



South Carolina's New Privacy Law

The South Carolina Financial Identity Fraud and Identity Theft Protection Act

Presented by Kay Tennyson
Nelson Mullins Riley & Scarborough, LLP
October 7, 2008

Nelson Mullins' publications and programs are intended to provide reference materials about the subject matter for educational purposes. These materials may reflect the views and opinions of individual preparers, or recognizable academic approaches, but are not intended to state the position of the Firm, nor do they represent legal or professional advice. Attorneys using Nelson Mullins' publications or orally conveyed information in dealing with a specific client's or their own legal matters should conduct their own research and analysis as appropriate. Nelson Mullins neither undertakes nor incurs any attorney-client relationship by providing any such publications or information.

Copyright © 2008 Nelson Mullins Riley & Scarborough, L.L.P. All Rights Reserved. These materials may not be reproduced in whole or in part without the express written permission of Nelson Mullins.

Privacy – A Definition

- Privacy, n. The state of being free from intrusion or disturbance.



Six Degrees



Privacy – A Definition

- In today's digital world, however, this term encompasses far more....



Privacy – A Definition

- Privacy means taking care of your own personal information.
- Privacy means taking care of your employees' personal information.
- Most importantly, privacy means . . .

***TAKING CARE OF
SOUTH CAROLINA RESIDENTS'
PERSONAL INFORMATION!***

Privacy Protection: So How Do I Do That?

- The simple answer:



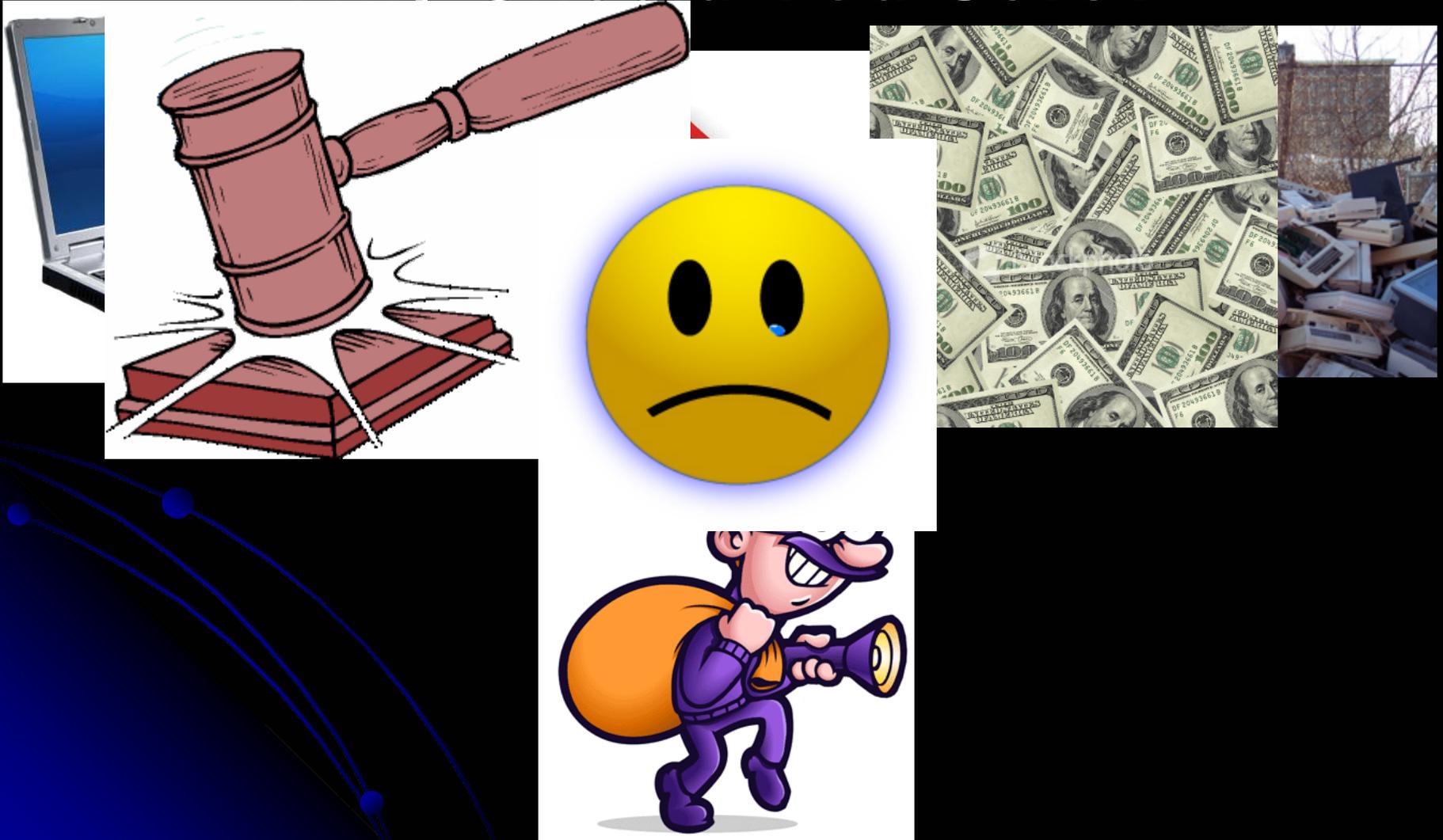
BE PREPARED!

Privacy Protection: Today's Focus

- What information do you have to protect?
- What is a security breach?
- What do you do if you have a security breach?
- What are possible consequences of a security breach?



Privacy Protection: Why Should You Care?



Privacy Protection: But Does This Really Happen?

PENNSYLVANIA
Department of State



STATE OF CONNECTICUT
DEPARTMENT OF MOTOR VEHICLES

Wisconsin Department of
Revenue
revenue.wi.gov

Serving businesses, governments, individuals & practitioners

State of Rhode Island
Department of Administration

Department of
Revenue
Division of Motor Vehicles



FLORIDA DEPARTMENT OF
**CHILDREN
& FAMILIES**

PA pennsylvania
DEPARTMENT OF PUBLIC WELFARE

DEPARTMENT OF PUBLIC WELFARE

Nelson Mullins Riley & Scarborough LLP

The S.C. Financial Identity Fraud and Identity Theft Protection Act



The S.C. Financial Identity Fraud and Identity Theft Protection Act

- Impacts businesses.
- Impacts "public bodies" and "agencies."
- Some portions effective December 31, 2008.
- Breach notification portions effective July 1, 2009.

What Information Do Agencies Have to Protect?

"Personal identifying information." Includes resident's first name/initial, last name combined with one of the following:

- SSN, driver's license or ID card number.
- Financial account number or card number and access code/password that would permit access to financial account.
- Other information allowing access to a person's financial resources or will uniquely ID a person.

What Information Do Agencies Have to Protect?

"Personal identifying information" does not include information lawfully obtained from public information or from government records lawfully made available to public.

If personal data redacted/encrypted, not

- considered "personal identifying information" for purposes of Act.

S.C. Code Ann. § 16-13-510.

How are State Agencies Affected?

- Restrictions on use of social security numbers.
- Requirement to protect personal identifying information during transfer or disposal.
- Requirement to notify when a security breach occurs.

Restrictions on Use of Social Security Numbers

- Restrictions apply to use of full social security number or six or more digits of the number. S.C. Code Ann. § 30-2-310(A)(1)(a).
- Collect only for legitimate purposes or if required by law. S.C. Code Ann. § 30-2-300(2).
- Minimize dissemination. S.C. Code Ann. § 30-2-300(3).
- Do not collect until need for SSNs is clearly documented. S.C. Code Ann. § 30-2-310(A)(1)(a).

Restrictions on Use of Social Security Numbers

DO NOT:

- Make SSNs available to public;
- Imprint on any card required to access government services;
- Require transmission over Internet unless encrypted or the connection is secure;
- Require for access to website unless another authentication device is also used;
- Print on materials mailed to the individual (unless required by law to include). S.C. Code Ann. § 30-2-310(A)(1)(e) – (i).

Restrictions on Use of Social Security Numbers

- *Segregate* social security numbers from other information in a document for easy redaction;
- Upon individual's request, at/before collecting, *provide* a "statement of the purpose or purposes" for which the number is being collected and used.

S.C. Code Ann. § 30-2-310(A)(1)(b)-(c).

Restrictions on Use of Social Security Numbers

- An entity that uses SSNs as part of employment or benefit records is exempt from prohibitions regarding use of SSNs.

S.C. Code Ann. § 30-2-310(A)(2).

- But: Best practices suggest not using if not necessary.

Restrictions on Use of Social Security Numbers

May disclose SSNs only:

- To another governmental entity (if necessary);
- Under court order, warrant, or subpoena;
- For public health purposes;
- On certified copies of DHEC vital records;
- On recorded document in official county/court records *if expressly required* by law, court order, or rule adopted by state registrar on records of vital events;
- To an employer for employment procedures.

S.C. Code Ann. § 30-2-320(1)-(7).

Protecting Personal Information During Transfer or Disposal



Protecting Personal Information During Transfer or Disposal

- Agency must modify personal information by shredding, erasing, or other means. S.C. Code Ann. § 30-2-310(C).
 - Agency may contract with a person whose business is disposing of records to do this. (But, *be sure that company is complying with the law.*) S.C. Code Ann. § 30-2-310(D).

Protecting Personal Information During Transfer or Disposal

- Agency must remove personal information and sanitize information technology hardware and storage media.
 - Must follow standards/policies from SC's Chief Information Officer. S.C. Code Ann. § 30-2-310(B).
- Agency's IT manager must verify that the information has been removed before transfer or disposal.
S.C. Code Ann. § 30-2-310(B).

What is a Security Breach?



What is a Security Breach?

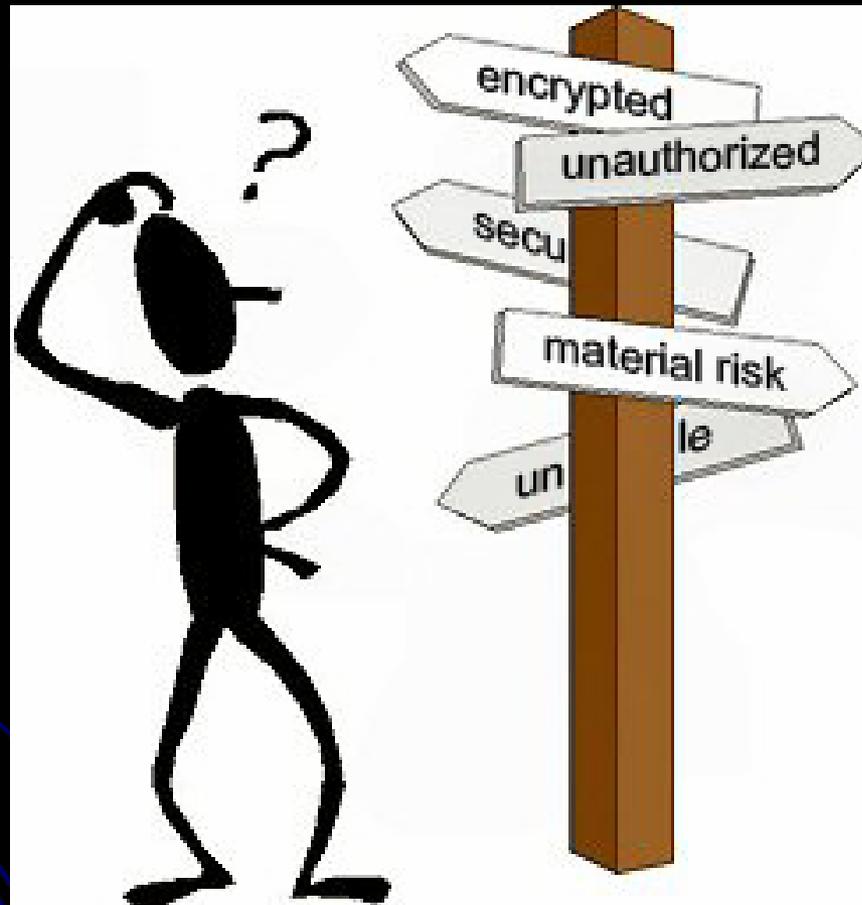


What is a Security Breach?

A "breach of the security of the system" means "unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, 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 a resident."

S.C. Code § 1-11-490(D)(2) (emphasis added).

What is a Security Breach?



What is a Security Breach?

The Act requires action when there has been a "breach of the security of the system."

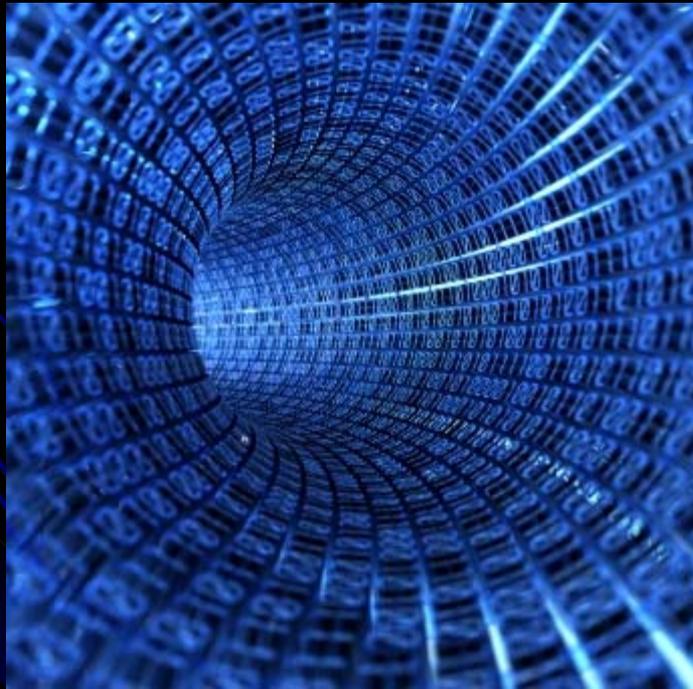
See S.C. Code § 1-11-490(A); (D)(2).

From here, we will use "security breach" to mean a breach "of the security of the system."

What is a Security Breach?

Unauthorized access to and acquisition of computerized data S.C. Code Ann. § 1-11-490(D)(2).

E.g., someone hacked into database; stolen laptop.



What Is a Security Breach?

- Data accessed/acquired was "*usable*."
- If encryption/redaction prevents access to data, it is "unusable," and no "breach" to report.
- If encryption is broken, data has not been rendered "unusable."



What Is a Security Breach?

- May have "breach" if security, confidentiality, or integrity of personal identifying information maintained by the agency is compromised;

Has information been placed in a "compromising position"?

What is a Security Breach?

Unauthorized access;

Usable data;

Compromising position;

If YES to all of these, then what next?

What is a Security Breach?

If Unauthorized access; Usable data;
Compromising position;

THEN CONSIDER WHETHER:

Illegal Use *Has Occurred*;

Illegal Use is *Likely to Occur*;

Potential Use Creates "*Material Risk*" to
consumer.

What is a Security Breach?

If agency has experienced:

- Unauthorized access of usable data (data compromised)

Must Notify IF:

- Illegal use happened or likely to happen

OR

- Material Risk to Resident because of data's compromise.

What is a Security Breach?

An exception.

- Good faith acquisition by the agency or its employee for agency purposes is not a breach of "security of the system"
- Only if the information is not used or subject to further unauthorized disclosure.

S.C. Code Ann. § 1-11-490(D)(2).

Security Breach: Now What?



Security Breach: Now What?

- **Disclose breach to S.C. residents.**
S.C. Code Ann. § 1-11-490(A).
 - If have data as to residents of other states, consider those states' laws regarding notice.
- **For agencies that maintain but do not own the data, notify the owner of the data if the information was acquired by an unauthorized person.** S.C. Code Ann. § 1-11-490(B).
- **If notifying more than 1000 people at one time, must also notify the Dept. of Consumer Affairs and all national consumer reporting agencies.**
S.C. Code Ann. § 1-11-490(I).

Security Breach: Now What?

Timeframe for Notice

- Without unreasonable delay and within the most expedient time possible.
- Consider legitimate needs of law enforcement.
- Time is allowed to identify measures needed to determine scope of breach and restore integrity of data system.
- Delay if impedes criminal investigation. Resume notification after all-clear from law enforcement.

S.C. Code Ann. § 1-11-490(A)&(C).

Security Breach: Now What?

How to Provide Notice

- Writing
- Electronically
 - If consistent with primary way you communicate with individuals
- Telephone
- Substitute Notice
 - Only if cost of providing notice exceeds \$250,000;
 - More than 500,000 people need to be contacted; or
 - Agency has insufficient contact information.

S.C. Code Ann. § 1-11-490(E).

Security Breach: Now What?

Substitute Notice

- Sending e-mails;
- Conspicuously posting the notice on your website; or
- Notifying major statewide media.

S.C. Code Ann. § 1-11-490(E).

Security Breach: Now What?

- Agencies may use their own notification procedure if:
 - Procedure already maintained as part of an information security policy for treatment of personal identifying information; and
 - Consistent with timing requirements of the Act.

S.C. Code Ann. § 1-11-490(F).

Security Breach: Now What?

S.C. Residents Have a Private Right of Action

- S.C. resident "injured" by agency's violation of notice requirement may bring private suit and may recover damages and attorney's fees.
- Residents may also seek an injunction to enforce compliance.
- Knowing and willful violation of the Act makes agency subject to a \$1000 fine for each resident whose information was accessible because of the breach.

S.C. Code Ann. § 1-11-490(G)-(H).

Effective Date of the Act

- S.C. Code Ann. §§ 30-2-300 and 30-2-310 take effect on December 31, 2008.
 - Requirements for using social security numbers
 - Requirements before disposal or transfer
- S.C. Code Ann. § 1-11-490 takes effect on July 1, 2009.
 - Requirements of "breach of security of system"
 - Notice
 - Private right of action

Conclusions

- The S.C. Financial Identity Fraud and Identity Theft Protection Act places significant responsibilities on handling personal information.
- Failure to fulfill your obligations can lead to significant penalties and result in litigation.

Pop Quiz

- Agencies need not disclose a breach if the data was password-protected.
- Agencies may contract the disposal of records containing personal information to a third party.
- Agencies must provide upon request the purposes for which a SSN is being obtained.
- If more than 1,000 people must be notified of a breach, the agency must also notify the Attorney General's office.

