

IDENTITY THEFT IN SOUTH CAROLINA: 2014 UPDATE



Marti Phillips, Esq.
Director, Identity Theft Unit
South Carolina Department of Consumer Affairs

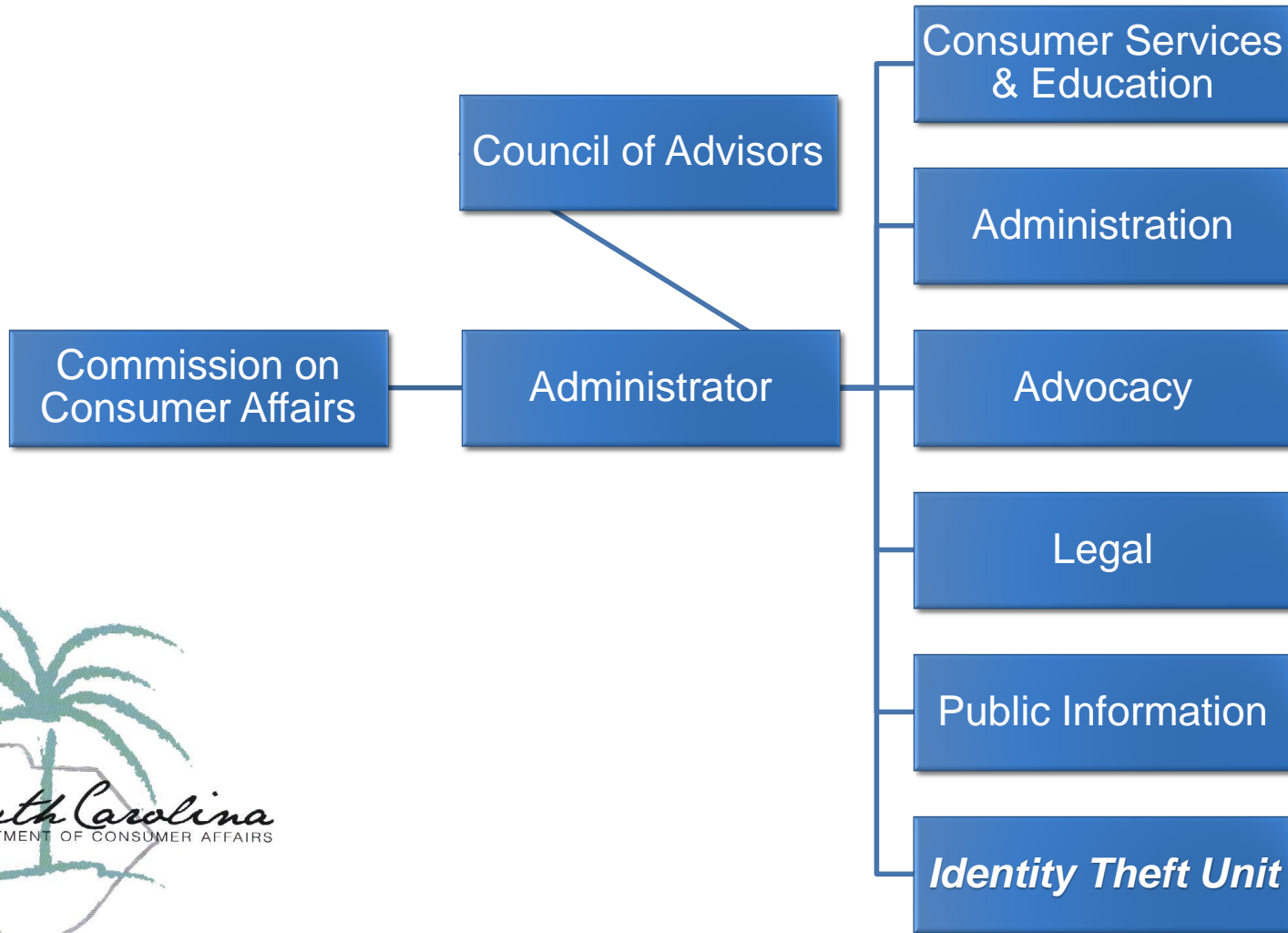
This presentation is not meant to serve as a substitute for reading various laws discussed, seeking legal counsel or otherwise requesting Department guidance and/or interpretations. The presentation merely serves as an introduction and overview.

Roadmap

- **SCDCA Identity Theft Unit**
 - Update
 - SC Statistics
 - FTC Consumer Sentinel
- **FIFITPA Update**
 - PII Definitions – *Changes*
 - *State Agency Requirements*
- **Legislative Updates**



SCDCA Organizational Structure



SCDCA Identity Theft Unit



Education

Provide education and outreach to SC consumers across the state; increase awareness and knowledge about identity theft & the steps to protect against id theft; and what to do if a victim.

Guidance

Provide ongoing guidance to SC id theft victims throughout the process of resolving their particular identity theft situation and mitigating negative effects.

Enforcement

Handle administration and enforcement of SC's *FIFITPA* and other identity theft-related consumer protection laws, including receipt of security breach notifications and ensuring reporting and notification requirements are met.

SCDCA Identity Theft Unit cont...



First year Accomplishments:

- ✓ Made **34 presentations** to over **14,700 people**, including consumer groups, state agencies, law enforcement and businesses;
- ✓ Fielded more than **4,200 calls**, approximately **50%** of which consisted of scam reports;
- ✓ Received **108** intake forms from identity theft victims;

SCDCA Identity Theft Unit cont...

First year Accomplishments cont:

- ✓ Garnered over **\$110,000 in refunds, credits and adjustments** for consumers through identity theft mitigation;
- ✓ Received **43 security breach notices**, affecting nearly **600,000** South Carolinians;
- ✓ Reached over **2,000** consumers through an AARP Senior Day at the SC State Fair.

SCDCA Identity Theft Unit cont...

www.consumer.sc.gov

SC.GOV Online Services Agency Listing Search consumer.sc.gov Search

SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS

QUICK LINKS ▶ HOME CONTACT US FILE A COMPLAINT LICENSEE LOOKUP Font Size: A + A - Reset

ABOUT US

CONSUMER INFORMATION

BUSINESS/INDUSTRY INFORMATION

NEWS RELEASES & PUBLICATIONS

LEGAL

PRIVACY STATEMENT

Tweets Follow SC Consumer Affairs @SCDCA

Three simple steps to back up your PC [ow.ly/CaVWW](#) #NCSAM #sctweets #SCDCA Tips

Welcome

The South Carolina Department of Consumer Affairs (DCA) is the state's consumer "Department" is the state's consumer protection agency. In 1974, DCA has more than thirty-five years of experience protecting South Carolina consumers while recognizing those businesses that act honestly and fairly.

The Department accomplishes its mission by: 1.) acting as an effective regulator, 2.) providing complaint mediation services that are unmatched at both state and federal levels, 3.) saving millions for both consumers and small businesses through insurance rate filing intervention, 4.) serving as an educational portal for consumers and businesses alike, and 5) informing the public on effective ways of preventing and mitigating identity theft situations.

Click [here](#) to learn more about the agency.

What's New?

Identity Theft Information

State-Provided Identity Protection Service with

Helpful Links

IDENTITY THEFT RESOURCES

Business Complaint Response Portal

Search Complaints

Credit Card Repayment Calculator

SCBOS Online Filing

consumer access

Identity Theft Intake Form

SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS
2221 Devine St. • STE. 200 • PO Box 5757 • Columbia, SC 29250
www.consumer.sc.gov • 800-922-1594

IDENTITY THEFT UNIT

IDENTITY THEFT INTAKE FORM

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

Tell Us About Yourself: Mr. Mrs. Ms.

Name: _____

Mailing Address: _____ City: _____

State: _____ Zip Code _____ Daytime Telephone Number: () _____

Age Range: 18-25 26-35 36-45 46-55 56-65 66-75 76+

Preferred Method of Contact: Mail Telephone E-mail: _____

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 Security Breach notice? Yes No

If so, please list the name of the company(ies): _____

What personal information was included in the breach (e.g. SSN, bank account number, etc.)? Please list: _____

Credit Report Information

Have you reviewed your credit report(s) within the last year? Yes No

If yes, which credit reports did you review?

TransUnion Date: _____ Equifax Date: _____ Experian Date: _____

Have you placed a Fraud Alert on your credit report(s) within the last 90 days? Yes No

Which agency did you contact to place the Fraud Alert? TransUnion Equifax Experian

Have you placed a Security Freeze on your credit report(s)? Yes No

Which agency(ies) did you contact to place your Security Freeze?

TransUnion Date: _____ Equifax Date: _____ Experian Date: _____

SCDCA Identity Theft “Toolkit”

A PUBLICATION OF THE SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS

identity theft

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 2-3 STOPPING THE DAMAGE

PAGE 2-4 REPAIRING THE DAMAGE

PAGE 5 DAMAGE CONTROL

SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS

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 INCOME TAX FRAUD

STEP BY STEP:	NOTES:
<input type="checkbox"/> For federal tax fraud, contact the Internal Revenue Service (IRS).	<input type="checkbox"/> Report the fraud and ask for IRS ID Theft Affidavit Form 14039. <input type="checkbox"/> 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. <i>IRS Identity Protection Specialized Unit</i> 1-800-908-4490 www.irs.gov/identitytheft
<input type="checkbox"/> Request a FREE federal tax return transcript and/or a tax account transcript.	<input type="checkbox"/> 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."
<input type="checkbox"/> Contact the IRS Taxpayer Advocate office in SC.	<input type="checkbox"/> This office will help you navigate through the process of resolving issues with your tax records. 1-800-908-9946 www.irs.gov Click "Help & Resources" then click "Contact Your Taxpayer Advocate," pick "SC"
<input type="checkbox"/> 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 also.	<input type="checkbox"/> Complete tax fraud form CID-27: Tax Violation Complaint Form. 803-898-5953 www.sctax.org/tax+information/reporttaxfraud SC Department of Revenue Attn: Tax Fraud Division Market Pointe Service Center 300-B Outlet Pointe Blvd PO Box 21587 Columbia, SC 29221

TURN PAGE OVER FOR ADDITIONAL INFORMATION

SCDCA Identity Theft Guide

A PUBLICATION OF THE SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS

IDENTITY THEFT

what you need to know

• • • • •

Step By Step: What To Do After a Security Breach

#1: Place a fraud alert on your credit reports.

It's **FREE**, stays in place for 90-days and requires potential creditors to take steps to verify that the applicant is in fact you.

You **only** have to contact 1 of the 3 credit reporting agencies (CRA) to place the alert. Once you place the alert, you will receive notice that you can get 1 **FREE** copy of your credit report from **each** of the CRAs. It is a great idea to request all three reports and make sure that everything on them is accurate.

Equifax: 800-685-1111
TransUnion: 800-680-7289
Experian: 888-397-3742

#2: Consider placing a security freeze on your credit reports.

It's **FREE** and will prevent potential creditors and other third parties from accessing your credit report for new products or services, unless you temporarily lift the freeze. **You must call each of the CRAs to do this.** It is **FREE** to place, thaw and lift the freeze for SC residents. Once you place the freeze, you will receive a personal identification number (PIN) you can use to thaw or lift the freeze. Make sure to keep it in a safe place. For more information on the freeze, including *how to place, thaw and lift one*, see page 3.

#3: Monitor your financial and personal statements closely.

Ensure that your bills and statements are arriving on time and are completely accurate. Remember, identity thieves can use your social security number the same way you do. Including to receive:

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

So, monitor medical and benefits statements and always be on alert for any suspicious or unexpected letters or phone calls!

#4: Interested in a monitoring service?

Think you might need some help keeping track of everything? Monitoring services typically offer to do what you can freely do yourself (see steps 1-3 above). Just remember to research the company to ensure they are (1) TRUSTWORTHY, RELIABLE and LEGIT and (2) their services fit your needs.

WHAT'S INSIDE:

Learn What Tools are at YOUR Disposal page 2	How to Place, Thaw & Lift a Security Freeze page 3	Are YOU a Victim of Identity Theft? page 5
--	--	--

Next: ID Theft Numbers

FTC Consumer Sentinel

SC Stats: ID Theft Complaints

2013 – 17th

2012 – 17th

2011 – 20th

2010 – 29th

2009 – 28th

2008 – 29th

2007 – 30th

2006 – 32nd

2005 – 36th



Identity Theft Complaints Count from South Carolina Victims = 3,374

Identity Theft Types Reported by South Carolina Victims

Rank	Identity Theft Type	Complaints	Percentage ¹
1	Government Documents or Benefits Fraud	1,075	32%
2	Phone or Utilities Fraud	488	14%
3	Credit Card Fraud	447	13%
4	Bank Fraud	256	8%
5	Loan Fraud	156	5%
6	Employment-Related Fraud	137	4%
	Other	922	27%
	Attempted Identity Theft	198	6%

January 1 – December 31, 2013

How SC Victims' Information is Misused – Top 3*

- **32% Government Documents/Benefits Fraud**
 - Unlawful use or counterfeit of gov't issued documents
- **14% Phone or Utilities Fraud**
 - Obtaining these services with false info
- **13% Credit Card Fraud**
 - Opening a line of credit with false info



* From FTC Consumer Sentinel 2013 Report

Data Security Breaches – SC residents

From July 2008 - October 28, 2014

SCDCA has received:



- **157** security breach notices
- Affecting more than **7,387,958** South Carolina consumers.

UP NEXT: FIFITPA & Recent Amendments

FIFITPA Legislative Background

- **Bills ~ Comprehensive Result =**
 - S. 453, Act 190-2008
 - *Amends several different Code Sections*
- www.consumer.sc.gov
- **Effective Dates**
 - *December 31, 2008 & July 1, 2009 (Security Breach Portion)*
- **2013 Amendments: H. 3248 & Proviso 117.136 (FY14)**
 - *Definitions & Security Breach Portion*
- **2014 Budget Proviso 117.117 (FY15)**



FIFITPA Effective Dates

Eff. December 31, 2008:

- Consumer Identity Theft Protection § 37-20-110, *et seq.*
- Personal Identifying Information Privacy Protection §30-2-300, *et seq.*
- Crime of Dumpster Diving § 16- 11 -725
- Credit/Debit Card Receipts § 16-13-512
- Crime of Financial Identity Fraud § 16-13-510

FIFITPA Effective Dates cont...

Eff. July 1, 2009:

- Breach of Security of State Agency Data § 1 -11 - 490
- Breach of Security of Business Data § 39-1-90



Eff. July 1, 2014 – June 30, 2015 (FY15):

- **Budget Proviso 117.117 (Data Breach Notification – State Agency)**

FIFITPA Effective Dates cont...

2013 Amendment = H.3248 eff. April 23, 2013

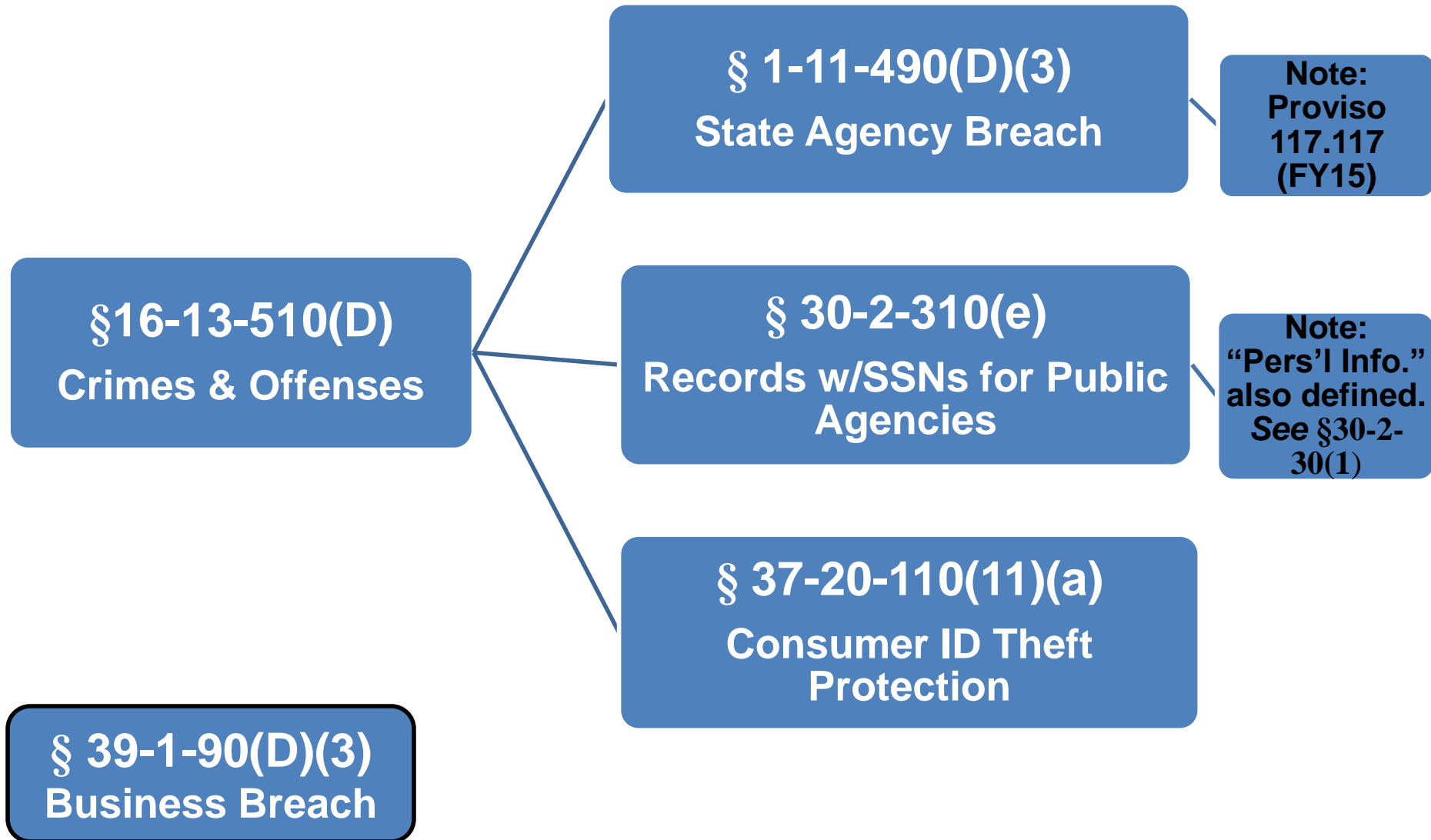
Amends § 16-13-510

- Broadens scope of ***Financial Identity Fraud***;
- **Revises definition of *Personal Identifying Information (PII)***;
- Defines ***Financial Resources***;
- Provides ***Venue*** for prosecution of identity fraud offense
- Conforms language to fin. transaction crime = ***not a defense*** that some acts did not occur in this state or within city/city county, local jurisdiction

Amends § 39-1-90 Breach of Security & *Business Data*

- **Revised definition of PII**

What's the definition of PII?



§ 16- 13-510(D) (amended by H. 3248 eff. 4/23/2013)

Personal identifying information (PII) includes but is not limited to :

- SSNs
- DL number or state ID card number
- Checking account numbers
- Savings account numbers
- Credit card numbers
- Debit card numbers
- PIN numbers
- Electronic ID numbers
- Digital signatures
- Dates of birth
- Current or former names*
- Current/former addresses when used w/other info in this section
- Other #s/pwords/info that may be used to access fin. resources, #s, or info issued by govt/reg entity that will uniquely identify individual/financial resources

*First + Last; Middle + Last; First, Middle, + Last, but only when the names are used in combination with, and linked to other identifying information provided.

§ 1-11-490(D)(3) Breach of security of state agency data

PII has same meaning as PII in §16-13-510(D)

- SSNs
- DL number or state ID card number
- Checking account numbers
- Savings account numbers
- Credit card numbers
- Debit card numbers
- PIN numbers
- Electronic ID numbers
- Digital signatures
- Dates of birth
- Current or former names*
- Current/former addresses when used w/other info in this section
- Other #s/pwords/info that may be used to access fin. resources, #s, or info issued by govt/reg entity that will uniquely identify individual/financial resources

*First + Last; Middle + Last; First, Middle, + Last, but only when the names are used in combination with, and linked to other identifying information provided.

Sidebar:

State Agencies & Security Breaches

S.C. Code Ann. § 1-11-490 *et seq.*

- Title 1– Administration of Government
 - Chapter 11- State Budget and Control Board
 - Section 490- **Breach of security of state agency data;** notification; rights and remedies of injured parties; penalties; notification of Consumer Protection Division.
- Effective 7-1-2009
 - ***FY15 Changes ~ Proviso 117.117***
(Effective July 1, 2014 - June 30, 2015)



Sidebar cont...

Budget Proviso 117.117 (FY15)

Part 1B section 117 X90-GENERAL PROVISIONS

2014-2015 Appropriation Act

Will discuss 117.117 more fully...

- *State agency breach notification requirements and how proviso amends § 1-11-490;*
- *For now – just looking at difference in PII definition.*

FY15 → Budget Proviso 117.117 changes PII definition for state agencies! eff. 7/1/14-6/30/15 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 that relate to a resident of this State, when the data elements are neither encrypted nor redacted or when the data elements are encrypted and encryption also acquired:
 1. SSN;
 2. Driver's license number or state ID card #;
 3. Financial account #, or credit card or debit card # in combination with any required security code, access code, or password that would permit access to a resident's financial account; **or**
 4. Other #s or information which may be used to access a person's financial accounts or #s or information issued by a governmental or regulatory entity that uniquely will identify an individual.

(The term does not include information that is lawfully obtained from publicly available information.)

§ 30-2-310(e) Collection of and maintenance & disposition of records containing SSNs by public agencies:

(A)(1) Except as provided in Sections 30-2-320 and 30-2-330 of this article, a public body, as defined in Section 30-1-10(B), may not:

(e) intentionally communicate or otherwise make available to the general public an individual's social security number or a portion of it containing six digits or more or **other personal identifying information**. **"Personal identifying information"**, as used in this section, has the same meaning as **"personal identifying information"** in Section 16-13-510, except that it does not include electronic identification names, including electronic mail addresses, or parent's legal surname before marriage;

§ 30-2-310(e) Collection/maintenance/disposition of records w/SSNs by public agencies cont.:

PII has same meaning as PII in §16-13-510(D)

- SSNs
- DL number or state ID card number
- Checking account numbers
- Savings account numbers
- Credit card numbers
- Debit card numbers
- PIN numbers
- Electronic ID numbers
- Digital signatures
- Dates of birth
- Current or former names*
- Current/former addresses when used w/other info in this section
- Other #s/pwords/info that may be used to access fin. resources, #s, or info issued by govt/reg entity that will uniquely identify individual/financial resources

*First + Last; Middle + Last; First, Middle, + Last, but only when the names are used in combination with, and linked to other identifying information provided.

§ 37-20-110(11)(a) Consumer Identity Theft Protection

PII has same meaning as PII in §16-13-510(D)

- SSNs
- DL number or state ID card number
- Checking account numbers
- Savings account numbers
- Credit card numbers
- Debit card numbers
- PIN numbers
- Electronic ID numbers
- Digital signatures
- Dates of birth
- Current or former names*
- Current/former addresses when used w/other info in this section
- Other #s/pwords/info that may be used to access fin. resources, #s, or info issued by govt/reg entity that will uniquely identify individual/financial resources

*First + Last; Middle + Last; First, Middle, + Last, but only when the names are used in combination with, and linked to other identifying information provided.

§ 39-1-90(D)(3) Breach of Security of Business Data...

(2013 Amendment = H.3248 eff. 4/23/13)

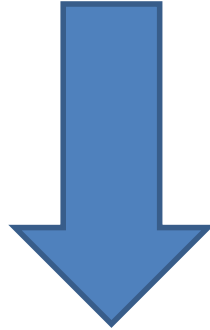
PII:

- first name or first initial **and**
- last name
- **in combination with** and linked to any **one or more** of the following data elements that relate to a resident of this State, when the data elements are neither encrypted nor redacted or when the data elements are encrypted and encryption also acquired:
 1. SSN;
 2. Driver's license number or state ID card #;
 3. Financial account #, or credit card or debit card # in combination with any required security code, access code, or password that would permit access to a resident's financial account; **or**
 4. Other #s or information which may be used to access a person's financial accounts or #s or information issued by a governmental or regulatory entity that uniquely will identify an individual.

(The term does not include information that is lawfully obtained from publicly available information.)

Up Next: Proviso 117.117

Budget Proviso 117.117 (FY15)



**State Agency Data Breach
Notification**
(§ 1-11-490 *et seq.*)

§ 1-11-490 *et seq.*

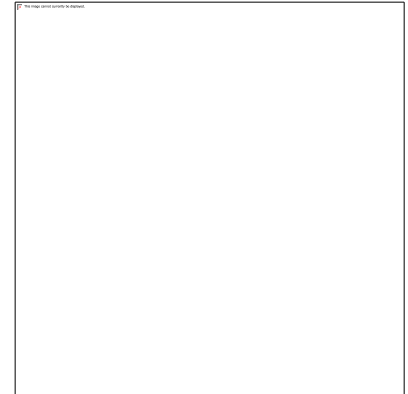
Important Definitions

§ 1-11-490(D)(1)

Agency means any:

- **agency,**
- **department,**
- **board,**
- **commission,**
- **committee, or**
- **institution of higher learning**

*--of the State or a political
subdivision of it*



Unchanged by Proviso 117.117

§ 1-11-490 *et seq.*

Important Definitions cont...

§ 1-11-490(D)(2) (emphasis added)

Breach of the Security of the System =

- the unauthorized access to and
- acquisition of
- computerized data
 - that was not rendered unusable through encryption, redaction, or other methods that compromise the security, confidentiality, or integrity of PII maintained by the agency,

When:

- illegal use of the information:
 - has occurred or is reasonably likely to occur OR
- use of the information creates a material risk of harm to the consumer.

Unchanged by Proviso 117.117

§ 1-11-490 *et seq.* Important Definitions cont...

§ 1-11-490(D)(3)

Personal Identifying Information has the same meaning as 'personal identifying information in § 16-13-510(D).

Remember:

§ 16-13-510(D) – was amended in 2013 to “broader” definition (list).

Proviso 117.117 changes PII to the “combination definition”...





§ 1-11-490 *et seq.* Important Definitions cont...

FY15 → Budget Proviso 117.117 eff. 7/1/14 - 6/30/15

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 that relate to a resident of this State, when the data elements are neither encrypted nor redacted or when the data elements are encrypted and encryption also acquired:
 1. SSN;
 2. Driver's license number or state ID card #;
 3. Financial account #, or credit card or debit card # in combination with any required security code, access code, or password that would permit access to a resident's financial account; **or**
 4. Other #s or information which may be used to access a person's financial accounts or #s or information issued by a governmental or regulatory entity that uniquely will identify an individual.

§ 1-11-490 *et seq.* Important Definitions cont...

FY15 → Budget Proviso 117.117 changes definition (eff. 7/1/14 - 6/30/15) PII means:

Cont...

The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

State Agency Security Breach cont...

Notification Required (*Owner of Data*): §1-11-490(A)

An agency of this State:

- **owning or licensing** computerized data OR other data
- that includes PII
- shall disclose **a any** breach of the security of the system
- following discovery or notification of the breach in the security of the data
- to **a any** resident of this State
- whose ~~unencrypted and unredacted~~ PII :
 - was, or is reasonably believed to have been, acquired by an unauthorized person
 - ~~when the illegal use of the information has occurred or~~
 - ~~is reasonably likely to occur or use of the information creates a material risk of harm to the resident.~~

Changes by Proviso 117.117 indicated above

State Agency Security Breach cont...

§1-11-490(A) Notification Required (Owner of Data)
cont..**2013**→ **Budget Proviso 117.117 adds:**

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the agency may consider the following factors, among others:

- (1) indications that the **information is in the physical possession and control** of an unauthorized person, such as a lost or stolen computer or other device containing information;***
- (2) indications that the **information has been viewed, downloaded, or copied**; or***
- (3) indications that the information **was used by an unauthorized person**, such as fraudulent accounts opened or instances of reported identity theft.***

State Agency Security Breach cont...

Notification Required (*Maintainer of Data*): § 1-11-490(B)

An agency **maintaining** :

- computerized data or
- other data
- that includes ***PII***
- that the ***agency does not own***
- shall notify ***the owner or licensee of the information***
- of a breach of the security of the data
- ***immediately following discovery, IF***
- the PII
 - was, **OR**
 - is reasonably believed to have been,
 - acquired by an unauthorized person

Unchanged by Proviso 117.117

State Agency Security Breach cont...

Timeliness of Disclosure - § 1-11-490/Proviso 117.117

The disclosure must be made:

- **In the most expedient time possible and without unreasonable delay;**
- ~~Consistent with the legitimate needs of law enforcement~~
- **With measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.**
(Language not in Proviso)

State Agency Security Breach cont...

Timeliness of Disclosure - § 1-11-490/Proviso 117.117 cont...

Disclosure may be delayed if:

- A law enforcement agency determines that the notification impedes a criminal investigation.
- **BUT** notification must be made after the law enforcement agency determines that it no longer compromises the investigation.

Budget Proviso 117.117 adds =

Delay cannot exceed 72 hours after discovery unless agency requests and AG grants (in writing) add'l delays of up to 72 hrs each upon a determination that such notification impedes criminal investigation.

State Agency Security Breach cont...

- **Notification Methods ~ § 1-11-490(E)/Proviso 117.117**
 - (1) **written notice;**
 - (2) **electronic notice, IF:**
 - the person/**agency's primary method of communication** with the individual is by electronic means, **the person to whom notice is required has expressly consented to receiving said notice in electronic form**, or is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 USC and Chapter 6, Title 26 of the 1976 Code;
 - (3) **telephonic notice ; OR**
 - (4) **substitute notice IF:**
 - the cost of providing notice > \$250,000 **OR**
 - >500,000 people affected **OR**
 - The agency has insufficient contact information.
 - e-mail notice when the agency has an e-mail address for the subject persons;
 - conspicuous posting of the notice on the agency's web site page, if the agency maintains one; or
 - notification to major statewide media.

State Agency Security Breach cont...

Notification Methods ~ § 1-11-490(E)/**Proviso 117.117**
cont...

Proviso 117.117 adds:

Regardless of the method by which notice is provided, such notice shall include:

- **Contact information for the agency making the notification; *and***
- **A description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization;**
- **Including specification of which of the elements of personal/private information were, or are reasonably believed to have been, so acquired.**

State Agency Security Breach cont...

Notification Methods ~ § 1-11-490/**Proviso 117.117** cont...

Proviso 117.117 *deletes* “quasi-safe harbor”

§ 1-11-490(F)

- Agency is in compliance if it maintains its own notification procedures as part of an information security policy and is otherwise consistent with timing requirements and notifies subject persons in accordance with its policies in the event of a security breach.

State Agency Security Breach cont...

Notification to SCDCA & CRAs ~ § 1-11-490(H)



□ **When:**

- Provide notice to > 1,000 persons at 1 time
- **Without unreasonable delay notify:**
 - Department of Consumer Affairs and
 - All consumer reporting agencies (CRAs) that compile and maintain files on a nationwide basis, as defined in 15 USC Section 1681a(p)

□ **Notice Must Include:**

- Timing,
- Distribution, &
- Content of Notice

Mail To:

SCDCA Identity Theft Unit
RE: Security Breach Notification
P.O. Box 5757
Columbia, SC 29250

Unchanged by Proviso 117.117

State Agency Security Breach cont...

Penalties:

▫ **Private Cause of Action**~ Section 1-11-490(G)

- A resident of this State who is injured by a violation of this section, in addition to and cumulative of all other rights and remedies available at law, may:
 - (1) **institute a civil action to recover damages;**
 - (2) **seek an injunction to enforce compliance; and**
 - (3) **recover attorney's fees and court costs, if successful.**

▫ **Administrative Fines** ~ Section 1-11-490(H)

- An agency that
- ***knowingly and willfully*** violates this section is subject to an administrative fine
- up to **\$1,000** for ***each resident*** whose information was accessible by reason of the breach

Unchanged by Proviso 117.117

State Agency Security Breach cont...

- **DCA Informal Interpretation** (May 6, 2010)
 - **Question 1**: *Does § 1-11-490 (consumer notification of breach) apply to the unauthorized access to and acquisition of paper records, consisting mainly of facsimiled documents, containing unredacted personal identifying information?*
 - **YES**
 - Reading Act as a whole (“other data”), definitions (“computerized data”), potential absurd result, etc.

State Agency Security Breach cont...

“Computerized data” is not defined within the section, however, when seeking to ascertain the meaning of an undefined statutory term, dictionaries may be utilized. Georgia Carolina Bail Bonds, Inc. v. City of Aiken and Goddard, 354 S.C. 18, 24, 579 S.E.2d 334, 337 (Ct.App. 2003). When combining the dictionary definitions provided for ‘computerized’ and ‘data’, the phrase means “facts, information, statistics, figures, details, observations, material(s), evidence; text” stored, performed or produced by computer. *The Oxford Dictionary: American Edition*, 288 and 355 (1996).

Looking to the phrase alone, the very broad definition encompasses items processed or stored with or in a computer, as well as paper documents originating therefrom, which would include facsimiles whereby the fax machine stores data received and/or distributed. A particular clause in a statute, however, should not be construed in isolation, but “in conjunction with the purpose of the whole statute and policy of the law.” Univ. of S. Cal. v. Moran, 365 S.C. 270, 278,617 S.E.2d 135,139 (Ct. App. 2005). While the definition of “breach of the security of the system” solely makes reference to “computerized data,” other portions of the statute additionally make reference to “other data” or “data.” As shown above, section 1-11-490(A) utilizes such phrasing in delineating who this section applies to – a state agency “owning or licensing computerized data or *other data*.” Subitem (B) also requires agencies maintaining “computerized data or *other data*” on behalf of other persons to notify the owner of the information of “a breach in the security of the data.” If the Legislature solely intended

“computerized data” to be the subject of the notification requirements, it would not have included “other data” in items (A) and (B). A statutory provision shall not be ignored and shall be interpreted to give effect to each provision while avoiding an absurd result as “the Court must presume the Legislature did not intend a futile act, but rather intended its statutes to accomplish something.” TNS Mills, Inc. v S.C. Dep’t of Revenue, 331 S.C. 611, 620, 503 S.E.2d 471, 476 (1998).

If the Department ignored statutory language and determined that the Legislature only wanted South Carolina consumers to be notified of a breach of their personal identifying information if such information constituted “computerized data,” an absurd result would occur.

State Agency Security Breach cont...

Question 2: What steps must be taken to comply with the notification provision contained in § 1-11-490(I) (notify SCDCA & CRAs when >1000 affected)?

- the **date of the breach**,
- **date the agency became aware** of the breach,
- **date the notice** was/will be **sent** to affected consumers,
- **method of consumer notification** (ie: mail, telephone, electronic),
- **number of consumers affected**, and
- the **content** of the consumer notice (ie: copy of the letter sent to consumers).

Security Breach cont...

- **Businesses must comply with similar security breach requirements.**

See § 39-1-90.

- **Definition of PII = same as included in Proviso 117.117 for agencies, but permanent through H3248 (2013).**



UP NEXT: Legislation

New SC Legislation: S.148

“Protected Consumer Bill”

Credit Report & Security Freezes for Protected Consumers ; Credit Record

- Amends FIFITPA to add a class of protected consumers & provide method of creating **credit record** for purpose of freezing (preemptive)
- “Protected Consumer” =
 - Individual under age 16
 - Incapacitated person w/guardian or conservator
- **Signed by Gov. on April 7, 2014 ~ Eff. Jan. 1, 2015**

“Pending” SC Legislation

S.1086 – would amend:

- § 1-11-490 (State Agency Breach)
- § 39-1-90 (Breach of Business Data)
- Require:
 - **The breach notice provided to affected consumers describe the breach – certain elements***
 - **Breach notices include contact information for SCDCA**
 - **Delete provision(s) that agency/business may adhere to its own policy re notification (“quasi-safe harbor”)**
 - **Notification delay ~ shall not exceed 72 hours unless AG grants additional delay (state agency only!)**

S.1086 cont...

***Certain elements:**

- Clear and conspicuous
- Description of the incident in general terms
- Description of the type of PII believed to have been subject to unauthorized access and acquisition
- Description of general acts of business/agency to protect PII from further access
- Telephone number for the business/agency a person may call for more info

Wrap-Up

SCDCA as a Resource

- **ID Theft Scenarios:**

- Security Breach @ Your Agency
- Security Breach of a Business
- Victim of ID Theft
- Partnerships
- FIFITPA Guide – ***coming soon!***



More Info ~ Identity Theft

[WWW.CONSUMER.SC.GOV](http://www.consumer.sc.gov)

SC.GOV Online Services Agency Listing Search consumer.sc.gov Search

SOUTH CAROLINA
DEPARTMENT OF CONSUMER AFFAIRS

QUICK LINKS ▶ HOME CONTACT US FILE A COMPLAINT LICENSEE LOOKUP Font Size: A + A - Reset

ABOUT US

CONSUMER INFORMATION

BUSINESS/INDUSTRY INFORMATION

NEWS RELEASES & PUBLICATIONS

LEGAL

PRIVACY STATEMENT

Tweets Follow

SC Consumer Affairs @SCDCA 3h

What you need to know about price gouging as the winter storm approaches! #SEstorm #SCTweetshttp://ow.ly/tw8FQ

Welcome

The South Carolina Department of Consumer Affairs ("Department") is the state's consumer protection agency. In 1974, DCA has more than thirty-five years of experience protecting South Carolina consumers while recognizing those businesses that act honestly and fairly.

The Department accomplishes its mission by: 1.) acting as an effective regulator, 2.) providing complaint mediation services that are unmatched at both state and federal levels, 3.) saving millions for both consumers and small businesses through insurance rate filing intervention, 4.) serving as an educational portal for consumers and businesses alike, and 5) informing the public on effective ways of preventing and mitigating identity theft situations.

Click [here](#) to learn more about the agency.

What's New?

Identity Theft Information

State-Provided Identity Protection Service with

Helpful Links

IDENTITY THEFT RESOURCES

Business Complaint Response Portal

Search Complaints

Credit Card Repayment Calculator

SCBOS Online Filing

Marti Phillips

803-734-4241

mphillips@scconsumer.gov



Toll Free: 1-800-922-1594

Fax: 803-734-4229

www.consumer.sc.gov