

**YOUR CUSTOMER'S PRIVACY RIGHTS:
WHOSE FINANCIAL INFORMATION
IS IT ANYWAY?**

***PRIVACY LEGISLATION AND REGULATION
AFFECTING THE CREDIT PROFESSIONAL***

***SCOTT E. BLAKELEY, ESQ.
BLAKELEY & BLAKELEY LLP
Wells Fargo Bank Tower
2030 Main Street, Suite 210
Irvine, CA 92614
VOICE: 949/260-0612
FAX: 949/260-0613***

***Los Angeles Office
Home Savings Bank Tower
660 South Figueroa Street, Suite 1830
Los Angeles, California 90017
Voice: 213/385-5815
Fax: 213/385-5817***

**E-MAIL: SBLAKELEY@BANDBLAW.COM
INTERNET: www.bandblaw.com**

BLAKELEY & BLAKELEY LLP

FIRM PROFILE: Blakeley & Blakeley LLP represents its creditor clients in the areas of creditor rights, commercial litigation and collection, credit documentation, e-commerce, bankruptcy and out-of-court-workouts. B&B's collective experience and legal and practical understanding of vendors' rights results in cost-effective representation and develops solutions to vendors' problems. B&B's attorneys have extensive experience working with vendors. Members of the firm routinely speak to national industry groups and trade associations concerning creditors' rights and frequently publish articles in national and regional publications concerning creditors' rights.

Scott Blakeley is a partner in the California law firm of Blakeley & Blakeley LLP, where he advises companies around the country regarding creditors' rights, commercial law, e-commerce and bankruptcy law. He was selected as one of the 50 most influential people in commercial credit by Credit Today. He is contributing editor for NACM's *Credit Manual of Commercial Law*, contributing editor for American Bankruptcy Institute's *Manual of Reclamation Laws*, and author of *A History of Bankruptcy Preference Law*, published by ABI. Credit Research Foundation has published his manuals entitled *The Credit Professional's Guide to Bankruptcy*, *Serving On A Creditors' Committee* and *Commencing An Involuntary Bankruptcy Petition*. Scott has published dozens of articles and manuals in the area of creditors' rights, commercial law, e-commerce and bankruptcy in such publications as *Business Credit*, *Managing Credit*, *Receivables & Collections*, *Norton's Bankruptcy Review* and the *Practicing Law Institute*, and speaks frequently to credit industry groups regarding these topics throughout the country. He is a member on the board of editors for the California Bankruptcy Journal, and is co-chair of the sub-committee of unsecured creditors' Committee of the ABI. Scott holds an B.S. from Pepperdine University, an M.B.A. from Loyola University and a law degree from Southwestern University. He served as law clerk to Bankruptcy Judge John J. Wilson.

**YOUR CUSTOMER'S PRIVACY RIGHTS: WHOSE
FINANCIAL INFORMATION IS IT ANYWAY?**

I. Overview

- A. A customer's privacy rights are at the forefront of legislation and regulation, and appear a hot topic into the future
- B. As technology continues to shape the electronic credit department and the ease in which customer information may be collected and shared, a credit professional should be mindful of a customer's privacy rights and enactment of new legislation in this area.
- C. A number of laws have been passed by state legislatures and Congress, and a number are pending, to protect privacy
- D. What is private information?
 - 1. Elusive definition: Does it include information that is publicly available?
- E. Broadly worded legislation that attempts to protect information in a particular context may be interpreted to a general application
- F. Unintended consequence of privacy legislation is to impede sharing of account information of commercial accounts and collection of commercial debts, which may reduce the amount of debt collected and increasing the cost of credit
- G. Privacy legislation limited to individuals may reach commercial credit, such as with sole proprietors, general partners and individual guarantors of business debt
- H. Corporate Free Speech: attempts to outlaw or restrict sale of personal information and public records met with First Amendment right to communicate with customers
- I. Big Five accounting firms and consulting firms launch specialized units that sell privacy audits to comply with new state and federal privacy laws and enforcements of existing laws. Privacy audits to bring in \$2 billion by 2003

BLAKELEY & BLAKELEY LLP

- J. Many companies may be unfamiliar with own information gathering practices and sharing of information, triggering investigations by the FTC
- K. Compliance with new legislation for privacy on the Internet may cost businesses between \$9 billion and \$36 billion
- L. Class action attorneys gear up for new invasion of privacy claims against businesses

II. Recent Theft of Private Information

- A. Theft of Wells Fargo Notifies Consumers Pursuant to SB1386
 - 1. Wells Fargo had to issue its third letter under SB1386 because of theft of confidential information
 - 2. Wells Fargo notified affected customers in letters throughout the nation that they should contact the three major credit bureaus to file a security alert
 - 3. The most recent theft was of four computers containing names, addresses, loan numbers and social security numbers of some Wells Fargo customers with student loans and mortgage escrow accounts
- B. ChoicePoint, Inc. Falls Victim to Con Artists
 - 1. In February 2005, ChoicePoint, Inc., one of the largest collectors of consumer data, notified over 100,000 people outside of California that ChoicePoint fell victim to con artists posing as merchants
 - 2. Checkpoint, Inc., is a spin off of the credit reporting agency Equifax, Inc.
 - 3. Checkpoint allegedly stores over 19 billion public records in its database in suburban Atlanta, Georgia
 - 4. The con artists may have gained access to addresses, phone listings, Social Security numbers and credit card numbers

BLAKELEY & BLAKELEY LLP

5. It is alleged that the con artists operated for over a year, defrauded at least 750 people, and obtained access to over 100,000 consumer records
6. The con artists used multiple fake merchant accounts to gain access to thousands of records
7. Originally ChoicePoint only notified 35,000 people in California of the breach, but after receiving some criticism and discovering the breach of their security included information of people nationwide, they issued the additional notifications to approximately 145,000 consumers
8. This incident highlights the lack of continuity between state and federal laws
9. While California is leading the charge in requiring notification to consumers when their information is illegally obtained, there is no federal law that requires this

C. Westlaw Asked to Suspend Access to People Finder Service

1. United State Senator Charles Schumer of New York asked Westlaw to suspend access to its People Finder database because of fears the system could be easily accessed by identity theft criminals
2. Westlaw claims the People Finder systems has stores information for 230 million people, 139 households, 71 million phone numbers and 160 million Social Security numbers
3. Westlaw states that the People Finder database is only used by a very limited number of specialized customers
4. Schumer's office alleged that the database is available to anyone who is willing to pay for it

D. LexisNexis Group Issues Warning

1. LexisNexis reported that approximately 30,000 records may have been accessed by the unauthorized use of passwords from legitimate subscribers
2. These records included names, addresses and social security numbers

BLAKELEY & BLAKELEY LLP

E. Home Depot Ignores Use of Social Security Information

1. Also in February 2005, Alan R. Sporn obtained a judgment against Home Depot for \$1.15 million after his Social Security number was stolen and used to obtain credit from Home Depot by third parties
2. Sporn discovered a problem when his application to refinance his home was rejected because so many credit inquirers from Home Depot had been made regarding his creditworthiness
3. Home Depot's credit department ignored his concerns and requests to help him clean up his credit report
4. Only after Sporn obtained the judgment and attempted to collect at the bank that handles Home Depot's payroll accounts did Home Depot take notice
5. Home Depot appealed the decision and lost, Home Depot is now exploring additional options to have the decision overturned

III. California Privacy Law/SB1386

A. Purpose

1. SB1386 requires a company that does business in California to notify consumers when there may have been unauthorized access to their electronic personal information
2. SB1386 also requires that safeguards are in place to protect a customer's private information
3. SB1386 is a California statute that may apply to all states. The law is intended to protect customers from the risk of identity theft through notifying them of misuse of their personal information so they can take steps to protect their assets

B. Key Terms of SB1386

1. Electronic Credit Department
 - a. SB1386 applies to those companies that store personal information on computers

BLAKELEY & BLAKELEY LLP

2. What Information is Covered?
 - a. SB1386 covers personal information, which is defined as a person's first and last name, in combination with the Social Security number, credit card number or driver's license number
3. What is a Security Breach?
 - a. SB1386 requires notification upon a security breach
 - b. However, the statute does not define what constitutes a security breach
 - c. The statute requires notification even where the company only suspects there has been a breach
4. Must a Company reside in California?
 - a. SB1386 applies to companies outside of California that do business within the state
 - b. In an extreme example, a company with but a single California customer, and no offices, employees or computers within California, may be required to report a breach of security

C. Notice Requirement

1. SB1386 requires a company give prompt notice to customers after a security breach
2. Notice may be via e-mail or regular mail
3. Should a company fail to disclose a security breach, it may be liable even if the customer's personal information is never used

D. Complying with SB1386

1. If SB1386 applies to your customers, the following steps should be considered.
2. Encryption
 - a. SB1386 may result in companies doing business in California improve their data security

BLAKELEY & BLAKELEY LLP

- b. SB1386 is silent as to the mechanics for detecting and responding to a security breach
- c. However, a company that encrypts the personal data may be exempt from SB1386

3. Privacy Policy and Notices

- a. The credit professional should consider how customer information is stored
- b. People's names, such as with a guarantor or an individual credit card paying customer, should be kept separate from their other personal information, e.g., Social Security number and credit card number
- c. The credit professional should have its company adopt a policy as to notification of California customers in the event of a security breach, storing private information and sharing private information with third parties
- d. To reduce the risk of a security breach, employee access to customers' private financial information should be restricted

4. Security

- a. In addition to privacy notices, SB1386 requires a customer's information is secure. Personal information should be protected by reasonable security safeguards against such risks as loss or unintended disclosure of customers' information

5. Written Manual

- a. The vendor should have a company policy manual advising of its privacy policy.

6. Training

- a. Train credit and sales as to the privacy policy
- b. SB1386 applies to agents of the company cloaked with authority to request personal

BLAKELEY & BLAKELEY LLP

financial information from a customer

- c. Perhaps the biggest risk for a company in this area is the theft of a company laptop
- d. Some companies have employed a Chief Privacy Officer or an information manager to comply with privacy policy

7. Credit Application

- a. The credit application dealing with the sole proprietor and general partner should disclose the policy of keeping personal financial information secure

8. Personal Guarantee

- a. The personal guarantee should likewise disclose the policy of keeping personal financial information secure.

9. Privacy Audit

- a. Big Five accounting firms and consulting firms have launched specialized units that sell privacy audits to comply with legislation
- b. Consultants review a company's computer databases to determine how personal identifiable information is maintained

E. Violation of SB1386

- 1. SB1386 creates the right for customers to sue to recover damages for violation of the statute
- 2. SB1386 is silent as to damages, although a company may see claims for costs associated with identity theft as a result of a security breach, as well as emotional distress and class actions

IV. Gramm-Leach-Bliley Act of 1999/The Financial Services Modernization Act/Title V

A. Purpose

- 1. Repeals the Glass-Steagall Act that separated commercial banking from other businesses

BLAKELEY & BLAKELEY LLP

2. Provides for extensive privacy protections and restrictions on disclosure of information about accounts
 3. Requires safeguards to protect private information
- B. Federal Statute
1. Applies to all states
 2. States may adopt legislation that imposes greater privacy protections
 3. FTC issued rules to prohibit credit bureaus from continuing to sell "header" information
- C. Consumer Legislation
1. Sole proprietors, general partners and individual guarantors of business debt
- D. Key Terms of GLB Act
1. Privacy Duty
 - a. Financial Institution has duty to protect the security of customers' non-public personal information
 - b. Financial Institution may not disclose non-public personal information unless notice provided
 2. What is a Financial Institution?
 - a. Broadly defined: "any institution engaged in the business of providing financial services to customers who maintain a credit . . . relationship with the institution."
 - b. According to rules set forth by the FTC, a business entity that is not a traditional financial institution be "significantly engaged" in financial activities before GLB applies
 - d. Law firms which provide tax related services may be included in the FTC's definition of a financial institution even though they are

BLAKELEY & BLAKELEY LLP

already required to keep all client information confidential

- e. Trans Union credit reporting service files suit against FTC contending it is not a "financial institution" under GLB. Federal court rejects claim, giving FTC discretion in their interpretation of GLB language
- f. FTC broadly interprets statutory language with its regulatory and enforcement powers

3. What is Customer Relationship?

- a. Determine whether compliance with initial privacy notice requirements is necessary
- b. Continuing relationship between FI and party under which the FI provides one or more products that are to be used primarily for personal purposes
- c. If party does not have a customer relationship with a FI, then notice is required only where there is an intent to disclose nonpublic information to third parties
- d. Requires FI to safeguard the privacy of information relating to its customers, requires notice of those safeguards, and limits the ability of FI to disseminate nonpublic information
- e. GLB Does not apply to customers of a financial institution that are corporations or LLC's
- f. GLB does not apply to individuals, such as sole proprietors, when they obtain financial products for business or commercial purposes. Whether credit extended is for commercial purposes may be analyzed under the criteria set forth in Regulation Z and the Truth-In-Lending Act.

4. What is private information?

BLAKELEY & BLAKELEY LLP

- a. Three categories of information:
 - i. Publicly available information: nature, not the source of information, determines whether public information
 - ii. Personally identifiable information: information collected in connection with transaction, including information collected in connection with application. Information includes payment history
 - iii. Nonpublic personal information: personally identifiable financial information that is not publicly available information
- b. FTC views any personally identifiable information provided to FI, even if available from other public sources, covered by GLB Act
- c. Court rules that GLB Act bars credit bureaus from selling "credit headers", which are a consumer's names, address and Social Security number to marketers and information brokers. Prior to GLB Act, information brokers sold information without consent. FTC viewed "credit headers" as "financial information" under GLB Act and court agreed. The header does not include financial information about credit history or bank accounts. FTC views that identifiable information provided to FI, even if available to from other public sources, covered by GLB Act.
- d. What restrictions on commercial credit?
 - i. Sharing account information at credit industry meeting?
 - ii. Providing a credit rating of customer?
 - iii. Reporting delinquent account information to third party credit provider?

E. Notice Requirements

- 1. If GLB applies, steps that must be taken are:

BLAKELEY & BLAKELEY LLP

- a. Initial Notice
 - i. Requires FI to provide an initial notice of their privacy policy and if they will disclose nonpublic personal information
 - ii. Includes disclosing information to affiliates
 - iii. Disclosure must clearly and conspicuously state practice of disclosure and security of nonpublic personal information
 - iv. Electronic notice effective, provided consumer agrees
 - v. Initial notice required by July 1, 2001
 - b. Annual Notice
 - i. Requires FI to provide annual notice whether personal information is to be shared
 - ii. Electronic notice effective, provided consumer agrees
 - c. The notice requirements of privacy policies are intended to allow potential customers the opportunity to review the policies of a FI
 - d. Privacy notices must be in writing, unless customer agrees to receive one in electronic format. Posting of notice on Web site is acceptable if customer agrees
- F. Opt Out Right
- 1. If FI intends to share private information, it must provide party with an opportunity to opt out
 - a. Initial opt out opportunity 30 days after initial notice
 - b. Gives consumers the opportunity to limit how far a financial institution can spread personal information, including monthly income, social security numbers, credit card spending habits and account balances.

BLAKELEY & BLAKELEY LLP

c. Less than 1% have opted out.

G. Customer Consent

1. Some say companies should be required to get explicit consent from customer before sharing personal information.
2. May complicate routine transactions such as loan processing and would ultimately be more costly for the consumer.
3. Certain state agencies refuse to release information of sole proprietors. The State Board of Equalization refuse to release information of sole proprietors holding licenses or permits.

H. Stages of Credit Transaction Subject to GLB Act and Compliance

1. Privacy Policies and Notices
 - a. Inventory of information collected and sharing practices
 - b. Adopt policy as to notification, storing private information and sharing private information
 - i. List of information collected and to be shared that must be disclosed
 - ii. Identify list of customers that receive initial and annual notice
 - iii. Limit employee access to private information
 - c. Protect against threats to records
2. Written Manual. Policy manual within sales and credit department advising of privacy policy
3. Training. Train credit and sales as to privacy policy
 - a. GLB Act applies to agents of the company cloaked with authority to request information from applicant

BLAKELEY & BLAKELEY LLP

4. The Credit Application
 - a. Disclosures. The credit application should disclose the policy of sharing private information
 - b. Consent. The credit application should contain a statement that expressly authorizes sharing of credit information
 5. Guarantee
 - a. The personal or corporate guarantee should expressly authorize the sharing of credit and financial information
 6. Record Retention
 7. Privacy Audit
 - a. Big Five accounting firms and consulting firms launch specialized units that sell privacy audits to comply with legislation
 - b. Consultants review company's computer databases to determine how personal identifiable information is used
- I. Violation of GLB Act
1. Creates liability for anyone who obtains or discloses information, without knowledge of any inappropriate conduct
 2. Liability not limited to party participating in prohibited deception, but extends through the subsequent chain of custody
 3. Defense to Alleged Violation
 - a. Corporate Free Speech: attempts to outlaw or restrict sale of personal information and public records met with First Amendment right to communicate with customers
 - i. Government restriction of sharing of information is slippery slope. Where is the line drawn?

BLAKELEY & BLAKELEY LLP

- ii. Trans Union corporate free speech argument fails: court rules that FTC's interest in protecting privacy rights under GLB Act outweighs First Amendment Rights

J. Regulation and Enforcement of GLB Act

1. Private Enforcement

a. Individual Action

b. Class Action Litigation

- i. Claim for corporation invasion of privacy

- ii. Traditionally, privacy laws protected against invasions by the government, not by business. Case law is dated.

2. Public Enforcement

a. Federal Trade Commission

3. Penalties and Liabilities

a. Criminal penalty: five years

b. Attorneys' Fees and Costs

c. Punitive Damages

V. Bankruptcy

A. Toysmart.com: The Privacy Pledge Problem

- 1. Confidentiality pledge: dot-com enters into agreement with customers that pledges information will remain private. Privacy company certifies website

- 2. Toysmart.com make privacy pledge that customer information will remain confidential. Toysmart runs into financial difficulty and attempts to sell customer list through bankruptcy

- a. FTC sues Toysmart for deceptive trade practice; 39 state attorney generals sue to enjoin sale

BLAKELEY & BLAKELEY LLP

- b. FTC and Toysmart reach settlement to sell to similarly situated company, but bankruptcy court rejects
- c. Disney pays \$50,000 to have customer list destroyed

Privacy Guarantee

[W]e take great pride in our relationships with our customers and pledge to maintain your privacy while visiting our site. Personal information voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party.

- 3. In an attempt to avoid Toysmart's problems of blocking the sale of a customer list, some dot-com e-tailers have changed their privacy statement. Amazon now discloses:

In the unlikely event that Amazon.com, or substantially all of its assets are acquired, customer information will, or course, be one of the transferred assets.

- 4. Egghead.com filed bankruptcy and Fry's Electronics agreed to acquire its assets, including its customer database, for \$10 million. As a condition of the sale, Fry's is requiring that only 10% or fewer of Egghead's active customers opt out of the plan to transfer their personally identifiable data to Fry's.
- 5. Microsoft's new Internet Explorer 6 allows users to screen Web sites according to their privacy policies. The feature can automatically keep your computer from beaming information to Web sites that don't meet certain criteria, and it can summarize a site's privacy practices.

- B. Information on Bankruptcy Petitions

BLAKELEY & BLAKELEY LLP

1. Individual debtors in bankruptcy must provide sensitive information, including account numbers, social security numbers, balances, income sources and payment histories
 2. National database of bankruptcy information to answer creditor inquiries
 3. The Bankruptcy Reform Act of 2001 requires more details concerning individual's income and expenses that would be publicly available
 4. How to safeguard tax returns and wage statements
 5. Whether privacy protection will be afforded sensitive data supplied in bankruptcy cases
- C. Bankruptcy Reform Act of 2001
1. Prohibits companies in bankruptcy from selling their customer lists to raise money to pay creditors
 2. Provides for a consumer privacy ombudsman if the debtor attempts to sell data

VI. Privacy Commission

- A. Commission to make recommendations to Congress on privacy legislation
1. 17 member bipartisan Privacy Protection Commission
 2. 18 months to study privacy issues and report to Congress
 3. Considers both the need for privacy protection and purpose for sharing information, as well as existing legislation and regulation

VII. Fair Credit Reporting Act

- A. Purpose
1. Regulates the use of the individual credit reports and credit information
 2. The collection of business, trade, and commercial credit reports are not covered by the FCRA

BLAKELEY & BLAKELEY LLP

3. The FCRA insures those credit reporting agencies, and the users of such reports, will respect a consumer's right to privacy by pulling consumer credit reports only after express written authorization of the consumer
 4. Intended to protect applicants and to provide accurate information to or about applicants involved in credit transactions
- B. What is a Credit Report?
1. A credit report may be any written or oral report communication bearing on a consumer's credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living
 2. The credit report must be either used or expected to be used, or it must have been collected in whole or in part, for a "permissible purpose."
- C. The FTC Opinion
1. The FTC states that a vendor must obtain the consumer's consent prior to pulling a consumer credit report
 2. However, the FTC makes clear that the scope of the FCRA is limited to credit reports
- B. Legitimate Business Purpose Exception Not Recognized
1. The FTC notes that the business exception "provides no authority for a vendor to obtain a consumer report in connection with a credit application for any commercial purpose." Opinion at p.3.
 2. Credit information providers, such as Experian, are generally not safe harbors for vendors that contract with the information provider for credit reports. The contract between the vendor and the credit information provider generally states that the information provider is not liable for the vendor's failure to obtain a consumer's consent
- C. Relevance of Consumer Reports When Commercial Credit Extensions Are Made To A Corporation, LLC or partnership

BLAKELEY & BLAKELEY LLP

1. Often the payment history of such a corporation is the reflection of the payment history of the officer or the shareholder
 2. To reduce the risk of nonpayment, a credit professional may seek a personal guaranty from a corporate officer or shareholder, or limited liability corporation member, before extending commercial credit. In connection with this guaranty, a credit executive may wish to review the guarantor's personal credit history
- D. Notification If Credit Is Declined Based Upon Credit Report
1. Credit grantor provide notice if the credit grantor is denying credit, or otherwise taking adverse action with respect to the credit application, based upon the information provided by the credit report
 2. The notice can be oral, in writing, or electronic. The credit grantor is required to provide the name, address and telephone number of the consumer-reporting agency
 3. The credit grantor must notify the consumer of the consumer's right to obtain a free copy of the consumer report. Notice must also be provided of the consumer's right to dispute with the consumer-reporting agency the accuracy or completeness of any information in the consumer report
- E. Penalties For Violating FCRA
1. The private enforcement: punitive damages
 2. Criminal penalties may also be assessed including fines and imprisonment against any person who knowingly and willfully obtains a consumer report under false pretenses
- F. Considerations
1. FRCA Authorization Contained In Credit Application
 - a. A separate form, or addendum to accompany the credit application

BLAKELEY & BLAKELEY LLP

- b. The party that the credit professional seeks authorization may not be the same party that signs the credit application
- c. A credit application that provides general authority for the credit professional to pull a consumer credit report on a corporation's officers may be insufficient

The undersigned consents to *[insert: Name of Your Business]* obtaining a consumer credit report on _____ *[insert—name of the sole proprietor/ President/Officer of corporation, LLC, partnership]* for the purpose of evaluating the creditworthiness of _____ *[insert—name of the sole proprietor/ President/Officer of corporation, LLC, partnership]*, in connection with this Application.

Signed By:

*[name of sole proprietor/President/
Officer of corporation/LLC/partnership]*

2. FCRA Authorization Contained In Personal Guarantee

The undersigned consents to *[insert: Name of Your Business]* obtaining a consumer credit report on _____ *[insert—name of the guarantor]* for the purpose of evaluating the creditworthiness of _____ *[insert—name of the guarantor]*, in connection with an application for business credit.

Signed By:

*[type name of guarantor here]
[Social Security Number and home address]*

VIII. Fair Debt Collection Practices Act

- A. Broadly worded privacy legislation may impede collection of debt

IX. Electronic Communications Privacy Act

X. Right to Financial Privacy Act

- A. Financial institution may not provide a federal authority access to financial records of customer, absent consent

XI. Pending Privacy Legislation

A. Federal

- 1. Consumer Internet Privacy Enhancement Act
 - a. Privacy defined to include an individual's name, address and telephone number
- 2. Consumer Privacy Protection Act
- 3. Consumer Online Privacy and Disclosure Act
- 4. Spyware Control and Privacy Protection Act

B. Senator Diane Feinstein Introduces Federal Privacy Legislation

- 1. California Senator Diane Feinstein introduced the Notification of Risk to Personal Data Act in January of 2004
- 2. This act would establish a standard for which businesses and government agencies will be required to notify victims that a criminal has acquired their personal data
- 3. The standard is if there is a reasonable basis to conclude a criminal has acquired personal data
- 4. In addition, Feinstein would like to force brokers to ask for permission from people to sell their sensitive personal information
- 5. Currently, California's SB1386 is the only law that requires companies, if operating in California, to notify consumers if personal information was acquired by unauthorized parties

BLAKELEY & BLAKELEY LLP

- C. State
 - 1. Over 100 privacy bills pending in most states
- D. Industry groups have successfully fought tougher privacy laws in Congress and at state level thus far, however, that may change in the next couple of years

INTERNET SITES	
Anti-Telemarketing Site	www.antitelemarketer.com
Coalition Against Unsolicited Commercial E-Mail	www.cauce.org/about/resources.shtml
Consumers Against Supermarket Privacy Invasion & Numbering	www.nocards.org
Electronic Frontier Foundation	www.eff.org
Electronic Privacy Information Center	www.epic.org
E-mail Scams	www.ftc.gov/bcp/online/pubs/alerts/doznalrt.htm
Federal Trade Commission	www.ftc.gov/privacy/index.html
Kidz Privacy Web Site	www.kidsprivacy.org
Privacy Advice	www.nclnet.org/essentials/privacy.html
Privacy Rights site	www.privacyrights-now.com
Spam	www.junkbusters.com

BLAKELEY & BLAKELEY LLP

Tool	What It Is	Who Offers It	Cost	Comment
Fraud Alert	A warning to companies looking at your credit to be wary of thieves who may be impersonating you.	The three big credit-tracking agencies; Equifax (www.equifax.com ⁷), Experian (www.experian.com ⁸) and TransUnion (www.transunion.com ⁹).	Free	Federal law requires agencies, upon request, to place an alert on accounts for at least 90 days. Extended alerts can last up to seven years.
Credit Freeze	Locks up your credit files at credit-reporting agencies so identity thieves can't open accounts in your name.	Currently only available in California and Texas; coming in July to Vermont and Louisiana. Other states are considering it.	From free to \$10 to freeze your credit report at each agency, and from free to \$8 to unfreeze it.	You'll probably need to unfreeze your report at all three agencies when you want to apply for credit.
Identity Theft Insurance	Covers expenses beyond reclaiming your identity (think lost wages and legal fees).	Everyone from employers and insurers to banks, credit-card companies and credit-score firms.	From free to more than \$40 a year; insurers usually cover up to \$25,000 of expenses.	Some insurers require policyholders to carry a homeowner's or renter's policy, or impose other conditions.
Credit Monitoring	You get an alert when something changes in your credit file.	The big three, plus Fair Isaac, which compiles data into credit scores.	From \$4.95 to \$12.95 a month.	A good early warning of unusual activity, but it's going to cost you.
Paper Shredder	A device available at most office-supply stores that slices your papers into small pieces.	A company called Fellowes, among many others; even Target's Michael Graves line has one.	From \$20 or so to over \$500 for fast, high-capacity cross-cutting models.	An easy, low-cost way to ward off dumpster divers seeking your old credit-card bills.