A Publication of the South Carolina Department of Consumer Affairs

Identity THEFT *and the* LAW

A GUIDE FOR BUSINESS & GOVERNMENT

Their *information*,
Your *responsibility*.

TABLE *of* CONTENTS

Page left intentionally blank

The South Carolina Financial Identity Fraud and Identity Theft Protection Act

A brief introduction

Identity Theft is one of the nation's fastest growing crimes.
To aid in combating identity theft in South Carolina, the General Assembly passed the Financial Identity Fraud and Identity Theft Protection Act (The Act, The Law) (Act No. 190, 2008).

The Act provides several 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. Beginning July 2008 through December 2016, the South Carolina Department of Consumer Affairs (Department) received 248 data security breach notices affecting nearly eight million South Carolina residents.

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).

This brochure 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 South Carolina Department of Consumer Affairs' website at www.consumer.sc.gov or at the South Carolina's Legislature's website at www.scstatehouse.gov.

For questions about this guide or the Act, contact SCDCA directly at 800-922-1594.

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 *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 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).

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.

Penalties for businesses:

- Private Cause of Action: actual damages, attorney's fees; injunctions.
- Administrative Action by the Department of Consumer Affairs.

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.

Security Breach

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

Persons conducting business in this state and state agencies must notify South Carolina consumers when a security breach occurs.[1] 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.

For persons conducting business in South Carolina and owning or licensing computerized or other data[2], 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.

1 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.

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

Consumers must be notified through direct mail, telephone, or if certain conditions are met, notice can be sent 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 of Consumer Affairs and the national credit reporting agencies.

When a person is required to notify the Department of Consumer Affairs 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.*

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.)*
6. *Consider including information from the Department, including educational resources and the availability of consumer assistance in your notice.* ***See page 14 for more information.***

Penalties:

- Civil Action: damages, injunction, attorney's fees and costs;
- Administrative fines of up to $1,000 per affected resident.

Security Breach Notification

Security Breach Notifications should be mailed to:

Identity Theft Unit
Re: Security Breach Notification
South Carolina Department of Consumer Affairs
PO Box 5757
Columbia, SC 29250

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)

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.

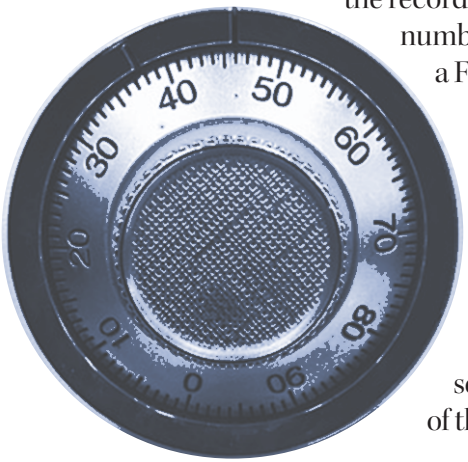
II. To a person acting pursuant to a court order, subpoena or other legal process.

III. The opening of an account or payment for a product or services authorized by the consumer.

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 prior to filing.*

Security Freeze

(Section 37-20-160)

South Carolina consumers can place a security freeze on their credit reports. When in place, the credit report cannot be accessed without the consumer's permission.

The freeze may be temporarily removed, or "thawed," at the consumer's request. The thawing can be for a specified time or a specific creditor and must be enacted within 15 minutes of the consumer's request. 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; child support agency; Department of Revenue; Department of Social Services when investigating fraud; local officials investigating or collecting delinquent amounts.

Businesses processing credit applications 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.

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

Equifax
www.equifax.com
800-685-1111
or TDD 800-255-0056
PO Box 105788, Atlanta, GA 30348

Experian
www.experian.com/freeze
888-EXPERIAN (397-3742)
or TDD 800-972-0322
PO Box 9554, Allen, TX 75013

TransUnion
www.transunion.com
888-909-8872
or TDD 877-553-7803
PO Box 6790, Fullerton, CA 92834

Protected Consumer Freeze

(Section 37-20-161)

Effective January 1, 2015, an amendment to the South Carolina Consumer Protection Code allows parents, guardians, and representatives to create and freeze 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, the credit reporting agency will create a credit file in that protected consumer's name and freeze it, helping to deter identity theft.

Parents/guardians must contact each credit reporting agency to place this freeze. There is no charge to place a protected consumer freeze.

For more information about security freezes, contact the Department of Consumer Affairs or visit www.consumer.sc.gov.

SCDCA's Identity Theft Unit

Offering tailored assistance to victims of ID theft

The Identity Theft 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.

IDENTITY THEFT UNIT
education. guidance. enforcement.

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.

800-922-1594
www.consumer.sc.gov
2221 Devine St., STE. 200
PO Box 5757
Columbia, SC 29250

Other Provisions Under the Act

Seller/Lender Credit Card Issuer (Section 37-20-120): 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 put the following on the document: social security number, driver's license number, checking account, credit card or debit card number, etc. A violation is a misdemeanor with $500 find 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.

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.

Identity Theft and the Law: Q&A

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 Consumer Affairs 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 of Consumer Affairs 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. As always, the Department of Consumer Affairs is available as a resource to answer questions and provide educational literature on the Act.

Definitions Index:

Additional Resources:

Federal Trade Commission Privacy and Security
www.ftc.gov
(Click "Tips & Advice"--> "Business Center"--> "Privacy & Security")

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

OnGuard Online
www.OnGuardOnline.gov

South Carolina Division of Technology
www.admin.sc.gov/technology

Consumer Financial Protection Bureau
www.consumerfinance.gov

The Consumer Federation of America
(Checklist for Breached Entities)
http://consumerfed.org/wp-content/uploads/2016/09/9-7-16-7-Questions-to-Ask_Fact-Sheet.pdf

CONNECT WITH US:

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

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

Check out our YouTube channel.
youtube.com/scdcatv

WWW.CONSUMER.SC.GOV

Page left intentionally blank

South Carolina Department of Consumer Affairs
2221 Devine St. STE 200 • PO Box 5757 • Columbia, SC 29250
800-922-1594 • www.consumer.sc.gov

- Summer 2017 -