

**MORTGAGE BANKERS ASSOCIATION
LEGAL ISSUES IN MORTGAGE
TECHNOLOGY CONFERENCE**

November 15 - 17, 2006

Phoenix, Arizona

**2006 Federal Developments in Data Information
Security**

Presented by:

**Melissa L. Richards, Esq. Shareholder, Buchalter Nemer
General Counsel, California Mortgage Bankers Association**

Sandra P. Thompson, Ph.D., Esq. Shareholder, Buchalter Nemer

Federal Trade Commission Press Release: January 26, 2006

ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress

At Least 800 Cases of Identity Theft Arose From Company's Data Breach

Consumer data broker ChoicePoint, Inc., which last year acknowledged that the personal financial records of more than 163,000 consumers in its database had been compromised, will pay \$10 million in civil penalties and \$5 million in consumer redress to settle Federal Trade Commission charges that its security and record-handling procedures violated consumers' privacy rights and federal laws. The settlement requires ChoicePoint to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to establish and maintain a comprehensive information security program, and to obtain audits by an independent third-party security professional every other year until 2026.



Framework of Existing Federal Laws and Rules

Title V, Gramm Leach Bliley Act -- Added to S. 900 for the purpose of ensuring that each "*financial institution*" has an affirmative obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. Directs the FTC, among other state and Federal banking and insurance agencies to finalize privacy regulations covering these areas:

- ◆ to ensure the security and confidentiality of customer records and information;
- ◆ to protect against any anticipated threats or hazards to the security or integrity of such records; and
- ◆ to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.



Framework of Existing Federal Laws and Rules

FTC Safeguards Rule [16 CFR Part 314] – This rule implementing GLB Act, effective May 23, 2003, directs the financial services industry to design a security program containing the following elements:

- ❑ Designate an employee(s) to coordinate the information security program;
- ❑ Do a risk assessment of the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information and assess the sufficiency of any safeguards in place to control the risks;
- ❑ Design and implement information safeguards to control the identified risks and regularly test or monitor the effectiveness of the safeguard's key controls, systems and procedures;
- ❑ Oversee service providers. Select only those providers capable of maintaining appropriate safeguards for customer information. Require them by contract to implement and maintain safeguards;
- ❑ Evaluate and adjust the information security program in light of testing and monitoring results, any material changes to the operations or business arrangements, or any other circumstances having a material impact on the program.



Framework of Existing Federal Laws and Rules

Section 216 of the FACT Act – Requires FTC, in coordination with other agencies, to issue a Safeguards Rule “requiring any person that maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose to properly dispose of any such information or compilation”.

FTC Disposal Standards Rule [16 CFR Part 682] - This implementing rule, which took effect June 1, 2005, applies to non-bank financial institutions that, for a business purpose, maintain or possess consumer information*, including mortgage lenders and brokers. Its intent is to reduce the risk of consumer fraud and other harms, such as identity theft, which can result from the improper disposal of sensitive consumer information.

*Consumer information does include personal identifiers such as SSN, DL, phone #, email address and physical address.

* Consumer information does not include aggregate information or data that does not identify individuals.

FTC Disposal Standards Rule

“Disposal” Defined [16 CFR 682.1]

- ❑ Discarding or abandonment of consumer information; or
- ❑ The sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored.

Covered entities must ensure that when computer equipment is sold, discarded or donated, all “consumer information” stored in the computer has been properly disposed of.



FTC Disposal Standards Rule

Reasonableness Standard Applied to Disposal [16 CFR 682.3; Notice of Final Rulemaking at 18]

Covered entities must consider the sensitivity of the consumer information, the nature and size of the entity's operations, the costs and benefits of different disposal methods, and relevant technological changes.

Consider policies and procedures that require burning, pulverizing, or shredding of papers containing consumer information.

Implement policies and procedures that require the destruction or erasure of electronic media containing consumer information.

After doing due diligence, entering into a contract with a third party vendor engaged in the business of record destruction that incorporates FTC disposal standards and monitoring the vendor's compliance with those standards.

When using third parties to maintain or otherwise possess your consumer information, execute service contracts that require adherence to FTC disposal standards and actively monitor them for compliance.

Regulatory Guidelines For Depository Institutions, their Holding Companies and Operating Subsidiaries (FRB, OCC, OTS, FDIC, NCUA)

(1) “*Interagency Guidelines Establishing Information Security Standards*” (70 Federal Register 15736, 3/29/05).

<http://www.ots.treas.gov/docs/7/73262.pdf>; *see also*:

<http://occ.treas.gov/consumer/Customernoticeguidance.pdf>

Describes response programs, including customer notification procedures for addressing unauthorized use of customer information that could result in harm to a customer.



Regulatory Guidelines For Depository Institutions, their Holding Companies and Operating Subsidiaries (FRB, OCC, OTS, FDIC, NCUA)

(2) "Interagency Guidelines Establishing Standards for Safe-guarding Customer Information" (66 Federal Register 8616, 2/1/01)

<http://www.occ.treas.gov/fr/fedregister/66fr8616.htm>

Describes standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

Directs banks to oversee Service Provider Arrangements: perform due diligence; contractually require compliance with Guidelines; monitor for compliance.

Regulatory Guidelines For Depository Institutions, their Holding Companies and Operating Subsidiaries (FRB, OCC, OTS, FDIC, NCUA)

Standard for Providing Customer Notice

When becoming aware of an incident of unauthorized access to “sensitive customer information”, the bank should:

- Investigate to promptly determine whether that information has been/will be misused;
- Notify the affected customer(s) of security breach. Notification may be delayed on account of written request by law enforcement investigators.
- “Sensitive customer information” includes name, address, phone #, SSn, DL #, account/credit/debit care #, PIN or password.

Regulatory Guidelines For Depository Institutions, their Holding Companies and Operating Subsidiaries (FRB, OCC, OTS, FDIC, NCUA)

Suggested Content for Customer Breach Notice

- Clear and conspicuous format.
- Description of the incident and the type of customer information that is the subject of unauthorized access or use.
- Describe what has been done to prevent further unauthorized access of customer information.
- Include a toll free telephone # for further information and assistance.
- Remind the customer to remain vigilant over the next 12 to 24 months and promptly report incidents of suspected identity theft to the bank.



Regulatory Guidelines For Depository Institutions, their Holding Companies and Operating Subsidiaries (FRB, OCC, OTS, FDIC, NCUA)

Also when appropriate, advise the customer to:

- regularly review their account statements.
- alert consumer credit reporting agencies of fraud/identity theft incidents.
- periodically review credit reports for discrepancies (and how to get one free credit report per year)
- go to www.ftc.gov or call FTC's toll free number for additional consumer information regarding identity theft.



Federal Legislation Pending-Prior to November, 2006 Election

The 2006 Congress considered over 20 bills addressing data information security. Not one bill was enacted before the November election. The Front Runners were:

Federal Legislation Pending – The Front-Runners

The Financial Data Protection Act of 2005 [H.R. 3997] – Would require all “consumer reporters” handling sensitive financial personal information to provide notice to consumers of data security breaches that are likely to result in harm or inconvenience. Such notice should be designed to help consumers protect themselves and mitigate against the risk of identity theft or account fraud. Breach notices would be furnished to the United States Secret Service, functional regulators, involved third parties, and consumers.

- Adds a new Section 630 to the Fair Credit Reporting Act for data security safeguards.
- Imposes the obligation on consumer reporters to maintain, reasonable policies and procedures to protect the security and confidentiality of sensitive financial personal information relating to any consumer against any loss, unauthorized access, or misuse that is reasonably likely to result in harm or inconvenience to such consumer.



Federal Legislation Pending – The Front-Runners

- Policies and procedures regarding proper disposal of “sensitive financial personal information.”
- Requires an immediate data security breach investigation if the credit reporter-- (A) becomes aware of any information indicating a reasonable likelihood that a data security breach has occurred or is unavoidable; (B) becomes aware of information indicating an unusual pattern of misuse of sensitive financial personal information handled by a consumer reporter indicative of financial fraud; or (C) receives a “consumer notice” [of security breach].



Federal Legislation Pending – The Front-Runners (con't.)

Requires notification of security breach be sent to affected customers.

Content of notice specified:

- a) Description of the type of information and accounts subject to the breach; statement identifying the party responsible, if known, that suffered the breach; date or time period the breach is reasonably believed to have occurred; actions taken by consumer reporter to restore security and confidentiality of breached information; toll free phone # to call for further information; and FTC summary of consumer rights when they become victims of identity theft.
- b) A prominent statement must also be included in the breach notice to the effect that file monitoring will be made available to the consumer free of charge for a period not less than 6 months. Provide a toll free telephone # for consumer to request such service.
- c) No provision for Federal preemption of patchwork of state information security laws and their breach notification requirements.



Federal Legislation Pending – The Front-Runners

The Data Accountability and Trust Act [H.R. 4127] – To require commercial entities whose business is to collect, assemble or maintain data in electronic form containing personal information for sale to a third party- "information brokers" - and those who contract with a third party to do the same, to establish security policies and procedures for the treatment and protection of personal information, and to provide for nationwide notice in the event of security breach. Of note:

- Gives consumers the right to access their files maintained by information brokers, free of charge, one time per year.
- "Personal information" means an individual's name, address, or phone # in combination with 1 or more of the following: SSN, DL#, Financial account number or credit/debit card number with PIN or access code.
- Prohibition on "Pretexting" by information brokers (obtaining personal information by false pretenses).



Federal Legislation Pending – The Front-Runners

The Data Accountability and Trust Act [H.R. 4127] – (Cont'd.)

- Requires information brokers to send breach of security notifications to affected consumers and to FTC. Third party contractors need only provide notification to the information broker. Notice to be given promptly after discovery of security breach, investigation and mitigation.
- Regulates content of security breach notification – description of personal information accessed; toll free telephone # to call; right to receive free credit reports on a quarterly basis for 2 years; contact information for the major credit reporting agencies; and contact information for FTC.
- Encryption “Safe Harbor” gives information brokers an exemption from these requirements.
- **Preempts state information security laws.**



Postscript: November 2006 Election Results

As a result of the November elections, the Democrats have taken control of the House and Senate. With committee and subcommittee chairmanships changing hands, the passage of a Federal data information security bill that preempts the patchwork of state information security laws containing breach notification requirements, is now UNCERTAIN.

For “best practices,” look to Interagency Banking Guidelines. Continue compliance efforts under GLB Act, FCRA and their respective FTC Rules.