

South Carolina Department of Consumer Affairs

**FINANCIAL IDENTITY FRAUD AND
IDENTITY THEFT PROTECTION ACT
WORKSHOP**

Panel 2

Responding to Data Security Breaches

**Kathleen Goodpasture Smith
Haynsworth Sinkler Boyd, P.A.
October 7, 2008**

**Haynsworth
Sinkler Boyd, P.A.**

ATTORNEYS AND COUNSELORS AT LAW

Responding to Data Security Breaches

- Do not panic
- Do not overreact or under react
- Review requirements of **SC Financial Identity Fraud and Identity Theft Protection Act** as explained by earlier panelist
- Put yourself in shoes of person(s) whose identity has been compromised

(Federal) Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

- May be helpful as example in responding
- Applies to financial institutions
 - Banks, thrifts, credit unions
- Issued by federal financial institution regulatory agencies
 - Office of Comptroller of Currency, Federal Reserve Board, Federal Deposit Insurance Corporation, Office of Thrift Supervision
- Effective March 29, 2005
- 70 FR 15736

(Federal) Interagency Guidelines Establishing Information Security Standards

- Basis for later Interagency Guidance on Response Programs
- Issued by federal financial institution regulatory agencies February 1, 2001
 - OCC, FRB, FDIC, OTS
- Gramm-Leach-Bliley Act § 501(b) required standards to ensure security and confidentiality of customer information

(Federal) Information Security Standards (cont'd)

- Require financial institutions to:
 - Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information
 - Assess likelihood and potential damage of these threats
 - Assess sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risk

Minimum Components of Response Program

- Assess nature and scope of incident identifying:
 - Customer information systems accessed or misused
 - Types of customer information accessed or misused
- Notify primary federal regulator as soon as possible
 - Compare to SC requirement to notify Department of Consumer Affairs and consumer reporting agencies in certain circumstances

Minimum Components/Steps to Contain and Control Incident

- Prevent further unauthorized access
- Take appropriate steps as applicable
 - Monitor accounts
 - Freeze accounts
 - Close accounts
 - Preserve records and other evidence
 - Notify customers when warranted
 - Compare to SC requirement on notification to SC residents

Minimum Components/Customer Notice

- Affirmative duty to protect customer information against unauthorized access or use
- Timely notice to:
 - Manage reputation risk
 - Reduce legal risk
 - Maintain good customer relations
 - Enable customers to take steps to protect against consequences of identity theft

Minimum Components/Customer Notice (cont'd)

- After unauthorized access, reasonable investigation to promptly determine likelihood information has been or will be misused
 - If misuse occurred or reasonably possible, notify affected customers as soon as possible
- Notice may be delayed if appropriate law enforcement agency determines notice will interfere with criminal investigation and provides written request to delay
 - Notify customers as soon as it will not interfere with investigation

Minimum Components/Customer Notice (cont'd)

- Affected customers
 - May limit notice to these if can determine precisely
 - If unable to determine, notify all in group
- Third party service provider
 - If service provider involved, responsibility on financial institution to provide notice (but may contract for provision of notice)

Minimum Components/Customer Notice/Contents

- Clear and conspicuous
- Describe incident in general terms
- Describe type of customer information affected
- Describe steps taken to protect information from further unauthorized access
- Include telephone number for further information and assistance
- Remind customers to remain vigilant over 12 to 24 months and promptly notify financial institution of suspected identity theft

Minimum Components/Customer Notice/Contents (cont'd)

- Include additional items as appropriate
 - Recommend review account statements and report suspicious activity
 - Describe and explain fraud alerts customer may place in consumer reports
 - Recommend periodic free credit reports
 - Inform about FTC guidance

Minimum Components/Customer Notice (cont'd)

- Deliver by any manner designed to ensure customer reasonably expected to receive it
 - Telephone
 - Mail
 - E-mail if valid e-mail address and customer has agreed

Responding to Data Breaches

- Remember Rule Number 1
 - **DO NOT PANIC!**
- Remember Rule Number 2
 - Review requirements of **SC Financial Identity Fraud and Identity Theft Protection Act** and comply!

THANK YOU!

Kathy Smith

Haynsworth Sinkler Boyd, P.A.

803-540-7903

ksmith@hsblawfirm.com

Haynsworth
Sinkler Boyd, P.A.

ATTORNEYS AND COUNSELORS AT LAW