

Identity THEFT *and the* LAW

A GUIDE FOR BUSINESS & GOVERNMENT

Their *information*,
Your *responsibility*.

TABLE *of* CONTENTS

Introduction	4
Business Records Disposal	6-7
Security Breach	8-11
Security Freeze	12
The Protected Consumer Freeze	13
Social Security Numbers	14-15
Other Provisions Under the Act	16
ID Theft and the Law: Q & A	17
Tips for Protecting PII	18
Other Laws of Interest	19
Additional Resources	20

The South Carolina Financial Identity Fraud and Identity Theft Protection Act

A brief introduction

To combat identity theft in South Carolina, the General Assembly passed the Financial Identity Fraud and Identity Theft Protection Act (The Act, FIFITPA, The Law) (Act No. 190, 2008).

The Act provides protections for consumers in the areas of security freezes, credit reports, records disposal, security breaches and more. The Act also places requirements on businesses and public bodies with regard to the collection, maintenance and disposal of consumers' personal information. All portions of the law, except the provisions regarding security breaches, became effective on December 31, 2008. The security breach provisions became effective on July 1, 2009.

In 2013, portions of the law were amended relating to initiation of law enforcement investigations of identity theft and the definition of personal identifying information (PII) (Act No. 15, 2013). Annually since 2014, the General Assembly has supplanted certain provisions applicable to state agencies via budget proviso(s). In 2018, the Fair Credit Reporting Act¹ was updated to allow any consumer to place a security freeze on their credit report. It also provides the ability to place a protected consumer freeze for children/dependants.

This brochure is produced by the South Carolina Department of Consumer Affairs (Department) and is meant to highlight important portions of the Act and not to serve as a substitute for reading the Act. References to portions of the laws amended or added by the Act are to the appropriate section number within the South Carolina Code of Laws. The complete Act may be found on the Department's website at consumer.sc.gov or at the South Carolina Legislature's website at scstatehouse.gov.

For questions about this guide or the Act, contact the Department.

¹ The Fair Credit Reporting Act in its entirety is codified at 15 U.S.C. §§ 1681 to 1681x.



2008

December 31st, majority of South Carolina's Financial Identity Fraud and Identity Theft Protection Act (FIFITPA) became effective.

2009

July 1st, FIFITPA security breach provisions became effective.



2013

Portions of FIFITPA were amended relating to law enforcement investigations of identity theft and the definition of personal identifying information.

2014

FIFITPA updated to allow for a protected consumer freeze.



2018

The Fair Credit Reporting Act was updated to allow any consumer to freeze their credit or place a protected consumer freeze for free.

Business Records Disposal

(Sections 37-20-190 & 30-2-310)

Persons conducting business in South Carolina and public bodies must properly dispose of records and items containing consumers' personal identifying information (PII). A person is defined as a natural person, an individual, or an organization.

A public body is defined as any department of the State, state board, commission, agency, and authority, public or governmental body or political subdivision, as well as any organization, corporation, or agency supported in whole or in part by public funds, including any bodies by whatever known name and quasi-governmental bodies of the State and its political subdivisions.

Personal identifying information (PII)* consists of, but is not limited to:

- | | |
|---|---|
| • social security numbers | • driver's license /State ID Card numbers |
| • checking account numbers | • savings account numbers |
| • credit card numbers | • debit card numbers |
| • personal identification (PIN) numbers | • electronic identification numbers |
| • digital signatures | • dates of birth |
| • current/former names, including first & last, middle & last or first, middle & last (but only when used in combination with and linked to other identifying information in this section). | |
| • current/former addresses, only when the addresses are used in combination with and linked to other identifying information in this section. | |

*See Section 16-13-510(D).

Business Records Disposal Cont.

(Sections 37-20-190 & 30-2-310)

Businesses and public bodies must make the PII unreadable or undecipherable when disposing of records and remove it from hardware, storage media and other items before selling, transferring or otherwise disposing of the item.

The director of a public body or its information technology manager must verify all confidential information is removed from computer items and items are sanitized in compliance with statewide and internal policies for protecting PII assets of their agency.

A business or public body can hire a third party to destroy records.

The following businesses are exempt from this section:

- Bank or financial institution subject to, and in compliance with, the Gramm-Leach-Bliley Act.
- A health insurer subject to, and in compliance with, the Health Insurance Portability and Accountability Act of 1996.
- A consumer credit reporting agency subject to, and in compliance with, the Fair Credit Reporting Act.

The Disposal Rule

Any business or individual who uses a consumer report for business purposes is subject to the federal Disposal Rule. This includes debt collectors, attorneys, lenders, mortgage brokers, and government agencies. The Rule requires that reasonable measures be implemented to ensure the proper disposal of information in consumer reports and records and prevent the unauthorized access to and use of the information. For more information visit ftc.gov.



Penalties for businesses include Private Cause of Action: actual damages, attorney's fees, injunctions; Administrative Action by the Department.

Security Breach

(Sections 1-11-490 & 39-1-90)

Persons conducting business in this state and state agencies must notify South Carolina residents when a security breach occurs². A security breach is the unauthorized access to, and acquisition of, items containing personal identifying information (PII) and the illegal use of the PII has occurred or is likely to occur. Disclosure of the breach must be made within a reasonable, expedient time from the discovery or notification of the breach. A third party maintaining data for another must notify the owner of a security breach. The owner of the data has the responsibility of notifying residents affected by the breach.

For persons conducting business in South Carolina and owning or licensing computerized or other data³, PII* means:

First name or first initial and last name in combination with and linked to any one or more of the following data elements relating to a South Carolina resident, when the data elements are neither encrypted nor redacted.

- social security number
- driver's license number or state identification card number
- financial account number, or credit card or debit card number in combination with any required security code, access code, or password
- other numbers or information which may be used to access a person's financial accounts or numbers/information issued by a governmental or regulatory entity that uniquely identified an individual

*See Section 39-1-90(D)(3).

For state agencies, PII has the same meaning as defined in Section 16-13-510(D), which is included on page 6 of this Guide. Additionally, agencies should monitor state budget provisos to ensure statutory definitions have not been supplemented.

² Pursuant to Section 1-11-490(D)(1), "state agency" means any agency, department, board, commission, committee, or institution of higher learning of the State or a political subdivision of it.

³ SCDCA issued Administrative Interpretation 11.490-1002 regarding security breaches. The AI can be viewed at consumer.sc.gov.

Security Breach Cont.

Residents must be notified through direct mail, telephone, or if certain conditions are met, via electronic means. In specific instances, notification of statewide media or substitute notice is permitted. If notice of a breach is sent to more than 1,000 persons at one time, the business or state agency must also notify the Department and the national credit reporting agencies.

Items for a business or state agency to include in a breach notice to South Carolina residents:

1. What happened?
2. What personal information was involved?
3. What are we (business/state agency) doing?
4. What can the consumer do?
5. Who can the consumer contact for more information? (include contact information for your organization, preferably a dedicated line if the breach was large.) Consider including information from the Department. See page 14 for more information.

When required to notify the Department and credit reporting agencies of a security breach, the notice should include all of the following:

1. When the breach occurred.
2. When the organization became aware of the breach.
3. Number of persons affected by the breach.
4. When notice was/will be sent to the affected persons.
5. Method of consumer notification. (e.g., mail, phone, electronic)
6. A copy of the notice sent to affected persons.



Penalties for noncompliance include civil action and damages, injunction, attorney's fees and costs. Administrative fines of up to \$1,000 per affected resident.

Security Breach Cont.

Sample Consumer Security Breach Notification Letter

Date
Organization's Name and Address
Affected Person's Name and Address

Dear (Person's Name):

I am writing to inform you that our organization experienced (or discovered) a security breach on or about (date of breach and when breach was discovered). Unfortunately, this has resulted in unauthorized access to your personal identifying information, specifically your (identify information that was or is reasonably believed to have been acquired).

(Organization Name) is taking this matter very seriously and has (describe steps taken to prevent further harm or access to the person's personal identifying information and indicate whether or not law enforcement and/or the Department of Consumer Affairs was notified of the breach). If you have any questions about this notice, please contact (name of contact person) at (contact's telephone number). You may also contact the South Carolina Department of Consumer Affairs at 1-800-922-1594 for guidance on avoiding and dealing with the effects of identity theft.

Sincerely,
(Organization's Representative)

Items to consider when drafting your security breach notice:



Write to your audience. How much do they know about security breaches? Anticipate what questions they will have. What is their reading level?



Use plain language. Avoid long sentences, unnecessary words and legal jargon. Replace complex terms with commonly known ones.



Design the letter for readability. Use at least 12-point font, bold headings and white space. Do not write full sentences using "all caps."

Security Breach Cont.

When contracting with a third party to assist in sending out or responding to recipients of a security breach notice, verify the vendor understands and can comply with the law. Tips include:

- 1** Make sure duties and expectations are clear in the contract. Include a requirement for your organization to review notice drafts and give final approval prior to distribution.
- 2** Ensure proper staff training and oversight if the vendor will be the contact for persons receiving the breach notices.
- 3** Establish processes so you can confirm the vendor is following the law throughout the term of the contract. Don't just take their word for it.
- 4** Get written confirmation from the vendor stating the duties were completed in accordance with applicable laws.

The Department has two web pages dedicated to security breaches notifications, one for businesses and one for consumers. On the business page you can find all the requirements, contact information, previous reports, and more.

Go to consumer.sc.gov, hover over "Business Resources/Laws" and click "Security Breaches."

The consumer page has education and links to every breach notice the Department has recently received.

A link to this page is at the top of the businesses page.

Security breach notifications should be sent to:



Legal Division
Re: Security Breach Notification
South Carolina Department of
Consumer Affairs
PO Box 5757
Columbia, SC 29250



scdca@scconsumer.gov

Security Freeze

(Section 37-20-160 & 15 U.S.C. §§ 1681c-1(i), (j))

When a security freeze is in place, a credit report cannot be accessed without the consumer's permission, making it harder for identity thieves to open new accounts in the consumer's name. While the Act first gave consumers this option, a 2018 amendment to the Federal Fair Credit Reporting Act preempts state security freeze laws. There are differences between the two.

The freeze may be temporarily removed, or "thawed," at the consumer's request. The thawing can be for a specified time and must be enacted within 1 hour if made via means other than mail. There is no cost to place, thaw or remove a security freeze.

The freeze does not apply to credit reports in certain circumstances, including those provided to government entities acting pursuant to a subpoena or court order; certain government entities like child support agencies; companies hired to monitor a credit file; when investigating fraud; local officials investigating or collecting delinquent amounts.

Consumers can place a freeze on their credit report by contacting the following credit reporting agencies:

Equifax

[equifax.com](https://www.equifax.com)

800-685-1111

or TDD 800-255-0056

PO Box 105788

Atlanta, GA 30348

Experian

[experian.com](https://www.experian.com)

888-EXPERIAN (397-3742)

or TDD 800-972-0322

PO Box 9554

Allen, TX 75013

TransUnion

[transunion.com](https://www.transunion.com)

888-909-8872

or TDD 877-553-7803

PO Box 6790

Fullerton, CA 92834

Businesses who pull credit reports are encouraged to include a question on their application regarding the presence of a security freeze on the consumer's credit report. Asking this question can help both parties avoid delays in the application process.



Protected Consumer Freeze

(Section 37-20-161)

2018 Amendments to the Fair Credit Reporting Act ("FCRA") also preempt South Carolina's protected consumer freeze law⁴. Parents, guardians and representatives may place a freeze on a protected consumer's credit file for free. A protected consumer is someone under the age of 16 or an incapacitated adult who does not currently have a credit report.

Upon receiving a request on behalf of a protected consumer that does not have a credit report, the credit reporting agency will create a credit file in that protected consumer's name and freeze it, helping deter identity theft.

Parents/guardians must contact each credit reporting agency to place the freeze. There is no charge to place a protected consumer freeze. For more information about security freezes, contact the Department or visit consumer.sc.gov.

Federal law also allows consumers to place a fraud alert on their credit report for free.

It alerts a business pulling the report to take extra steps to verify the consumer's identity. It last one year.

To place, consumers can call one of the major credit reporting agencies and they'll notify the other two.

SCDCA's Identity Theft Unit

Offering tailored assistance to victims of ID theft

The Identity Theft Unit (the Unit) is dedicated to educating consumers on avoiding scams and identity theft. The Unit also provides one-on-one assistance to victims of identity theft.



Consider referencing one of the Unit's various resources on security freezes, child identity theft, or scams on your company website or in a consumer security breach notice. If space is limited, simply include the Department's contact information. The Department also offers training for businesses on state and federal privacy laws. Visit consumer.sc.gov for information on upcoming webinars or to request in-person training.

⁴ See 15 U.S.C. §§ 1681c-1(j)

Social Security Numbers

(Sections 37-20-180 & 30-2-310)

Among other prohibitions, a public agency and a person may not:

- Make available to the public a person's social security number or six or more digits of the number.
- Require a person to transmit a social security number or six or more digits of the number on a card required for access to a product or service.
- Require a person to transmit a social security number or six or more digits of the number over the internet UNLESS there is a secure connection or the number is encrypted.
- Require a person to use his/her social security number or six or more digits of the number to access the web unless a password is also required.
- Print a person's social security number or six or more digits of the number on materials mailed to that person UNLESS state or federal law requires it.
- Sell, lease, loan, trade, rent or otherwise intentionally disclose a person's social security number or six or more digits of the number unless (1) the consumer consents in writing, (2) disclosure is for a legitimate business or government purpose or (3) disclosure is allowed by law.

This portion of the law does not apply to the following scenarios, among others listed in section 37-20-180(B):

- I. Collection, use or release of a person's social security number for internal verification.
- II. To a person acting pursuant to a court order, subpoena or other legal process.
- III. The opening of an account or payment for a product or services authorized by the consumer.

Social Security Numbers Cont.

Further, a public body:

- May not collect a person's social security number or six or more digits of the number UNLESS the body is (1) authorized by law or (2) the collection is imperative to the body performing its duties and responsibilities.
- When collecting a person's social security number or six or more digits of the number, must separate the number from the rest of the record, or as otherwise appropriate, so the number can be easily redacted pursuant to a Freedom of Information Act request.
- At a person's request, must give a statement of purpose for collecting the person's social security number or six or more digits of the number and how it will be used.
- Can only use a person's social security number or six or more digits of the number for the purpose stated.



Social security numbers and other identifying information may be released by a public body under certain circumstances, including (Section 30-2-320):

- Pursuant to a court order, subpoena, etc.
- For public health purpose.
- On a recorded document filed with court. *

*Remember to check court rules for provisions on privacy protection prior to filing. The rules can be found at sccourts.org.

Other Provisions Under the Act

(Section 37-20-120)

Seller/Lender Credit Card Issuer: Businesses that mail offers to receive a seller or lender credit card must verify a change of address that is substantially different from the address on the offer. A seller/lender credit card issuer is prohibited from mailing out additional credit cards to a new address if the card is requested within 30 days of the address change, unless the change of address is verified by the issuer.

Register of Deeds and Clerk of Court (Section 30-2-330):

Unless required by law, persons preparing or filing documents with the Register of Deeds or Clerk of Court cannot include certain information on the document: including social security number, driver's license number, checking account, credit or debit card number, etc.

Crimes

Financial Identity Fraud and Identity Fraud (Section 16-13-510) and "dumpster diving" (Section 16-11-725), the rummaging or stealing of another person's household garbage for the purpose of committing identity theft or fraud.

Penalties

The crime of "dumpster diving" can be either a misdemeanor or felony, dependent on willfulness. The crime of Financial Identity Fraud is considered a felony and punishable up to ten years of imprisonment and/or fines.

A violation is a misdemeanor with a \$500 fine per violation. A Register of Deeds and a Clerk of Court shall place notices in their respective office as well as on the internet regarding the restrictions above. The notice must be identical to that in Section 30-2-330 (C). An affected person may petition a court for an order compelling compliance if the Register of Deeds or Clerk of Court is not in compliance with this section.

Common Questions: Identity Theft and the Law

Q: What's the best way to dispose of documents containing personal identifying information?

A: The law requires that the records be shredded, erased or that another method is used that ensures the PII is unreadable or undecipherable.

Q: When should I notify the Department of a data security breach?

A: The requirement to notify the Department, and national credit reporting agencies, is triggered when more than 1,000 South Carolina residents are affected by your organization's security breach.

Q: Are there any consequences for not complying with the Financial Identity Fraud and Identity Theft Protection Act?





A: Yes. The Act provides several penalties, including being fined by the Department and sued by an affected person.

Q: What can I do to assist my staff and organization with complying with the Act?

A: Take stock of the PII your organization receives or has on file and develop a data security plan, data disposal plan and security breach plan. Implement staff training so they are clear on the organization's policies and procedures regarding the protection of PII. The Department is available as a resource to answer questions and provide education.

Tips for Protecting PII

Scammers often target businesses and agencies by sending fake invoices or posing as a fellow employee/manager, government agency or tech support. Here are a few starting points for how you can avoid scams or schemes trying to get PII or money from your business:

-  Be wary of email requests for personal, financial or other sensitive information and take time to verify the request in person or via telephone.
-  Remember - email is NOT a safe way to send sensitive information. Don't transmit account information or sensitive employee information by unsecured email.
-  Establish a multi-person approval process for transactions above a certain amount and sensitive information requests.
-  Train your staff on information security policies and how to spot the latest email scams. Update employees as you find out about new risks and vulnerabilities.

The Red Flags of a Scam



Scammers PRETEND to be someone you trust.

Whether it's a government agency, business or organization you know, scammers love to act like people they think you'll trust.



Scammers create a sense of urgency.

Scammers are in a rush to scam you before you can catch onto their act. They want you to act before you have time to think.



Scammers use intimidation and fear.

Playing on your emotions is a key scammer tactic.



Scammers use untraceable payment methods.

Scammers love to ask for payment in ways that are difficult to trace. These include wire transfers, prepaid debit cards, gift cards, cryptocurrency and payment apps. Some fraudsters will send you a fake check, tell you to deposit it, and then send them money back.

Other Privacy and Security Laws of Interest

State

[Consumer Identity Theft Protection](#)

S.C. Code Ann. Sec. 37-20-110, et seq.

[Breach of Security of Business Data](#)

S.C. Code Ann. Sec. 39-1-90

[Insurance Data Security Act](#)

S.C. Code Ann. Sec 38-99-10, et seq.

[Breach of Security of State Agency Data](#)

S.C. Code Ann. Sec. 1-11-490

[Family Privacy Protection Act](#)

S.C. Code Ann. Sec. 30-2-10, et. seq.

[Personal Identity Information Privacy Protection](#)

S.C. Code Ann. Sec. 30-2-310, et seq.

Federal

[Children's Online Privacy Protection Act](#)

15 U.S. Code Sec. 6501 et seq.

[Federal Trade Commission Act](#)

15 U.S. Code Sec. 45 et seq.

[Fair and Accurate Credit Transactions Act](#)

Public Law 108-159 (2003), 15 U.S.C. §§ 1681-1681x

[Gramm-Leach Bliley Act](#)

15 U.S. Code Sec. 6801 et seq.

[Right to Financial Privacy Act](#)

12 U.S. Code Sec. 3401 et seq.

[Fair Credit Reporting Act](#)

15 U.S. Code Sec. 1681 et seq.

[Health Insurance Portability and Accountability Act](#)

Public Law 104-191 (1996), 42 U.S.C. § 1320d et al.

Additional Resources:

Federal Trade Commission Privacy and Security
ftc.gov/business-guidance/privacy-security
FTC.gov/SmallBusiness

National Institute of Standards and Technology (NIST)
Computer Security Resource Center
csrc.nist.gov

OnGuard Online
OnGuardOnline.gov

South Carolina Division of Technology
admin.sc.gov/services/technology-services/information-security-privacy

Consumer Financial Protection Bureau
consumerfinance.gov

South Carolina Department of Consumer Affairs Security Breach Page
consumer.sc.gov/business-resources/laws/reporting-security-breach-businesses

FBI
ic3.gov

Definitions Index:

Person, 6
Personal Identifying Information, 6, 8
Public Body, 6
Security Breach, 8
State Agency, 8
Security Freeze, 12
Protected Consumer, 13



South Carolina Department of Consumer Affairs
800-922-1594 • consumer.sc.gov
- Fall 2025 -

© South Carolina Department of Consumer Affairs, 2025.
This brochure may be copied or reproduced for non-commercial,
educational purposes, so long as no changes or modifications are made.