



FEDERAL TRADE COMMISSION

WORKING FOR CONSUMER PROTECTION
AND A COMPETITIVE MARKETPLACE

Identity Theft & Data Security

Paul K. Davis, Attorney
Southeast Regional Office

Legal Landscape

LAWS GOVERNING DATA SECURITY

- **Federal Trade Commission Act (FTC Act)**
- **Gramm-Leach-Bliley Act (GLBA) Privacy Rule/Safeguards Rule/Pretexting**
- **Fair Credit Reporting Act (FCRA)**
- **FACTA / FTC Disposal/Red Flags Rules**
- **Other federal laws:**
 - **HIPAA: medical records**
 - **DPPA: motor vehicle records**
 - **FERPA: student education records**

Legal Standards

FEDERAL TRADE COMMISSION ACT

- **Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.”**
 - **Deception** — Prohibited practices include deceptive claims about the security a company provides for consumer information.
 - **Unfairness** — Requires companies holding sensitive data to have reasonable procedures in place to secure it.

Federal Trade Commission Act

Section 5(a)(1)

Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce are hereby declared unlawful.

DECEPTION THEORY

- **Representation or omission**
- **Interpreted reasonably under the circumstances**
- **Material aspect of the product or service**
- **Likely to cause injury to consumers**
- **Do not need to prove intent**

UNFAIRNESS THEORY

- **Act or practice**
- **Causes consumer injury**
- **Can't be avoided**
- **No countervailing benefit to consumers or competition**
- **Do not need to prove intent**

Legal Standards

GRAMM-LEACH-BLILEY ACT

- **Three main requirements**
 - **Financial privacy (Privacy Rule)**
 - **Security of financial information (Safeguards Rule)**
 - **Pretexting (Section 521)**

GLBA Privacy Rule

- ❑ **Requires financial institutions (or any company that meets the definition) to give privacy notices.**
- ❑ **Opt out notices.**
- ❑ **Limits on use and disclosure of non-public personal information.**
- ❑ **Disclosure of account numbers.**

GLBA Safeguards Rule

- Requires financial institutions to develop and implement appropriate physical, technical, and procedural safeguards to protect customer information.
- Companies must:
 - Develop a written information security plan
 - Designate employee(s) to coordinate safeguards
 - Identify and assess risks to customer information
 - Design and implement a safeguards program (regularly monitor, test, and update it)
 - Oversee service providers
- **CAUTION!** The definition of "financial institution" is broad. (Examples include auto dealers, realtors, tax preparers, & courier services)

Financial Activities-Examples

- ❑ **Lending, exchanging, transferring, investing for others, or safeguarding money or securities.**
- ❑ **Extending credit and servicing loans**
- ❑ **Collection agency services**
- ❑ **Real estate and personal property appraising**
- ❑ **Tax-planning and tax-preparation services**
- ❑ **Financial and investment advisory activities**
- ❑ **Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability or death and acting as principal, agent or broker for purposes of the foregoing.**

Financial Activities-Examples

■ Examples:

- (a) A retailer that extends credit by issuing its own credit card directly to consumers is a financial institution.
- (b) A retailer is not a financial institution if its only means of extending credit are “occasional” deferred payment plans.
- (c) A retailer is not considered a financial institution because it accepts payment in the form of cash, checks, or credit cards that it did not issue.

Financial Activities-Examples

The determining factor will depend upon the number of times an entity extends credit. If an entity “occasionally” extend credit to consumers it will not fall within the definition of a “financial institution.” In addition, if most consumers pay the entity by check, credit card, insurance assignment, the entity will not be regarded as a financial institution simply by occasionally allowing consumers to pay over time.

Financial Activities-Examples

- **Arranging loans for consumers. Companies that serve as a conduit between the consumer and the bank or consumer finance business participating in installment loan programs would be regarded as an agent of the financial institution. As such, the required GLB Act disclosures must be given when the loan application is submitted.**

Financial Activities-Examples

- **Turning delinquent accounts over to collection agencies does not render the company subject to the GLB Act. However, the servicing of delinquent account will.**

Financial Activities-Examples

An overview of the privacy requirements of the GLB Act is available online at the FTC's website, at www.ftc.gov/privacy/glbact/index.html. This guide provides more detailed information that will help you comply with the Privacy Rule's requirements for protecting consumer financial information. The FTC also provides sample disclosures in the appendix to the Privacy Regulations for a funeral home that extends consumer credit through retail installment contracts and does not share private financial information with any non-affiliated third parties.

Exceptions

- **To law enforcement entities or self-regulatory groups (to the extent permitted or required by law)**
- **To comply with Federal, State, or local laws**
- **To a consumer reporting agency**
- **In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit**

Pretexting

- **Practice of obtaining personal information (financial and telephone records) under false pretenses.**
- **Long history of challenging such practices.**
- **Congress enacted GLBA, especially sec. 521.**
- **GLBA specifically prohibits “false, fictitious, or fraudulent statements or representations to an officer, employee, or agent of a financial institution,” or pretexting.**

Pretexting

- **“Spoofing”**: Emails that appears to be from a legitimate organization, like your bank, the IRS, or even the FTC.
 - New attacks on banks/legitimate websites changed
- **Usually contains an attachment that, if opened, plants a Trojan or virus.**

Pretexting

Human Techniques:

- ❑ **Phone impersonation of system admins or Help Desk personnel.**
- ❑ **Phone impersonation of authority figures.**
- ❑ **Physical penetration of office areas.**

Legal Standards

FAIR CREDIT REPORTING ACT

- **Regulates credit bureaus, entities that use credit reports, and the businesses that furnish information to credit bureaus.**
- **Under the FCRA, credit bureaus must “Know their customers” and use “reasonable procedures” to allow access to consumer reports only to legitimate users.**
- **Under the FCRA, a business must:**
 - **Provide ID theft victims with certain info about a fraud without a subpoena (requires a police report).**
 - **Verify the identity of applicants who have fraud alerts on their credit reports.**
 - **Not sell or collect on a fraudulent debt (if a valid ID Theft Report is filed).**
 - **Not report a fraudulent debt to the credit bureaus (if a valid ID Theft Report is filed).**

FCRA Disposal Rule

- **Requires proper disposal of sensitive information derived from consumer reports.**
- **Who?**
 - **Consumer Reporting Companies, lenders, insurers, employers, landlords, mortgage brokers, attorneys and PI's, debt collectors, individuals who maintain information in consumer reports (e.g., for a tenant)**

FCRA Disposal Rule

- **How?**
 - **Burn, pulverize, shred**
 - **Destroy or erase electronic data**
 - **Due diligence in selecting and monitoring contractors.**

“RED FLAG RULES”

- **Required by Fair and Accurate Credit Transactions Act (FACTA)**
- **Joint FTC, Banking Agencies, and NCUA Requirements**
- **Applies to “financial institutions” and “creditors” with personal or household accounts involving multiple payments or transactions.**

DEFINITIONS

- **Financial Institution:** state or national bank, S & L, Credit Union that holds a deposit account or an account where the consumer makes transfers.
- **Creditor:** entity that regularly extends, renews, or continues credit. Includes finance companies, auto dealers, mortgage brokers, utility companies, and telecommunication companies.

BASIC REQUIREMENTS

- **Financial institutions and creditors must develop a written program that identifies and detects relevant warning signs (“Red Flags”) of Identity Theft.**
- **Respond to warnings and update program.**
- **Agencies have published Guidelines suggesting 26 possible red flags.**
- **A starting point, not a checklist.**

Examples

- **Alerts or warnings from a consumer reporting agency.**
- **Suspicious documents.**
- **Suspicious personal identifying information.**
- **Unusual use of or activity in a covered account.**
- **Notices from customers, IDT victims, law enforcement or other businesses.**

FACTA

ID Theft Prevention

- free credit report
- fraud alerts
- require card issuer to investigate COA
- ID Theft red flags
- require proper disposal of consumer report information

FACTA

ID Theft Prevention

- **credit card truncation**
- **CRAs must report address discrepancy to users**
- **truncation of SSN in consumer file disclosure**
- **dormant accounts must be closed & notice of activity in inactive accounts must be given**

FACTA

Victim Assistance

- **businesses must share credit, account, and application info w/ IDT victims**
- **prohibit sale/transfer of IDT debt**
- **trade-line blocking**
- **prohibit “repollution” of credit reports**
- **debt collectors must report IDT to creditor**



DETER · DETECT · DEFEND



www.ftc.gov/idtheft



Avoid ID Theft

How to Deter, Detect, and Defend Against Identity Theft

Presented (insert date)
By (insert organization's name)



DETER



DETECT



DEFEND

WHAT CAN YOU DO?

DETER

- Deter identity thieves by safeguarding your information

DETECT

- Detect suspicious activity by routinely monitoring your financial accounts and billing statements

DEFEND

- Defend against identity theft as soon as you suspect a problem

DETER·DETECT·DEFEND



www.ftc.gov/idtheft

FEDERAL TRADE COMMISSION | 600 PENNSYLVANIA AVE., NW WASHINGTON, DC 20580 | FTC.GOV/IDTHEFT | 1-877-ID-THEFT (438-4338)



DETER



DETECT



DEFEND

DETER identity thieves by safeguarding your information.

- Shred financial documents before discarding them
- Protect your Social Security number
- Don't give out personal information unless you're sure who you're dealing with
- Don't use obvious passwords
- Keep your information secure

DETER · DETECT · DEFEND

AVOID THEFT

www.ftc.gov/idtheft

FEDERAL TRADE COMMISSION | 600 PENNSYLVANIA AVE., NW WASHINGTON, DC 20580 | FTC.GOV/IDTHEFT | 1-877-ID-THEFT (438-4338)



DETER



DETECT



DEFEND

DETECT suspicious activity by routinely monitoring your financial accounts and billing statements.

- Be alert
 - Mail or bills that don't arrive
 - Denials of credit for no reason
- Inspect your credit report
 - Law entitles you to one free report a year from each nationwide credit reporting agencies if you ask for it
 - Online: www.AnnualCreditReport.com; by phone: 1-877-322-8228; or by mail: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281
- Inspect your financial statements
 - Look for charges you didn't make

DETER·DETECT·DEFEND



www.ftc.gov/idtheft

FEDERAL TRADE COMMISSION | 600 PENNSYLVANIA AVE., NW WASHINGTON, DC 20580 | FTC.GOV/IDTHFT | 1-877-ID-THEFT (438-4338)



DETER



DETECT



DEFEND

DEFEND against identity theft as soon as you suspect a problem.

- Place a “Fraud Alert” on your credit reports by calling any one of the three nationwide credit reporting companies:
 - Equifax: 1-800-525-6285
 - Experian: 1-888-397-3742
 - TransUnion: 1-800-680-7289
 - Review reports carefully, looking for fraudulent activity
- Close accounts that have been tampered with or opened fraudulently
- File a police report
- Contact the Federal Trade Commission

DETER·DETECT·DEFEND



www.ftc.gov/idtheft

FEDERAL TRADE COMMISSION | 600 PENNSYLVANIA AVE., NW WASHINGTON, DC 20580 | FTC.GOV/IDTHIFT | 1-877-ID-THEFT (438-4338)



Identity Theft

Consumer Complaint Data

South Carolina

January 1 - December 31, 2007



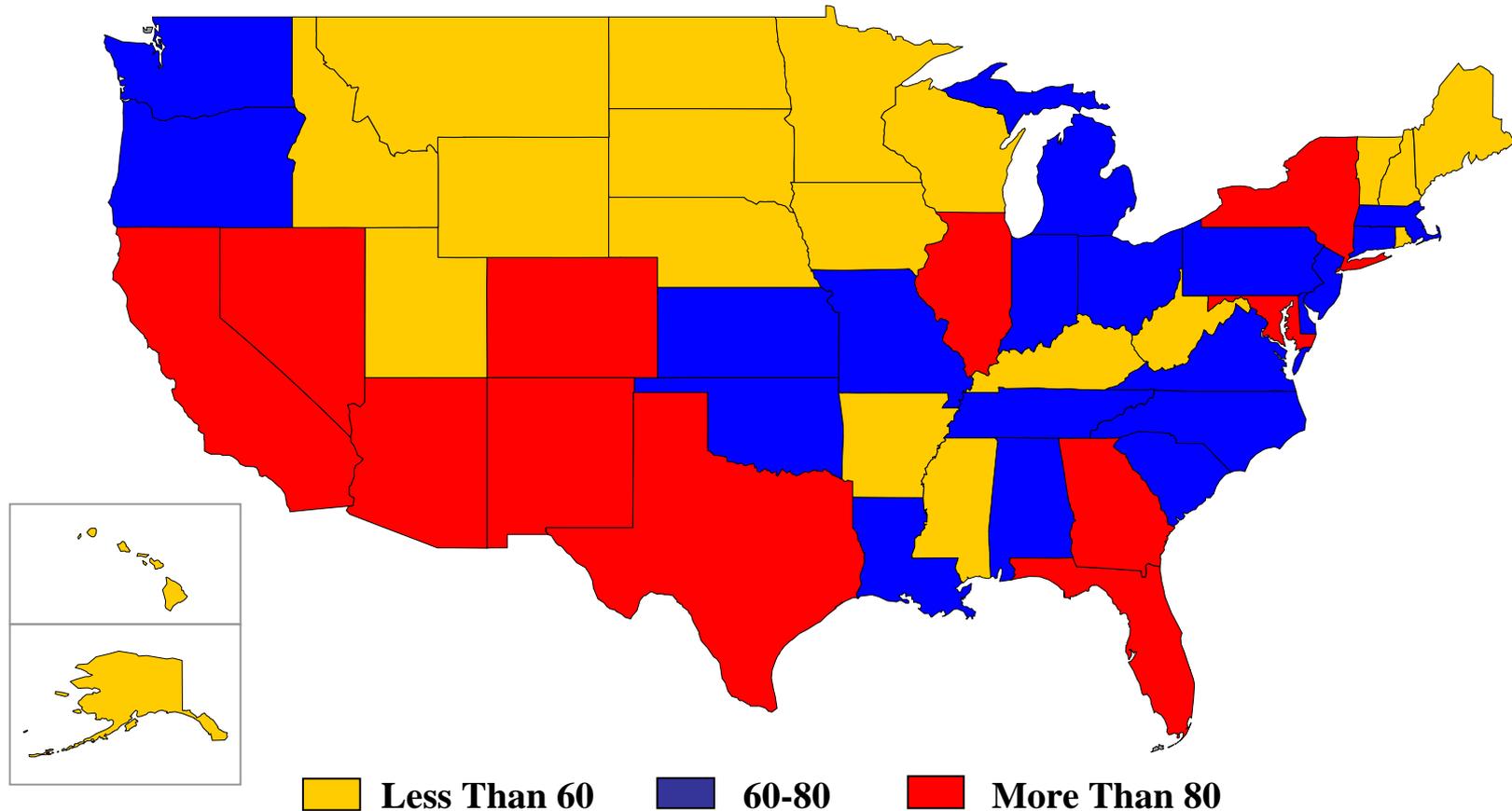
Federal Trade Commission
Washington, DC



Figure 4b

Identity Theft Complaints by State (Per 100,000 Population)¹

January 1 – December 31, 2007



¹These data are not based on a survey; the complaint figures presented are derived from self-reported and unverified consumer complaints contained in the FTC's database. Per 100,000 unit of population estimates are based on the 2007 U.S. Census population estimates (Table NST-EST2007-01 - Annual Estimates of the Population for the United States and States, and for Puerto Rico: April 1, 2000 to July 1, 2007). Numbers for the District of Columbia are 784 complaints and 133.2 complaints per 100,000 population.

Figure 4a



Identity Theft Complaints by State (Per 100,000 Population)¹

January 1 – December 31, 2007

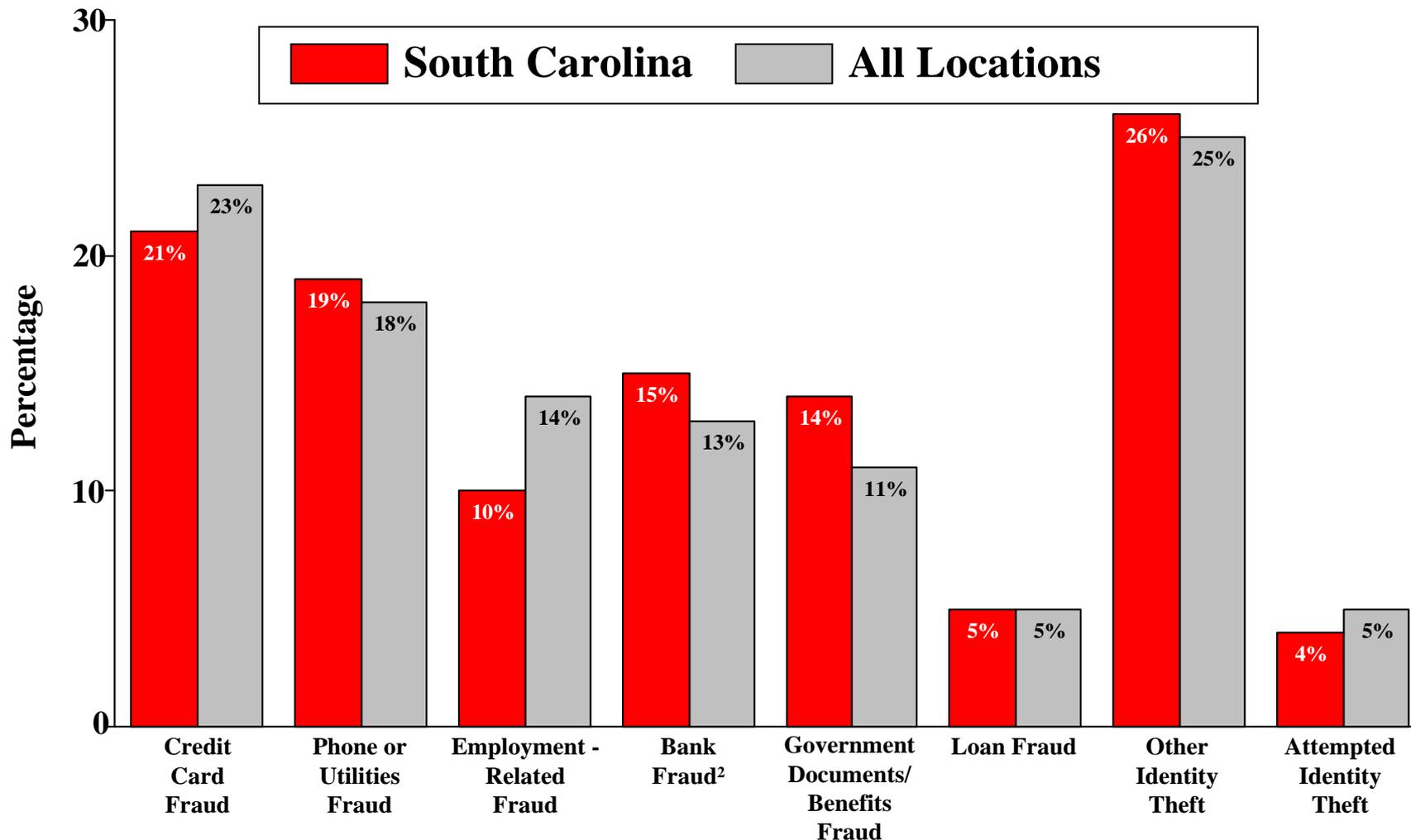
Rank	Consumer State	Complaints Per 100,000 Population	Number of Complaints	Rank	Consumer State	Complaints Per 100,000 Population	Number of Complaints
1	Arizona	137.1	8,688	26	Indiana	63.4	4,026
2	California	120.1	43,892	27	Ohio	62.6	7,178
3	Nevada	114.2	2,930	28	Louisiana	62.3	2,674
4	Texas	107.9	25,796	29	Kansas	61.0	1,694
5	Florida	105.6	19,270	30	South Carolina	60.6	2,670
6	New York	100.1	19,319	31	Utah	57.8	1,529
7	Georgia	91.6	8,744	32	Mississippi	57.3	1,673
8	Colorado	89.0	4,328	33	Arkansas	56.5	1,601
9	New Mexico	87.5	1,723	34	Rhode Island	56.0	592
10	Maryland	85.8	4,821	35	Minnesota	55.0	2,857
11	Illinois	80.2	10,304	36	Idaho	49.2	737
12	New Jersey	79.0	6,864	37	New Hampshire	48.9	643
13	Washington	76.4	4,942	38	Alaska	47.0	321
14	Pennsylvania	72.5	9,016	39	Hawaii	45.9	589
15	Michigan	70.3	7,079	40	Nebraska	44.7	793
16	Delaware	69.7	603	41	Wisconsin	43.7	2,450
17	Alabama	69.6	3,221	42	Kentucky	43.3	1,836
18	Virginia	69.0	5,319	43	Wyoming	42.5	222
19	Connecticut	68.8	2,409	44	Montana	40.8	391
20	Oregon	68.1	2,552	45	Maine	40.2	530
21	Missouri	67.4	3,962	46	West Virginia	40.2	729
22	North Carolina	67.0	6,069	47	Vermont	38.1	237
23	Massachusetts	66.5	4,292	48	Iowa	35.6	1,063
24	Tennessee	64.7	3,986	49	South Dakota	30.8	245
25	Oklahoma	63.9	2,312	50	North Dakota	28.5	182

¹These data are not based on a survey; the complaint figures presented are derived from self-reported and unverified consumer complaints contained in the FTC's database. Per 100,000 unit of population estimates are based on the 2007 U.S. Census population estimates (Table NST-EST2007-01 - Annual Estimates of the Population for the United States and States, and for Puerto Rico: April 1, 2000 to July 1, 2007). Numbers for the District of Columbia are 784 complaints and 133.2 complaints per 100,000 population.

Figure 1

How Consumers' Information Is Misused¹

January 1 – December 31, 2007



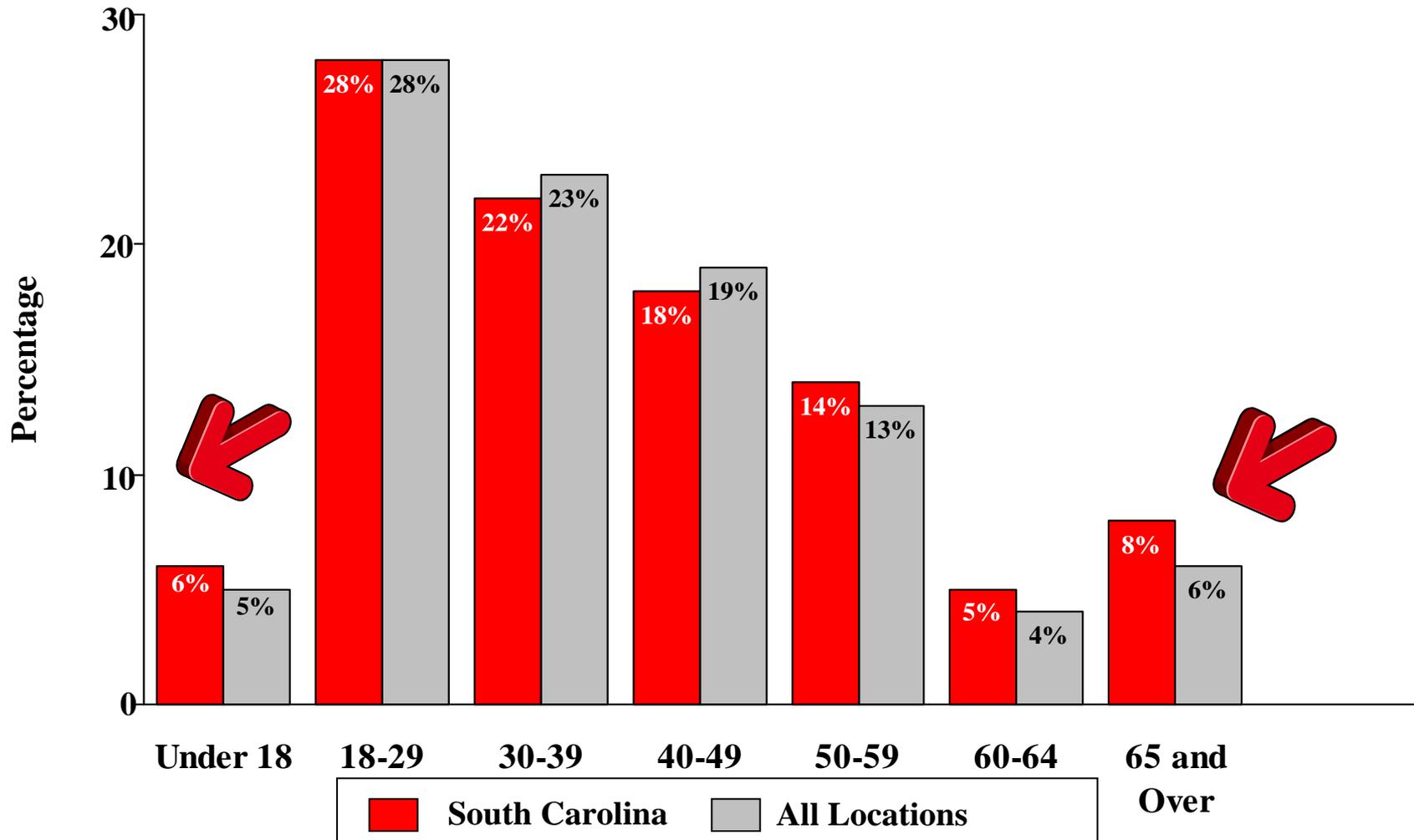
¹These data are not based on a survey; the complaint figures presented are derived from self-reported and unverified consumer complaints contained in the FTC's database. Percentages are based on the total number of complaints in the Identity Theft Data Clearinghouse: 2,670 from South Carolina consumers and 258,427 from consumers in all locations. Note that 16% of identity theft complaints from South Carolina consumers and from consumers in all locations include more than one type of identity theft.

²Includes fraud involving checking and savings accounts and electronic fund transfers.



Figure 3 Complaints by Consumer Age¹

January 1 – December 31, 2007

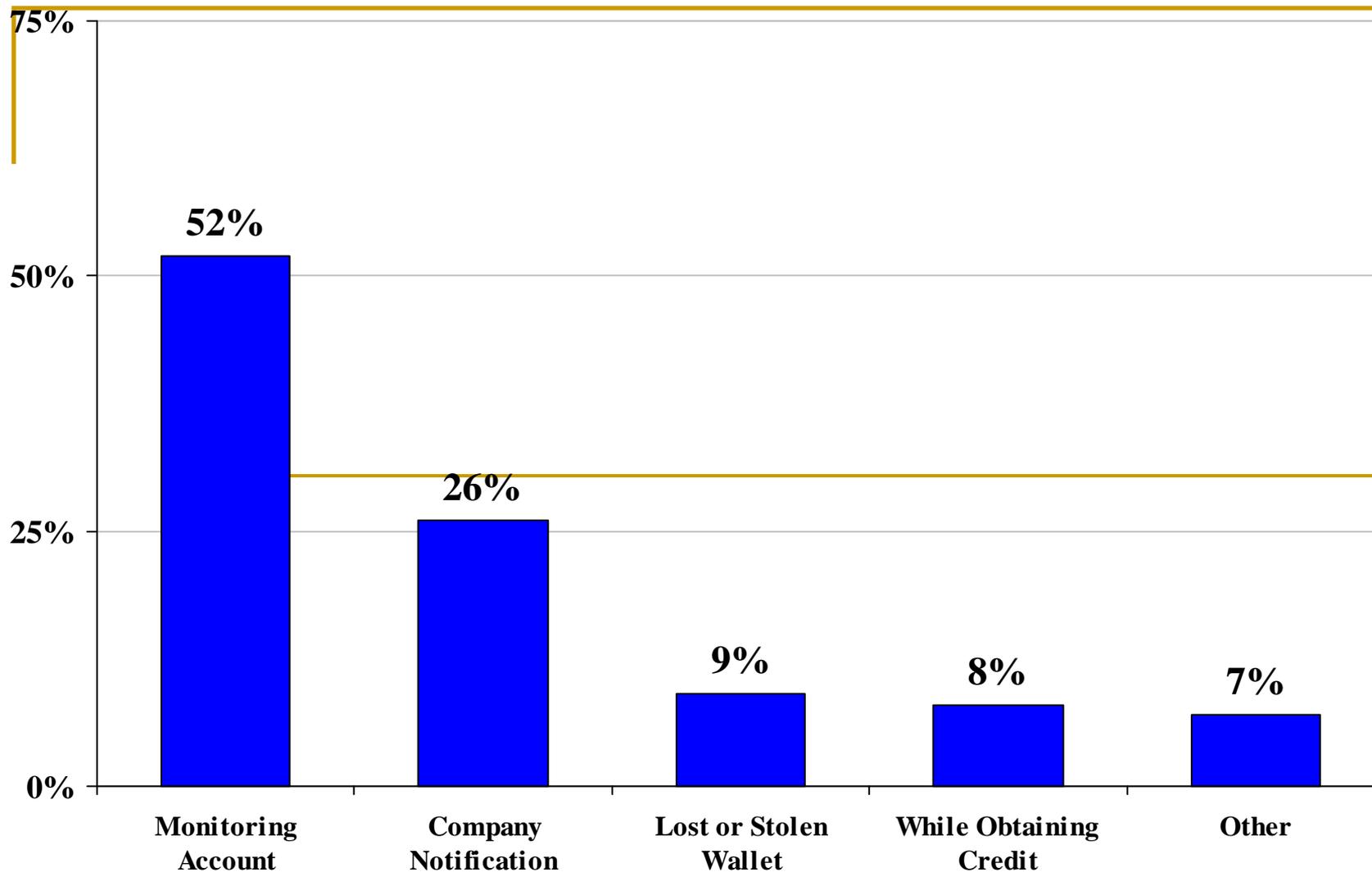


¹These data are not based on a survey; the complaint figures presented are derived from self-reported and unverified consumer complaints contained in the FTC's database. Percentages are based on the number of identity theft complaints where consumers reported their age: 2,500 from South Carolina consumers and 231,576 from consumers in all locations. 96% of consumers from South Carolina and 95% of consumers from all locations who contacted the Federal Trade Commission directly reported their age.



Federal Trade Commission
September 2003

How Victims Discovered ID Theft¹

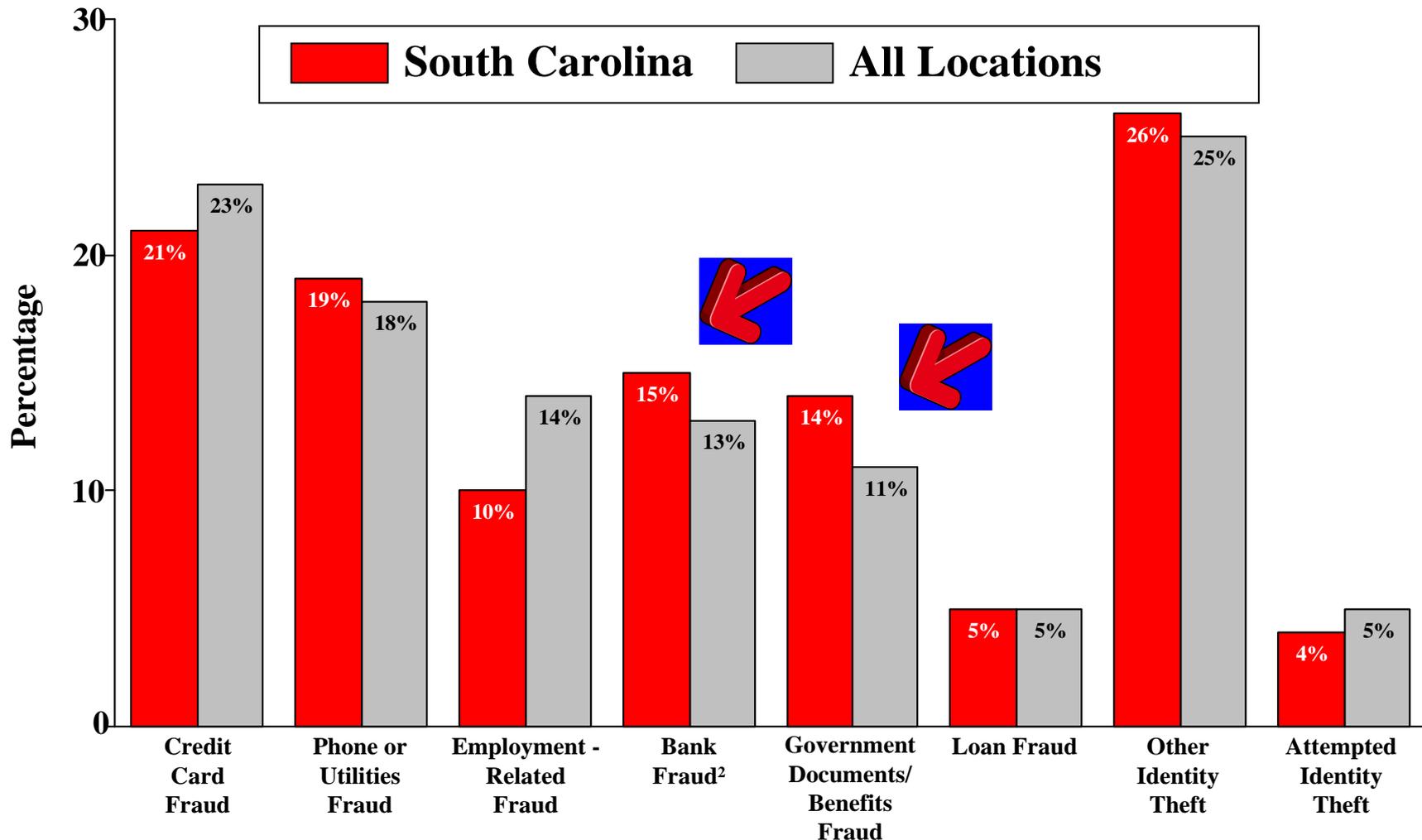


¹Source: Identity Theft Survey Report conducted by Synovate for the FTC (March-April 2003). Percentages based on respondents who indicated they had been the victim of identity theft within the past five years.

Figure 1

How Consumers' Information Is Misused¹

January 1 – December 31, 2007



¹These data are not based on a survey; the complaint figures presented are derived from self-reported and unverified consumer complaints contained in the FTC's database. Percentages are based on the total number of complaints in the Identity Theft Data Clearinghouse: 2,670 from South Carolina consumers and 258,427 from consumers in all locations. Note that 16% of identity theft complaints from South Carolina consumers and from consumers in all locations include more than one type of identity theft.

²Includes fraud involving checking and savings accounts and electronic fund transfers.

IDT - STATE V. COLUMBIA MSA

Type of IDT	STATE	MSA
Credit Card Fraud	21%	23.3%
Phone/Utilities Fraud	19%	19.5%
Bank Fraud	15%	16%
Gov't Docs/Benefits Fraud	14%	14%
Employment Related Fraud	10%	10.5%
Loan Fraud	5%	4.7%

FRAUD - STATE V. COLUMBIA MSA

Type of Fraud	STATE	MSA
Shop at Home/Catalog	10%	9.7%
Foreign Money Offers	8%	8.3%
Internet Services	7%	7.9%
Prizes/Sweepstakes/Lotteries	6%	6.3%
Computer Equip./Software	6%	4.2%

IDT - STATE V. CHARLESTON MSA

Type of IDT	STATE	MSA
Credit Card Fraud	21%	22.4%
Phone/Utilities Fraud	19%	19.0%
Bank Fraud	15%	14.1%
Gov't Docs/Benefits Fraud	14%	14.3%
Employment Related Fraud	10%	7.9%
Loan Fraud	5%	7.5%

FRAUD - STATE V. CHARLESTON MSA

Type of Fraud	STATE	MSA
Shop at Home/Catalog	10%	10.5%
Foreign Money Offers	8%	8.3%
Internet Services	7%	7.3%
Prizes/Sweepstakes/Lotteries	6%	6.7%
Computer Equip./Software	6%	
Internet Auctions		5.4% 

IDT - STATE V. GREENVILLE MSA

Type of IDT	STATE	MSA
Credit Card Fraud	21%	19.3%
Phone/Utilities Fraud	19%	19.5%
Bank Fraud	15%	17.1% 
Gov't Docs/Benefits Fraud	14%	12.1%
Employment Related Fraud	10%	11.2%
Loan Fraud	5%	4%

FRAUD - STATE V. GREENVILLE MSA

Type of Fraud	STATE	MSA
Shop at Home/Catalog	10%	10.8%
Foreign Money Offers	8%	6.7%
Internet Services	7%	8.3% 
Prizes/Sweepstakes/Lotteries	6%	5.7%
Computer Equip./Software	6%	5.9%

IDT - STATE V. MYRTLE BEACH MSA

Type of IDT	STATE	MSA
Credit Card Fraud	21%	26.2% 
Phone/Utilities Fraud	19%	16.9% 
Bank Fraud	15%	12.8% 
Gov't Docs/Benefits Fraud	14%	14.4%
Employment Related Fraud	10%	6.7%
Loan Fraud	5%	3.6%

FRAUD - STATE V. MYRTLE BEACH MSA

Type of Fraud	STATE	MSA
Shop at Home/Catalog	10%	7.6% 
Foreign Money Offers	8%	6.5% 
Internet Services	7%	4.7% 
Prizes/Sweepstakes/Lotteries	6%	5.3% 
Computer Equip./Software	6%	15.9% 

IDT - STATE V. SPARTANBURG MSA

Type of IDT	STATE	MSA
Credit Card Fraud	21%	19.2%
Phone/Utilities Fraud	19%	13.3% 
Bank Fraud	15%	17.1% 
Gov't Docs/Benefits Fraud	14%	14.6%
Employment Related Fraud	10%	9.2%
Loan Fraud	5%	3.7%

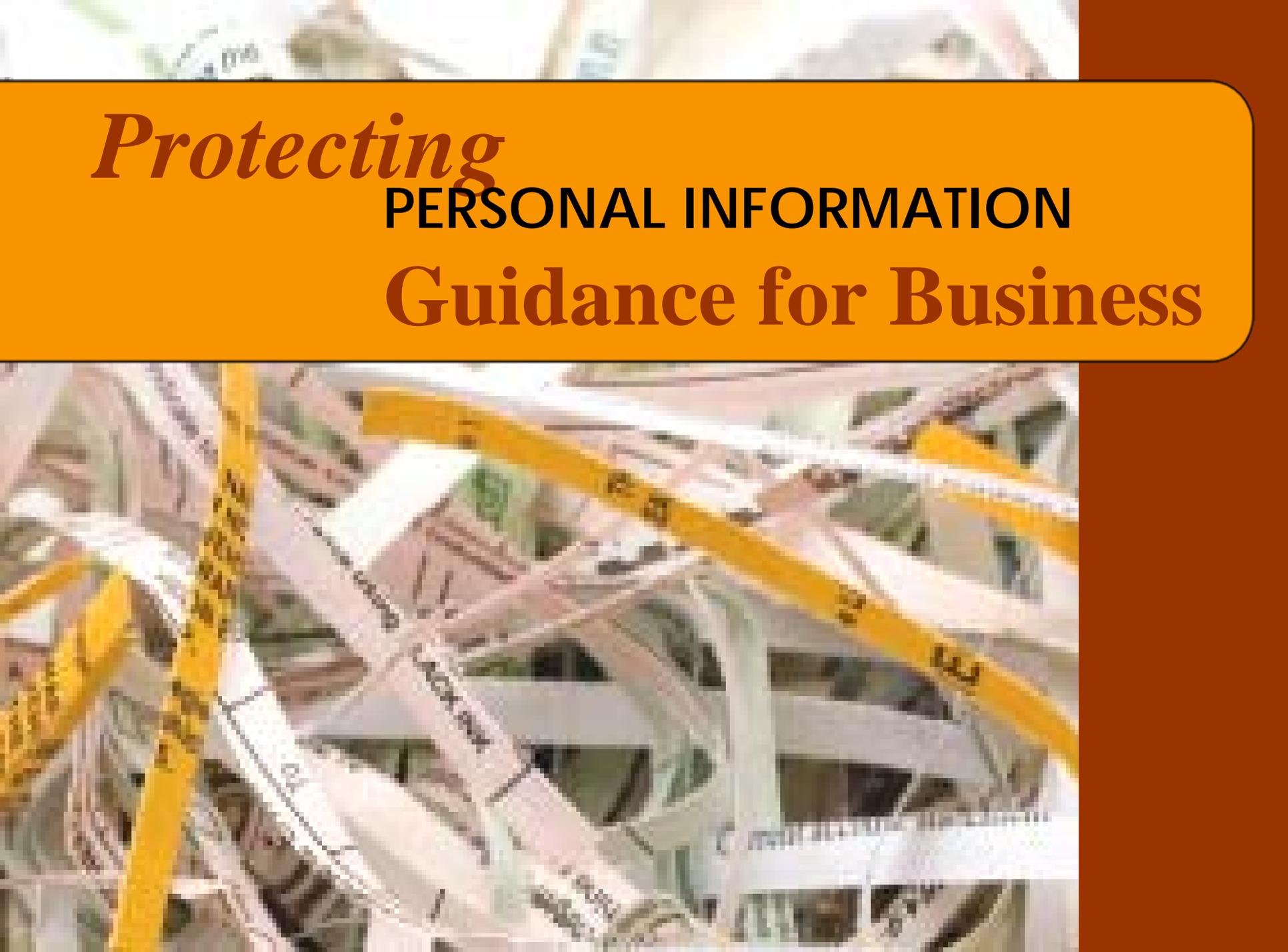
FRAUD - STATE V. SPARTANBURG MSA

Type of Fraud	STATE	MSA
Shop at Home/Catalog	10%	12.8% 
Foreign Money Offers	8%	6.1%
Internet Services	7%	7.8%
Prizes/Sweepstakes/Lotteries	6%	5.9%
Computer Equip./Software	6%	6.9%

Assisting Identity Theft Victims

- **Toll-free phone number for victims**
1-877-ID THEFT (438-4338)
 - **Callers receive counseling from trained personnel who provide guidance and advice**
- **Web site:**
www.consumer.gov/idtheft
 - ***Online complaint form***
 - ***Education***





Protecting

PERSONAL INFORMATION

Guidance for Business

Five Key Principles



1. Take stock.

2. Scale down.

3. Lock it.

4. Pitch it.

5. Plan ahead.

1) Take Stock.

Know what personal information you have in your files and on your computers.

- 
- Check files and computers for:
 - What information you have; and
 - Where it's stored. Don't forget cell phones, PDAs, offsite locations, and employees' home offices.
 - At every stage, determine who has access – and who should have access.

2) Scale down.

Keep only what you need for your business.

- Collect only what you need and keep it only for the time you need it.
- Don't use Social Security Numbers unnecessarily.
- Scale back on what you store on devices connected to the Internet.
- Scale down access.



3) Lock it.

Protect the information you keep.

TRAINING & OVERSIGHT

- Train employees and contractors about safe information security practices.
- Build training into hiring and orientation.
- Get tips, tutorials, and quizzes at www.OnGuardOnline.gov.



3) Lock it.

Protect the information you keep.

COMPUTER SECURITY

- Remember the basics: firewalls, strong passwords, and antivirus software.
- Use caution when storing information on a laptop, PDA, or cell phone.
- Check expert websites like www.sans.org and vendor websites for alerts and updates.
- Work with your Tech Team on network security.



3) Lock it.

Protect the information you keep.

PHYSICAL SECURITY

- Lock desks and drawers.
- Limit access to sensitive files.
- Train employees to keep personal information and facilities locked.
- Secure data that's shipped or stored offsite.



4) Pitch it.

Properly dispose of what you no longer need.

- 
- Shred, burn, or pulverize paper records you don't need.
 - Use wipe utility programs on computers and portable storage devices.
 - Place shredders around the office.
 - If you use consumer credit reports, you may be subject to the FTC's Disposal Rule.

5) Plan ahead.

Create a plan to respond to security incidents.

- 
- Put together a “What if?” plan in case of a security breach.
 - Designate a senior staff member to coordinate your response.
 - Investigate incidents right away.
 - Take steps to close off vulnerabilities.
 - Be cognizant of data breach statutes.

Free resources:

www.ftc.gov/infosecurity

STEPS YOU CAN TAKE NOW

- Bulk order free copies of *Protecting Personal Information: A Guide for Business* for your staff.
- Download articles – not copyrighted! –for client newsletters, websites, or business publications.
- Get buttons and banners to link to *www.ftc.gov/infosecurity*.
- Use the FTC's 20-minute online tutorial as part of your company training. Include all your staff: Receptionists, HR, accounting, IT, sales personnel, temps, etc.



CONTACT THE FTC

- Toll-free phone number for ID Theft victims
1-877-ID THEFT (438-4338)
Web site: www.consumer.gov/idtheft
- Toll-free phone number for consumer complaints and information
1-877-FTC HELP (382-4357)
Web site: www.ftc.gov



Law Enforcement

DECEPTIVE SECURITY PROMISES: FTC Act Section 5 Violations

■ Tower Records

- ❑ Promised users of its website that their personal information would be protected
- ❑ Introduced security vulnerabilities that allowed access to names, addresses, phone numbers and purchasing histories.



■ DSW Shoe Warehouse

- ❑ Failed to employ reasonable and appropriate security measures to prevent unauthorized access to credit and debit card magnetic stripe information collected from customers at its stores
- ❑ Allowed hackers to gain access to the information of more than 1.4 million customers, resulting in fraudulent charges.



Law Enforcement

GRAMM-LEACH-BLILEY SAFEGUARDS RULE

- Superior Mortgage
 - ❑ Failed to establish an information security program as required by the Rule.
 - ❑ Misrepresented that sensitive mortgage application information was encrypted before being sent by email.
- National Title Agency
 - ❑ Promised consumers they would protect their confidential financial information.
 - ❑ Tossed consumer's home loan applications in an open dumpster.



Law Enforcement

FTC ACT ORDERS (generally)

- Prohibit misrepresentations about the extent to which company protects the security, confidentiality, or integrity of personal information it collects from or about consumers.
- Companies must establish a comprehensive information security program that includes administrative, technical, and physical safeguards.
- Must obtain a security assessment from a qualified third party for a period of years.
- Must file annual compliance reports with FTC.
- Future violations subject to Civil Penalties.

Law Enforcement

CHOICEPOINT CASE

- Credit Reporting Agency failed to use reasonable procedures to screen prospective subscribers and monitor their access to sensitive consumer data, in violation of FCRA & FTC Act.
- These failures allowed identity thieves posing as legitimate businesses to obtain access to the personal information of over 160,000 consumers
- The complaint against ChoicePoint alleges approximately 800 cases of identity theft that arose out of these incidents.
- Record \$10 million civil penalty and \$5 million consumer redress for identity theft victims.



Four Points that Guide the FTC's Information Security Enforcement

1. Information security is an ongoing process.
2. A company's security procedures must be reasonable and appropriate in light of the circumstances.
3. A breach does not necessarily show that a company failed to have reasonable security measures – there is no such thing as perfect security.
4. A company's practices may be unreasonable and subject to an FTC enforcement even without a known security breach.