information on your report resulted from identity theft.
- Ask the agency to block the fraudulent information.

With Businesses:

- Write a letter to the business. Include a copy of your Identity Theft Report.
- Include proof of your identity, including your name, address, and Social Security number.
- Include a copy of your credit report. Explain which information on the credit report resulted from identity theft, and that it didn't come from a transaction you made or approved.

DAMAGE CONTROL

LONG TERM ALERTS

These **FREE** alerts can offer you even more protection than the initial fraud alert, but they have different conditions. So, read carefully and decide if either would apply to your situation.

Extended Fraud Alert

An extended fraud alert is only available to identity theft victims. The alert lasts for **seven years** and allows you to access **two copies** of your **credit report** from each credit reporting agency within a year of placing the alert. Your name will also be taken off marketing lists for prescreened credit offers for **five years**.

Unlike the initial fraud alert, you need to contact **EACH** credit reporting agency to get the extended fraud alert. The company may have you complete a request form and you *will* have to supply an Identity Theft Report.

The graphic below explains how to make an Identity Theft Report, which will help you prove you're a victim of identity theft. See page 2 for more information.



Active Duty Alert

This alert is available for military personnel who are deployed. To place the alert, contact **ONE** of the credit reporting agencies.



You may need to provide proof of identity, **such as a military ID, birth certificate or driver's license**. The alert will stay in place for **one year**, but can be renewed.

Your name will also be taken off marketing lists for prescreened credit offers for **two years**, unless you ask to be added back to the list.

HAS SOMEONE USED YOUR SOCIAL SECURITY NUMBER?

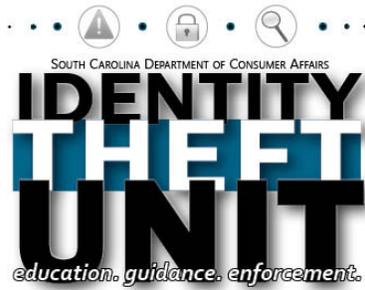


Someone illegally using your Social Security number (SSN) can cause a lot of problems. Identity thieves can use your info, like a SSN, the same way you do. Including to get:

- Government benefits
- Cell phones/utilities
- Tax Refund
- Driver's License/ID
- Medical benefits
- A Job

Make sure to sign up for my Social Security to monitor your account. This online tool (www.ssa.gov/myaccount) lets you view estimates of future retirement, manage benefits, change your address and direct deposit information, view earnings and Social Security and Medicare taxes you've paid and more. If someone is using your SSN for work, their earnings may show up on your statement. Once you create an account, it also prevents others from creating an account in your name. If you find any errors, contact the Social Security Administration (SSA). Find your local SSA Office by calling (866) 964-7594.

SSN card lost or stolen? Visit www.ssa.gov/ssnumber for the steps to get a new card or call (866) 964-7594 to find your local SSA office.



© South Carolina Department of Consumer Affairs, 2021.
This brochure may be copied or reproduced for non-commercial,
educational purposes, so long as no changes or modifications are made.



South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

PO Box 5757 • Columbia, SC 29250
(800) 922-1594 • www.consumer.sc.gov



Find the latest scam alerts and news here. twitter.com/scdca



Check out our YouTube channel. youtube.com/scdcatv



Look here for updates & educational materials. facebook.com/SCDepartmentofConsumerAffairs