

**California Privacy Laws & Reports
Relevant to Title Companies and Public Records
(Section One - California)**

I.	Abstracts of Judgment	Pg 3
II.	California Financial Information Privacy Act (CFIPA).....	Pg 4-5
III.	Disclosure of On-Line Privacy Policies	Pg 6
IV.	Disposal of Customer Records	Pg 7 <i>(Note that the FTC disposal rules became effective 6/1/05 and can be found at 16CFR 682)</i>
V.	Disclosure to Consumers of Information Provided to Direct Marketers.....	Pg 8-9
VI.	Notification to Consumers of a Breach of the Security of Data Containing Personal Information	Pg 10
VII.	Disclosures of Social Security Numbers	Pg 11
VIII.	Confidentiality of Addresses of Public Safety Officials.....	Pg 12
IX.	Confidentiality of Addresses for Victims of Domestic Violence and Stalking	Pg 13
X.	California Insurance Information and Privacy Protection Act and Department of Insurance Regulations Adopted Pursuant Thereto	Pg 14-18
XI.	Privacy Protections for Public Safety Officials <i>A Report by the California Department of Consumer Affairs Office of Privacy Protection</i>	Pg 19-23

**Federal Privacy Laws Applicability to Title Companies
(Section Two - Federal)**

I.	Title Company Privacy Rules under the Gramm-Leach-Bliley Act.....	Pg 25-35
II.	Privacy Laws and Underwritten Title Companies.....	Pg 36-42
III.	FTC Rule on Disposal of Consumer Report Information and Records <i>(ALTA Summary)</i>	Pg 43-44

Section One - California

California Privacy Laws & Reports Relevant to Title Companies and Public Records

I. Abstracts of Judgment

Code of Civil Procedure §674

The statute governing the content of an abstract of judgment requires a significant amount of personal information such as the name and last known address of the judgment debtor, the social security number and driver's license of the judgment debtor if known to the judgment creditor, and other names by which the judgment debtor is also known. The abstract may be recorded to establish a judgment lien.

A number of potential conflicts between the statutes governing recordation of an abstract of judgment and the California Financial Information Privacy Act could be resolved by exemptions found in the new law:

- The Act protects only "nonpublic" personal information. All information required in the abstract of judgment might be publicly available from one or another source.
- Disclosure is "necessary to effect, administer, or enforce" the transaction.
- Disclosure is authorized as a "securitization" of the transaction.
- Disclosure is "to comply with federal, state, or local laws, rules, and other applicable legal requirements."

The Commission believes that the new law's exemption for disclosure of information "necessary to effect, administer, or enforce" a financial institution's rights against a consumer is adequate to allow recordation of the kinds of information required by the abstract of judgment law. Further amendment of the new law is unnecessary. *(This is reprinted from Financial Privacy, 34 Cal. L. Revision Commission Reports 401 (2004). This is publication #222. Footnotes have been omitted.)*

II. California Financial Information Privacy Act (CFIPA)

Financial Code §4050-4060

The California Financial Information Privacy Act (also known as SB 1), became effective on July 1, 2004. The law:

- Establishes a three-tiered structure that governs the sharing of non-public personal information. Those tiers include:
 - ☑ Areas where the consumer must provide explicit consent before the information can be shared (opt-in);
 - ☑ Areas where the consumer must be given the opportunity to prohibit the sharing of information (opt-out); and,
 - ☑ Areas where information can be shared without restrictions from the consumer (no-opt).

Important to title companies, the new law incorporates several Gramm-Leach-Bliley Act provisions including non-public personal information not being information from federal, state or local government records. Under the law, non-public personal information does not include publicly available information that the financial institution has a reasonable basis to believe is lawfully made available to the general public from (1) federal, state, or local government records, (2) widely distributed media, or (3) disclosures to the general public that are required to be made by federal, state, or local law. Non-public personal information does include any list, description, or other grouping of consumers, and publicly available information pertaining to them, that is derived using any non-public personal information other than publicly available information, but shall not include any list, description, or other grouping of consumers, and publicly available information pertaining to them, that is derived without using any non-public personal information.

Sharing is allowed when necessary to affect, administer or enforce a consumer transaction. This includes where a disclosure is required in a transaction covered by the federal Real Estate Settlement Procedures Act (12 U.S.C. Sec. 2601 et seq.) in order to offer settlement services prior to the close of escrow (as those services are defined in 12 U.S.C. Sec. 2602), provided that (A) the non-public personal information is disclosed for the sole purpose of offering those settlement services and (B) the non-public personal information disclosed is limited to that necessary to enable the financial institution to offer those settlement services in that transaction.

Also the definition of financial institution tracks the Gramm-Leach-Bliley Act definition. "Financial Institution" means any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 of the United States Code and doing business in this state (The Gramm-Leach-Bliley Act).

The Ninth Circuit Court of Appeals has held that the affiliate-sharing preemption clause in the Fair Credit Reporting Act preempts SB 1 insofar as it attempts to regulate the communication between affiliates of "information," as that term is used in § 1681a(d)(1). That is, SB 1 is preempted to the extent that it applies to information shared between affiliates concerning consumers' "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" that is used,

expected to be used, or collected for the purpose of establishing eligibility for “credit or insurance,” employment, or other authorized purpose. On remand, the Ninth Circuit noted that the district court must determine whether, applying this restricted meaning of “information,” any portion of the affiliate-sharing provisions of SB 1 survives preemption and, if so, whether it is severable from the portion that does not. (American Bankers Association v. Gould No. 04-16560, DC. No. CV-04-00778-MCE June 20, 2005.)

III. Disclosure of On-Line Privacy Policies

Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code.

The statutes governing the security and confidentiality of consumer personal and identifying information obtained by persons and entities engaged in online business transactions seeks to regulate the use of personal information obtained through a web site or online service.

An “operator” is defined as a person or entity that collects “personally identifiable information” from California “consumers” for commercial purposes. Operators are required to conspicuously post their privacy policy on their web site or online service and to comply with that policy.

The privacy policy must identify the categories of personally identifiable information that the operator collects about individual consumers who use or visit its web site or online service and third parties with whom the operator may share the information. “Consumer” means “any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes.”

IV. Disposal of Customer Records

*(Note that the FTC disposal rules became effective 6/1/05 and can be found at 16CFR 682)
Title 1.81 (commencing with Section 1798.80) of Part 4 of Division 3 of the Civil Code.*

The statute governing the disposal by businesses of records containing the personal information of customers does apply to title companies. This is particularly significant as it applies to information which would be contained in an escrow or sub-escrow file.

Section 1798.80 of the Civil Code requires a business to ensure the privacy of a customer's personal information contained in records by destroying, or arranging for the destruction of the records by shredding, erasing, or otherwise modifying the customer record to make information therein unreadable or undecipherable through any means.

Any customer injured by a business' violation of these provisions is entitled to institute a civil action to recover damages, obtain injunctive relief, or seek other remedies.

V. Disclosure to Consumers of Information Provided to Direct Marketers

Civil Code Section 1798.83

The statutes governing disclosures to consumers of information provided to third parties for direct marketing purposes has an exemption for financial institutions subject to the California Financial Information Privacy Act. Since this act uses the federal Gramm-Leach-Bliley (GLB) definition of financial institutions, title companies would be exempt. Nevertheless, the statute is worthy of attention due to direct marketing performed by various customer groups.

Disclosure Requirement

A business that provides a customer's personal information derived from an established business relationship to a third party for direct marketing purposes is required to disclose the names and addresses of the third parties recipients of this information to customers who request this information in writing within 30 days of the request. (The terms "customer," "personal information," "established business relationship," "third party," and "direct marketing purposes" are defined in Civil Code Section 1798.83.

Exemptions

While the law generally applies to all businesses in California that generate "customer" information, Civil Code Section 1798.83 (h) *exempts* businesses from having to provide the names and addresses of third party recipients for direct marketing to customers who request this information if *one* of the following elements is met:

- (1) The business generating information for a third party recipient for direct marketing purposes is a "financial institution" as defined in the California Financial Information Privacy Act (CFIPA) enacted on August 28, 2003 and is already subject to the new privacy restrictions set forth in the CFIPA.

Note: Title companies fall within the definition of a "financial institution" as defined within both the CFIPA and GLBA and are required, to a limited extent, to comply with restrictions set forth in both acts. In other words, if a business (such as a title company) is considered to be a "financial institution" and is therefore required to comply with disclosure requirements set forth in the CFIPA, they are exempt from the requirements of this Act.

- (2) The information provided by the business to a third party recipient for direct marketing purposes is derived from the following:
 - (D) *Public record information relating to the right, title, or interest in real property or information relating to property characteristics, as defined in Section 408.3 of the Revenue and Taxation Code, obtained from a governmental agency or entity or from a multiple listing service, as defined in Section 1087, and not provided directly by the customer to a business in the course of an established business relationship (Civil Code Section 1798.83 (d)(1)(D)).*

Note: This exclusion, requested by CLTA, is meant to exempt all information compiled by a title company from the public record information held by the county assessor or county recorder.

Thus, since both of these two exemptions are applicable to title companies, few, if any, restrictions within this Act apply to information generated or compiled by a title company in the ordinary course of business.

VI. Notification to Consumers of a Breach of the Security of Data Containing Personal Information

Civil Code Sections 1798.29 and 1798.82

National attention has focused on the California statute requiring notification to persons whose personal information has been compromised by a breach of security.

Generally, a state agency (Civil Code §1798.29), or a person or business (Civil Code §1798.82) that conducts business in California, that owns or licenses computerized data that includes “personal information,” is required to disclose any breach of the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person. However, to the extent a database contained information from public records and other personal information then the disclosure requirements would apply. **Of primary importance to title companies, “personal information” is defined in Civil Code Section 1798.29(f), to exclude publicly available information derived from federal and state or local government records.**

The notifications may be delayed if a law enforcement agency determines that it would impede a criminal investigation. An agency, person, or business that maintains computerized data that includes “personal information” owned by another must also notify the owner or licensee of the information of any breach of security of the data.

VII. Disclosures of Social Security Numbers

Civil Code Section 1798.85 and Family Code Section 2024.5

A person or entity, including a state or local agency, may not use an individual's social security number in certain ways, including publicly posting or displaying it so that it is available to the general public. However, these provisions do not prevent the collection, use, or retention of social security numbers as required by state or federal law, or the use of social security numbers for internal verification or administrative purposes.

Subdivision (d) of Section 1798.85 specifically exempted from these requirements certain public records, including recorded documents, and government tax records required to be open to the public.

In addition, Section 2024.5 of the Family Code to allow the petitioner or respondent to redact any social security number from any pleading, attachment, document, or other written material filed with the court pursuant to a petition for dissolution of marriage, nullity of marriage, or legal separation. The Judicial Council form used to file such a petition, or a response to such a petition, must contain a notice that the parties may redact any social security numbers from those pleadings, attachments, documents, or other material filed with the court.

However, an abstract of support judgment, or any similar form created for the purpose of collecting child or spousal support payments may not have the social security number removed.

VIII. Confidentiality of Addresses of Public Safety Officials

Government Code Sections 6254.21 and 6254.24 and Penal Code Section 146e

Government Code Section 6254.21, prohibits any state or local agency from posting the home address or telephone number of any elected or appointed official on the Internet without first obtaining the written permission of that individual.

Section 6254.24 of the Government Code also prohibits any person from knowingly posting the home address of any elected or appointed official, or the official's spouse or child residing at the same location, on the Internet knowing that person is an elected, appointed official, or public safety official, and intending to cause imminent great bodily harm that is likely to occur, or threatening to cause imminent great bodily harm, to that individual. A violation of these provisions a misdemeanor, or a felony if it leads to the bodily injury of the official or his or her residing spouse or child.

Every person who maliciously, and with the intent to obstruct justice or the due administration of the laws, publishes, disseminates, or otherwise discloses the residence address or telephone number of any designated public safety officials, or that of the spouse or children of these persons residing with them without the authorization of the employing agency, is guilty of a misdemeanor.

IX. Confidentiality of Addresses for Victims of Domestic Violence and Stalking

Government Code Section 6205 of Division 7 of Title 1

California Law establishes a program to create "Address Confidentiality for Victims of Domestic Violence and Stalking" which authorizes persons to complete an application containing information in person at a community-based victims' assistance program for the purpose of enabling state and local agencies to respond to requests for public records without disclosing a program participant's residence address. The law requires the Secretary of State to act as that person's agent for service of process and to designate a substitute mailing address for program participants. The law is effective until January 1, 2008.

The Secretary of State is required to notify certain persons if there are court orders or court actions under these provisions and provides that a program participant who obtains a name change may lose his or her certification as a program participant under certain circumstances. Program participation is valid for four years unless the certification is withdrawn or invalidated.

A program participant may request that state and local agencies use the address designated by the Secretary of State as his or her address. When creating a public record, state and local agencies shall accept the address designated by the Secretary of State as a program participant's substitute address. When modifying or maintaining a public record, excluding the record of any birth, fetal death, death, or marriage registered under Division 102 (commencing with Section 102100) of the Health and Safety Code, state and local agencies shall accept the address designated by the Secretary of State as a program participant's substitute address. However, a state or local agency can use the actual address if the Secretary of State has determined that:

The agency has a bona fide statutory or administrative requirement for the use of the address which would otherwise be confidential under this chapter and the address will be used only for those statutory and administrative purposes and shall not be publicly disseminated.

This law does not appear to impact the recording statutes which may contain legal documents affecting title to real property. However, abstracts of judgment or other matters requiring an address could contain the substitute mailing address.

X. California Insurance Information and Privacy Protection Act and Department of Insurance Regulations Adopted Pursuant Thereto

Background

The Insurance Information and Privacy Protection Act (IIPPA) was enacted in 1980 for the purpose of establishing standards for the collection, use, and disclosure of information gathered in connection with insurance transactions.

The California State Legislature, however, acknowledged that title companies are significantly different than other lines of insurance in the information they use to conduct business and granted the title insurance industry and exemption from the IIPPA (Insurance Code Sections 791-791.27.) The exemption is found in Insurance Code Section 791.01(d):

(d) This article shall not apply to a person or entity engaged in the business of title insurance as defined in Section 12340.3.

The “business of title insurance” includes, but is not limited to, title searches, generating title insurance policies, administration of escrows for consumers and lenders, etc. Thus, title insurers and underwritten title companies authorized to conduct “the business of title insurance” are completely exempt from the privacy provisions of the IIPPA.

The Insurance Commissioner made an effort to reconcile the IIPPA with the Gramm-Leach-Bliley Act in regulations which were filed with the California Office of Administrative Law and thereafter became effective on March 24, 2003 as 10 Cal. Code Regs. §2689.1 et. seq. (2004). The regulations focus on the privacy notice and information security process.

The Commissioner promulgated these regulations pursuant to the implied authority granted by California Insurance Code Sections 791 et seq. and 15 U.S.C. Sections 6801(b) and 6805(b) to implement California Insurance Code and Gramm-Leach-Bliley privacy provisions consistent with providing individuals the maximum privacy protections permitted by those laws.

During the comment period on the proposed regulation, the CLTA strongly urged the DOI to modify the proposed regulations to state that the GLBA restrictions and protections, not the proposed regulations, will be applicable to licensees not subject to the regulations because of the exemption in CIC Section 791.01.

Final Regulations

The final regulations recognized the title company exemption by providing in §2689.2 that:

Licenses not subject to California Insurance Code Sections 791 et. seq., but subject to GLBA, 15 U.S.C. Sections 6801-6810, shall comply with GLBA privacy provisions, and with Sections 2689.12 through 2689.20 of these regulations.

The regulations do require that title companies comply with Article 4 – Standards for Safeguarding Nonpublic Personal Information (Sections 2689.12-2689.20.) These sections establish standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of nonpublic personal information, pursuant to California Insurance Code Section 791 and sections 501, 505(b), and 507, codified at 15 U.S.C. 6801, 6805(b) and 6807, of GLBA.

Each licensee is required to implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical, and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

A licensee's information security program must be designed to:

- (a) Ensure the security and confidentiality of customer information;
- (b) Protect against any anticipated threats or hazards to the security or integrity of such information; and
- (c) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The following sections in the regulations set forth the requirements which are applicable to title companies:

Section 2689.16.

The licensee:

- (a) Identifies reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;
- (b) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and
- (c) Assesses the sufficiency of policies, procedures, customer information systems, and other safeguards in place to control risks.

Section 2689.17.

The licensee:

- (a) Designs its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the licensee's activities.
- (b) Trans staff, as appropriate, to implement the licensee's information security program; and
- (c) Regularly tests or otherwise regularly monitors the key controls, systems and procedures of the information security program. The frequency and nature of these tests are determined by the licensee's risk assessment.

Section 2689.18.

The licensee:

- (a) Exercises appropriate due diligence in selecting its service providers; and
- (b) Requires its service providers, by contract, to implement appropriate measures designed to meet the objectives of this article, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied such obligations.

Interaction with FTC Regulations on Safeguarding Privacy

The DOI regulations on safeguarding information are generally consistent with the FTC regulations effective on May 23, 2002. The FTC, on May 23, 2002, enacted new regulations pursuant to the authority granted in the GLBA to specifically require "financial institutions" to develop and maintain security measures and safeguards to protect databases, computer files, paper documents, etc., containing "**nonpublic personal information**" as defined within the GLBA. The new regulations are entitled "Standards for Safeguarding Customer Information" and were codified in FTC regulations 16 CFR Part 314, published on May 23, 2002 in the Federal Register.

The Internet link to these new regulations can be found at the following FTC website:
www.ftc.gov/os/2002/05/safeguardfrn.pdf

The FTC regulations seek to ensure the security and confidentiality of customer records and information; protect against any anticipated threats to those records; and protect against other potential harm to consumers resulting from an unauthorized release of that information.

All "customer information" is to be protected. "Customer information" is defined to be "nonpublic personal information" as defined in 16 CFR 313.3 (n). In other words, public records and publicly available information would be excluded (as it is in the GLBA) from this definition.

Title companies are subject to these new regulations except with respect to solely public information since it would not be "customer information" as defined within the new regulations.

However, to the extent title companies generate, compile, use, or share "nonpublic personal information" (perhaps gleaned from Statement of Identity Forms, escrow documents, etc.) they would be subject to these new regulations in regards to how they handle that information.

In essence, whatever information title companies may possess that is "customer information" under the GLBA would be subject to the FTC safeguard requirements as outlined in these new regulations.

To the extent title companies possess nonpublic personal information, the FTC regulations require the companies to establish what is called an "Information Security Program" as defined within Section 314.3 of the new regulations.

This program must contain administrative, technical, and physical safeguards that are “appropriate to the size, complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue” (Section 314.3 (a)). Nonpublic personal information contained within computer files, paper, or other form is required to be protected (Section 314.2 (b)).

In addition, one or more employees are required to coordinate the program (Section 314.4 (a)) and it would need to be designed to protect against foreseeable internal and external risks (Section 314.4(b)). The necessary training, software expenditures, etc., must be undertaken (Section 314.4).

The FTC regulations do apply to nonaffiliated third parties with whom a title company contracts. However, there is a two year grandfathering of nonaffiliated third party service contracts from that part of the regulation which requires companies to require service providers to implement and maintain safeguards. However, the DOI regulations did not have a delayed period for service provider compliance.

The California regulations provide in §2689.24 that:

Within 90 days of the effective date of these regulations, all contracts that a licensee enters into or has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee’s behalf shall include or be amended to include a written requirement that the third party maintain the confidentiality of **nonpublic personal information** where the nonaffiliated third party obtains confidential nonpublic personal information in connection with the contract.

Revision to California DOI Regulation

The California Department of Insurance (“Department”) requested public comments in March of 2004 on draft proposed regulation changes as a result of the August 28, 2003, enactment of the California Financial Information Privacy Act (California Financial Code Sections 4050-4060) operative July 1, 2004.

The proposed amendment to 10 Cal. Code Regs. §2689.2 would, among other things, require that licensees not subject to the IIPPA, but subject to the GLBA (this means title companies), must also comply with the California Financial Information Privacy Act.

The CLTA suggested modifying the reference the CFIPA to reference only those provisions to which a licensee may be subject since some of the CFIPA may have been preempted by recent changes to federal law. The CLTA pointed out, specifically, that the text of the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et. seq. was amended by the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) (Public Law 108-159). (Dec. 4, 2003).

The United States District Court for the Eastern District of California had held that the affiliate sharing provisions of the California Financial Information Privacy Act Are not preempted by the Fair Credit Reporting Act (Am. Bankers Ass’n v. Lockyer, (No. Civ.S 04-0778 MCE KJ, 2004 WL 1490432 (E.D. Cal. June 30, 2004.)

The Ninth Circuit Court of Appeals, on June 20, 2005, reversed the District Court and held:

“that the affiliate-sharing preemption clause preempts SB1 insofar as it attempts to regulate the communication between affiliates of “information,” as that term is used in § 1681a(d)(1). That is, SB1 is preempted to the extent that it applies to information shared between affiliates concerning consumers’ “credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living” that is used, expected to be used, or collected for the purpose of establishing eligibility for “credit or insurance,,” employment, or other authorized purpose.” *American Bankers Association v. Gould* (No. 04-16560, D.C. No. CV-04-00778-MCE).

In the meantime the Department of Insurance has not finalized changes to the regulations but has indicated that the Department is currently evaluating the court's decision to determine appropriate regulation changes in light of the decision and the comments received last year.



OFFICE OF
**Privacy
Protection**

9/1/04

XI.

Privacy Protection for Public Safety Officials

Getting control of personal information like your home address and telephone number can be as difficult as getting an angry cat into a bag.

With a lot of effort, you can have some success, but there will continue to be information escapes—like limbs poking out of the bag—that you can't prevent.

The general strategies recommended here are similar to those used to reduce the chances of becoming an identity theft victim: Give out the minimum amount of personal information necessary to get what you want. Take advantage of opportunities to remove your information from databases and marketing lists. And, avoid getting on many lists in the first place.

The result will be to reduce the presence of your name, home address and phone number in the information marketplace, thereby making them that much less available. This will occur over time, as list compilers and marketers update their databases, and it won't be absolute. As an added bonus, you will also see a reduction in the volume of junk mail and telemarketing calls you receive.

Contents

General Strategies	2
Public Records	2
Get Off the Lists.....	3
Stay Off the Lists	5
Additional Resources.....	6



Dataquick
877-970-9171

Acxiom
Consumer Advocate Hotline
877-774-2094, or Email to
optout@acxiom.com

Get Off the Lists: Opt-Out Opportunities

- **Remove your name and address from "reverse directories" and "street address directories."**

Call or write the major directory companies to request that your information be removed.

Haines & Company, Inc. Criss-Cross Directory Attention: Director of Data Processing 8050 Freedom Ave. NW North Canton, OH 44720	Equifax Attention: List Suppression File 26955 Northwestern Highway South Field, MI 48034 800-873-7655
--	--

Remove your name and address from online "reverse directories." Enter your residential phone number, including area code, in www.Google.com. If your number is listed, you'll get your name, address and a map to your home. Click on "Phonebook results" above your name to go to a page that shows you how to remove your listing. Following the instructions for removing your listing will also lead you links to other online reverse directories from which you can remove your information. (It can take some searching around on the directories' web pages to find out how to remove your information.) Also, do a Google search on "reverse directories" to get links to more of them from which you can remove your listing.

- **Use Operation Opt-Out to get your name and address out of many databases and mailing lists.**

The non-profit Center for Democracy and Technology's Operation Opt-Out web site, at <http://opt-out.cdt.org>, makes it easy to opt-out of having your personal information shared and sold by many companies. The web site's "Generate Opt-Out Forms" section lets you print out letters addressed to many companies that do not offer a way to opt-out online. The "Opt-Out Online" section has links to many companies that allow you to opt-out online. The "Featured" section highlights web portals and online profilers. New categories are added periodically and you can sign up to receive e-mails from CDT on the latest steps to take to protect your privacy.



- **Sign up for the national Do-Not-Call Registry.**
If you haven't done so already, register your home telephone number(s) by calling 888-382-1222 or register online at <https://www.donotcall.gov/default.aspx>.

- **Remove your information from the lists of data compilers and mailing list companies.**

There are many companies that gather information from public records, telephone directories, consumer surveys and other sources. They compile the information and sell or rent it to other companies for marketing purposes. To be removed from the lists of the major data compilers, call or write as indicated below.

Donnelley Marketing Data Base Operations 4166 S. Bell Ames, IA 50010 888-633-4402	Experian Consumer Services 901 West Bond Lincoln, NE 68521 800-407-1088	Trans Union List Division P. O. Box 97328 Jackson, MS 39288-7293 888-567-8688
---	---	---

Also Acxiom and Equifax List Suppression File, listed above.

- **Tell your financial institutions not to share your personal information**
Read the privacy notices sent to you by your bank, credit card issuers, insurance and investment companies. Look for opportunities to opt-out of having your personal information shared with other companies. You don't have to wait for the annual notice to take advantage of your opt-out rights. For more information, see "Your Financial Privacy," available from the Office of Privacy Protection at www.privacy.ca.gov.
- **Opt out of lists to receive unsolicited pre-approved credit offers.**
Call 888-5OPTOUT, a number maintained by the national credit reporting agencies, to remove your name and address from circulation to financial companies that send most of the pre-approved credit offers that fill mailboxes. This is good for two years. Listen through to the end of the automated message and you will learn how to opt out permanently, by mailing in a request.
- **Have your name, address, and phone number removed from many other marketing lists.**
Sign up for the Direct Marketing Association's Mail Preference Service. This is a voluntary industry program. The service costs \$5 online at www.dmaconsumers.org/cgi/offmailinglist. It is free by writing to the address below.

DMA Mail Preference
Service P. O. Box 643
Carmel, NY 10512



- **Opt out of mail order catalogue database.**

Catalogue sales transactions are often reported to Abacus, which compiles a database of catalogue and publishers' customers. Abacus sells this data to other mail order companies. To opt-out of the Abacus database, provide your full name and current address.

Abacus
P.O. Box 1478
Broomfield, CO 80038
800-518-4453

Stay Off the Lists

- " **Don't fill out consumer surveys or marketing surveys.**

Consumer surveys are commonly used to compile mailing lists for marketing purposes. Don't fill out surveys attached to product "warranty registration cards." You do not have to complete and return the cards to enjoy your warranty rights. Write or call the companies below and ask to be removed from their mailing lists.

Equifax Direct Marketing Solutions
Consumer Response Center
26955 Northwestern Hwy, Suite
200 Southfield, MI 48034-8455
(800)873-7655

Experian Consumer Services at address given above.

- **Don't fill out sweepstakes entry forms.**

Sweepstakes and contests are often a means of gathering names and addresses for marketing purposes. To have your name removed from the major national sweepstakes mailers, contact the following:

American Family
Publishers
P. O. Box 652000
Tampa, FL 33662

Christopher Irving
Director, Consumer
Affairs
Publisher's Clearing House
382 Channel Drive
Port Washington, NY
11050
800-337-4724

Rosalyn McDavid
Time, Inc.
1271 Avenue of the
Americas
New York, NY 10020



Reader's Digest
Customer Service
Reader's Digest
Association, Inc.
1995 G Avenue
Red Oak, IA 51566
800-635-5006

Stephen Hamrock
Director of Customer Service
Suarez Corporation
7800 Whipple Ave. NW
North Canton, OH 44720
330-494-4282

- **When you give money to a charity or other group, ask them not to share your name and address.**

Enclose a note with your donation, asking them not to share, sell or rent your name to any other organization. Do the same when you order from a catalog.

Additional Resources for Protecting Personal Information

Association of Threat Assessment Professionals, www.atapusa.org/

California Office of Privacy Protection, www.privacy.ca.gov

CIS 1: Identity Theft Prevention Tips

CIS 2: Your Financial Privacy

CIS 5: Leave Me Alone: How to Slow the Flow of Unwanted Communications

Privacy Rights Clearinghouse, www.privacvrightrights.ca.gov

Fact Sheet I(a): Privacy Basics

Fact Sheet 4: "Junk" Mail: How Did They All Get My Address? Fact Sheet 11:

From Cradle to Grave: Government Records and Your Privacy Fact Sheet 14:

Are You Being Stalked? Tips for Protection

Sontag, Larry, // *'s None of Your Business: A Complete Guide to Protecting Your Privacy, Identity and Assets* (PMI, 2001).

This fact sheet is for informational purposes and should not be construed as legal advice or as policy of the State of California. If you want advice on a particular case, you should consult an attorney or other expert. The fact sheet may be copied, if (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the Office of Privacy Protection in the California Department of Consumer Affairs, and (3) all copies are distributed free of charge.

Section Two - Federal

Federal Privacy Laws Applicability to Title Companies

I. Title Company Privacy Rules Under the Graham-Leach-Bliley Act

NOTE: This document is only meant to highlight a number of questions and issues surrounding the recently enacted Graham-Leach-Bliley Act and the subsequently enacted Federal Trade Commission regulations that go into effect on July 1, 2001. ***This is not meant to be a substitute for the legal advice of your own counsel. The CLTA strongly suggests that your company undertake a privacy audit and recommends that you get a copy of the ALTA "Privacy Matters" tape and written seminar materials, which go into more detail on these issues.***

A. GENERAL QUESTIONS & ANSWERS

Q: What is the Graham-Leach-Bliley Act?

A: The Graham-Leach-Bliley Act (GLBA) was a federal act signed into law in 2000. The GLBA allows financial institutions to sell insurance products, in addition to their traditional lending services and products, to their consumers.

In addition, the GLBA also requires all financial institutions to adopt policies and procedures to better protect the "nonpublic personal information" of their consumers.

Q: Where do I look to find all of the privacy restrictions and requirements set forth in the GLBA?

A: Subsequent to the enactment of the GLBA, the Federal Trade Commission (FTC) developed extensive regulations setting forth the new requirements affecting financial institutions. A copy of the FTC regulations (16 CFR Part 313) may be accessed on the CLTA website at www.clta.org or by going to www.ftc.gov/os/2000/05/65fr33645.pdf.

Q: Does GLBA deal only with financial institutions? If so, what does that have to do with title companies?

A: Yes, the GLBA deals only with financial institutions. However, the term "financial institution" is defined broadly within the GLBA and the FTC regulations to include "insurance" companies and providers of "real estate settlement services." Therefore, title companies –underwriters and UTCs alike-- are subject to most of the privacy provisions of the GLBA.

Q: What constitutes "Nonpublic Personal Information"?

A: Nonpublic personal information is defined within the GBLA as "any personally identifiable financial information" and any list, compilation, or grouping of consumers (and all publicly available information relating to them) that is generated using any personally identifiable financial information **not** publicly

available. While the GLBA refers to personally identifiable *financial* information, it essentially means any personally identifiable information, financial or otherwise.

It is important to note that “nonpublic personal information” does *not* include “publicly available information,” or any list generated without using any personally identifiable information not found in public records. In addition, any aggregated list or compilation or other information that does not identify a specific consumer (e.g. does not include addresses or policy information) would not be considered nonpublic personal information.

Q: What about starters used to generate new title policies? Would those be considered “nonpublic personal information” or merely public records?

A: It is unclear if starters are or are not “nonpublic personal information.” CLTA strongly advises title companies closely analyze what information is contained in the starters, how they are compiled, the methods of storing them, and how they are shared between companies.

The FTC regulations clearly exempt from the definition of “nonpublic personal information” lists, groupings, and other compilations of information from county records, government records, phone books, etc. that is “not derived, *in whole or in part*, using personally identifiable financial information that is not publicly available.” Thus, if the information is gleaned *solely* from public records, it would not be subject to the GLBA restrictions.

However, “Personally identifiable information” (i.e. protected information) is defined to include information that makes clear “the fact that an individual is or has been one of your customers or has obtained a financial product or service from you” or “any information about your customer if it is disclosed in a manner that indicates that the individual is or has been your customer.”

Thus, the title information in the policy would arguably be non-protected public information. However, other information in the policy (e.g. title company name) might be considered “personally identifiable information.”

Q: Would a “farm package,” supplied to a real estate agent or broker (or other entity) for marketing purposes, constitute “nonpublic personal information” under the GLBA?

A: That depends. The FTC regulations clearly exempt from the definition of “nonpublic personal information” lists, groupings, and other compilations of information from county records, government records, phone books, etc. that is “not derived, *in whole or in part*, using personally identifiable financial information that is not publicly available.” Thus, if the information is gleaned *solely* from public records, it would not be subject to many of the GLBA restrictions.

However, “Personally identifiable information” (i.e. protected information) is defined to include information that makes clear “the fact that an individual is or

has been one of your customers or has obtained a financial product or service from you” or “any information about your customer if it is disclosed in a manner that indicates that the individual is or has been your customer.”

Thus, title companies will need to conduct an internal audit to determine exactly how the information in farm packages is compiled, stored, and shared with other entities such as real estate agents and brokers.

In addition, it would be wise to look to the later discussions in this document dealing with requirements for Disclosure Notices to consumers and Opt-Out Requirements under the GLBA.

Q: Is there a “test” I can use to determine if something is “publicly available information” as opposed to “nonpublic personal information”?

A: The FTC regulations define “publicly available information” to mean any data that a title company has a “reasonable belief” is lawfully available to the general public form:

- (1) Federal, state, or local government records (e.g. county recorder records);
- (2) Widely distributed data (e.g. telephone books, newspapers, websites, etc.);
and
- (3) Disclosures to the public that are required to be made by federal, state, or local laws.

In order to test the “reasonableness” of your belief, it is wise to ascertain if the information is of the kind that is available to the general public, and that the consumer has not taken steps to make sure that the information is being kept private.

It would also be wise to conduct an internal audit within your title company to determine exactly how and when the list or information in question was compiled and whether or not it was gleaned *solely* from public records or other sources cited above.

Q: For purposes of the GLBA, is a “consumer” only a person who actually purchases a title insurance policy, other product or service?

A: No. According to examples under the definition section of the FTC regulations, a “consumer” is a person who actually purchases, *or merely applies for*, a “financial product” such as a title policy, product, or service.

Q: When must title companies be in compliance with the FTC regulations concerning privacy?

A: Title insurance companies must be in compliance with the FTC regulations (16 CFR part 313) that *go into effect on July 1, 2001*.

Q: If California adopts its own regulations dealing with the issue of privacy and consumer records will title companies still be required to comply with GLBA and the FTC regulations?

A: Since federal law preempts state law, title companies must comply with the GLBA. However, the GLBA states, in essence, that it does not preempt any state law that provides consumers greater privacy protections. If California enacts a law then title companies may be in the unenviable position of having to be in compliance with both.

Q: In Southern California my title company often operates as a sub-escrow for an independent escrow company, and we have little or no contact with the consumer. Do the GLBA and FTC regulations still apply to me?

A: Probably, yes. Since both title insurers and UTCs provide “real estate settlement services,” their lack of direct contact with a consumer may not be all that relevant for purposes of determining whether or not the GLBA applies.

While the title company may be a sub-agent for an independent escrow company, it is still involved in conducting a title search and issuing a title policy (and any other product or service they sell that falls under the umbrella of “settlement service”) for the consumer purchasing the real property. This fact alone may bring the UTC and underwriter under the requirements of the GLBA, even when providing sub-escrow services.

Q: Generally speaking, what are the most important new privacy requirements under the GLBA for title companies?

A: Under the GLBA, as of July 1, 2001, title companies are subject to three new consumer privacy requirements:

- (1) Create and provide a Privacy Notice Disclosure (in layperson’s language) for all title company consumers;
- (2) Create a procedure that allows title company consumers the ability to “Opt-Out” of title companies sharing their Nonpublic Personal Information with others;
- (3) Create internal procedures and mechanisms to ensure the “Security and Integrity” of all title company consumers’ Nonpublic Personal Information.

B. THE PRIVACY NOTICE DISCLOSURE

Q: When must a Privacy Notice Disclosure be given to a title company consumer?

A: Generally speaking, a GLBA Privacy Notice Disclosure must be given to any consumer who purchases a residential title insurance product and service *at the time the product or service is sold or delivered*.

Under the GLBA, this disclosure must be provided when a “customer relationship” is established. The disclosure notice may be provided when a purchased policy is delivered or when an agreement to provide other insurance services is consummated.

The notice can be provided along with other materials you deliver to your residential customers, including the insurance contract or other materials you are providing.

Q: Must a Privacy Notice Disclosure be given to both residential and commercial title company consumers?

A: No. The GLBA requires providing the Privacy Notice Disclosure to residential consumers only.

Q: Does the GLBA or FTC regulations provide any examples of Privacy Notice Disclosures I can look at?

A: Yes. Please look at the examples in the FTC regulations.

A copy of the FTC regulations (16 CFR Part 313) may be accessed on the CLTA website at www.clta.org or by going to www.ftc.gov/os/2000/05/65fr33645.pdf.

Q: Under the GLBA, most insurers are required to provide the Privacy Notice Disclosure to their consumers *annually*. Does this apply to title companies?

A: No. Due to the successful efforts of the American Land Title Association (ALTA), GLBA was amended to recognize the special “one-time” interaction and relationship between a title company and the residential consumer. Title companies are only required to provide the Privacy Notice Disclosure to the consumer ***once***.

Q: Must my title company provide the notice to former customers?

A: No. The GLBA does *not* require a title company to provide the annual notice to consumers, or former customers, unless there is an ongoing relationship. However, other insurance companies who charge a monthly, quarterly, or annual premium will be required to provide the notice to their pre-existing customers. However, after July 1, 2001, new customers will be required to receive the new disclosure notice.

Q: Are UTCs subject to the same requirements regarding providing the Privacy Notice Disclosure to consumers as title insurance underwriters?

A: Generally speaking, yes. The GLBA privacy obligations are imposed on all “financial institutions” and the term encompasses all providers of “financial services,” including any entity that is engaged in insurance company, agency, and brokerage or credit activities.

A UTC is probably *not* subject to the GLBA privacy notice disclosure if:

- (1) The UTC is an agent or representative of the title insurer; and
- (2) The *underwriter* complies with and already provides the required notices; and
- (3) The UTC itself does not –independent of the underwriter(s)-- disclose any nonpublic personal information to any person other than the underwriter or its affiliates.

Q: Must a UTC use the same Privacy Notice Disclosure generated by its underwriter?

A: Title insurers and UTCs are *both* required to provide the Privacy Notice Disclosure to the consumer. However, the UTC may do so independently or utilize a *single* notice in conjunction with the underwriter. Thus, a UTC must review the Privacy Notice Disclosure of its underwriter(s), consider its own business model and affiliations, and decide best how to proceed with providing the notice to the consumer.

In some cases, redundancies may be unavoidable, but at least one notice must be provided and the UTC must handle the nonpublic personal information in the manner set forth in the notice(s).

Q: What is specifically required in the GLBA regarding the contents of “Privacy Notice Disclosure” for title company consumers?

A: The GLBA does not set forth any specific information-handling practice or procedures for title companies. However, it does require that all individual consumers be given a Privacy Notice Disclosure that details: (1) what categories of nonpublic personal information (if any) are collected and (2) to whom it may be released.

The following eight categories must be addressed in the notice:

- (1) The nonpublic personal information that your company collects (including the type of data and the method of collection);
- (2) The nonpublic personal information that may be released;
- (3) The affiliated and nonaffiliated third parties that may receive the nonpublic personal information (other than those to whom releases may be made under an exception –see discussion below regarding releases to affiliates and non-affiliates under the “Opt-Out” requirements);

- (4) Your company's policies and practices regarding the sharing or nonpublic personal information about former customers. (If your company treats customers and former customers the same, you may use the same clauses for both);
- (5) The nonpublic personal information released pursuant to contractual agreements with third party service providers and joint marketers, and the types of third parties providing the services (e.g. envelope stuffers);
- (6) The individual's right to "opt-out" of the release of nonpublic personal information to nonaffiliated third parties;
- (7) Any releases of regarding affiliate information sharing you are providing under FCRA;
- (8) You company's policies and practices regarding protecting the confidentiality, integrity, and quality of the nonpublic personal information you collect.

Q: Given the fact that the Privacy Notice Disclosure is to be given to residential consumers only, are there any special requirements regarding the language I can use?

A: Yes. These disclosures must be "clear and conspicuous" and "reasonably understandable" and "designed to call attention" to what is being disclosed. In other words, the disclosure must be in layman's language and easy to understand.

Q: If my title company does not disclose any nonpublic personal information whatsoever, am I still required to provide the Privacy Notice Disclosure to my customers?

A: Yes. However, since there is little to disclose, it may be possible to make these disclosures in a brief, summarized form.

Q: How accurate does my Privacy Notice Disclosure form have to be?

A: Given that your Privacy Notice Disclosure is a legal requirement, it is imperative that your company develops an accurate form that sets forth your information-handling practices and that your company adheres to those practices.

C. THE "OPT-OUT" REQUIREMENT

Q: When must the "Opt-Out Notice" be provided under the GLBA?

A: The GLBA notice must be provided only if nonpublic personal information is shared with a "non-affiliated third party" for a "non-exempted purpose." (See the discussion below regarding what constitutes a "non-affiliated third party" and "non-exempted purposes.")

Q: What is meant by the “Opt-Out” requirement in the GLBA?

A: Under the GLBA, a consumer has a right to exercise his or her right to prohibit a title company from releasing nonpublic personal information to another party. If the consumer exercises his or her right to prohibit this release of nonpublic personal information, it is commonly referred to as “opting-out.”

Q: Does the GLBA or FTC regulations have any examples of “Opt-Out” notices I can look at?

A: Yes. There are examples included in the FTC regulations.

A copy of the FTC regulations (16 CFR Part 313) may be accessed on the CLTA website at www.clta.org or by going to www.ftc.gov/os/2000/05/65fr33645.pdf.

Q: How long does a consumer have to “Opt-Out” of my title company releasing nonpublic personal information?

A: The consumer has 30 days to direct you not to release his or her nonpublic personal information. Thus, before you release nonpublic personal information, it would be wise to wait the 30 days before releasing any nonpublic personal information to a nonaffiliated third party. This may require developing a method of tracking this 30-day period.

Q: What information must be disclosed to the residential consumer in the Opt-Out Notice?

A: A title company must inform the consumer that they have the right to prohibit the title company from sharing nonpublic personal information with *unaffiliated third parties* for non-exempted purposes.

In addition, a title company must either provide a copy of its overall Privacy Notice Disclosure in conjunction with providing the opt-out notice, or the title company must notify the residential consumer that he or she has a right to review the overall privacy policy and instructions on how to get a copy of it.

A copy of an example of a notice that satisfies the GLBA is found in the FTC regulations. A copy of the FTC regulations (16 CFR Part 313) may be accessed on the CLTA website at www.clta.org or by going to www.ftc.gov/os/2000/05/65fr33645.pdf.

Q: Who must comply with providing this “Opt-Out” Notice to residential consumers?

A: Unlike the Privacy Notice Disclosure which must be made irrespective of whether or not any information sharing occurs, the “opt-out” notification is required *only if*

a title company will be releasing nonpublic personal information to a non-affiliated third party for a non-exempted purpose.

Q: What constitutes an “affiliated third party” in the context of the Opt-Out Notice requirements?

A: Under the GLBA, an “affiliate” is specifically defined as any company that is “related or affiliated by common ownership, or affiliated by corporate control or common corporate control, with another company.”

This means controlling, controlled by, or under common control with, another company. “Control means the power to vote 25 percent or more of any class of voting securities; control over the election of a majority of the directors, trustees, or general partners; or the power to exercise a controlling influence over the management or policies of a company.

The regulations define “common ownership” to mean overlapping ownership of twenty-five (25) percent or more. Thus, all subsidiaries of a parent company are considered affiliates of one another and of the parent.

In addition, some joint venture companies may constitute “affiliates” if your title company owns 25 percent or more of the joint venture or otherwise controls the affairs of the joint venture in any way.

Q: What are the “Exempted Purposes” alluded to earlier in the context of the Opt-Out Notice requirements?

A: If nonpublic personal information is released to a “non-affiliated third party” for the following purposes:

- (1) Processing and servicing transactions;
- (2) Service providers and joint marketing; and
- (3) Other limited exemptions.

Q: What is meant by “Processing and servicing transactions” within the context of an “Exempted Purpose” in the context of the Opt-Out Notice requirements?

A: The customer’s opt-out right is limited in that it does not allow the customer to prohibit a title company from releasing nonpublic personal information for *the purpose of processing or completing the transaction* (or a related transaction) for which the nonpublic personal information was collected in the first place.

In other words, the “opt-out” requirements do not apply if a title company releases nonpublic personal information “necessary to effect, administer or enforce a transaction” the customer authorizes, or that takes place in connection with certain processing and servicing functions a title company would ordinarily undertake.

“Necessary to effect, administer or enforce a transaction” is defined to include, among other things, releases of information in order to administer or service benefits or claims relating to the transaction or the product or service of which it is an essential part, and necessary to underwrite insurance. These things would include the following:

- (1) Account administration;
- (2) Reporting, investigating or preventing fraud or material misrepresentation;
- (3) Processing premium payments;
- (4) Processing insurance claims;
- (5) Administering insurance benefits; and
- (6) Participating in research projects or as other required or specifically permitted by federal or state law.

Q: What is meant by “Service providers and joint marketing” within the context of an “Exempted Purpose” in the context of the Opt-Out Notice requirements?

A: Title companies are not required to permit consumers to opt-out of the release of nonpublic personal information to a third-party under a “joint marketing agreement.” A title company would be wise to closely look at the joint marketing exception under the GLBA.

In addition, title companies are permitted to release a customer’s nonpublic personal information to unaffiliated third parties to market the title company’s own products and services without allowing the customer to opt-out. A good example of this would be if a title company compiles a list of customers (names and addresses) and provides that list to a company who stuffs envelopes and distributes the marketing materials on behalf of the title company. No opt-out opportunity for the consumer is required in this example.

Q: What are the “Other Limited Exceptions” within the context of an “Exempted Purpose” in the context of the Opt-Out Notice requirements?

A: There are several other limited exceptions to the Opt-Out requirements in under the GLBA. Specifically, the opt-out requirements do not apply when you release nonpublic personal information in the following situations:

- (1) The consumer specifically consents or directs the title company to do so;
- (2) To protect the confidentiality or securing of your records pertaining to the consumer, service, product or transactions, or to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability;
- (3) For required risk control or for resolving consumer disputes or inquiries;
- (4) To persons having a legal or beneficial interest relating to the consumer, or to persons acting in a fiduciary capacity on behalf of the consumer;

- (5) To provide information to a rate advisory organization, guarantee fund, rating agencies, persons assessing your compliance with industry standards, attorneys, accountants and auditors;
- (6) To a consumer reporting agency in accordance with FCRA, or from a consumer report reported by a consumer reporting agency;
- (7) In connection with a proposed or actual sale, merger, or transfer of a business or operating unit; or
- (8) To the extent specifically permitted or required under other provisions of law, or to comply with Federal, State or local laws, rules or other requirements.

Q: If my title company releases nonpublic personal information with a non-affiliated third party under one of the allowable GLBA exemptions, is the non-affiliated third party limited in how it can use the information? Must I verify how it is using the information?

A: Yes, the non-affiliate is limited in how it can use the information. The non-affiliated third party is required to limit its use of the nonpublic personal information to the stated purposes of the release.

However, you are *not* required to verify their compliance with the law.

D. Creating Internal Procedures and Mechanisms to ensure the “Security and Integrity” of all Title Company Consumers’ Nonpublic Personal Information

Q: Under the GLBA, is a title company required to create a comprehensive set of Internal Procedures and Mechanisms to ensure the “Security and Integrity” of all consumers’ Nonpublic Personal Information?

A: Yes. In order to do this, each title company should conduct an internal audit of the following:

- (1) What types of information do you collect pertaining to consumers?
- (2) Does any of this information fall into the category of “nonpublic personal information?”
- (3) If your title company collects “nonpublic personal information” how is it used by your company?
- (4) If your title company collects “nonpublic personal information” to whom is it released and for what purpose? Is it shared with affiliates and nonaffiliates?
- (5) If your title company collects “nonpublic personal information” how does the title company maintain it? What internal procedures and mechanisms are in place to ensure the security and integrity of that information?

It is important to note that these questions are only cursory in nature and in no way reflect the comprehensive internal audit a title company should conduct. For a list of comprehensive “Internal Audit Questions” we strongly suggest you contact the ALTA and get their “Privacy Matters” tape and written materials.

II. Privacy Laws and Underwritten Title Companies

A. What entities are subject to the Gramm-Leach-Bliley Act (GLBA)?

Generally speaking, all “financial institutions” compiling, utilizing, sharing, or storing “nonpublic personal information” are subject to the consumer constraints and safeguards as set forth in the GLBA.

B. Are UTCs considered “financial institutions” for purposes of the GLBA?

1) “Financial Institutions” as defined in 6809 (3) of the GLBA include UTC as agent of title insurer:

(3) Any institution the business of which is engaging in financial activities as described in Section 1843 (k) of title 12.

“Financial activities” relevant to the title industry are found defined within Section 1843 (k) (4) (B):

(B) Insuring, guaranteeing, or indemnifying against loss, harm, damage... and acting as principal, agent, or broker for purposes of the foregoing in any state.

Thus, to the extent UTCs are operating as an agent or broker for the underwriter in the issuance of a title insurance policy, they arguably fall within this definition of “financial activities” of a “financial institution.” (Escrow services would not fall within this definition, but do fall within the definition of “real estate settlement services” discussed below.)

2) Federal Trade Commission Regulations (16 CFR, Chapter 1, Part 313) define “financial institutions” providing “real estate settlement services” so as to include UTCs:

Specifically, the FTC regulations (adopted pursuant to authority granted in GLBA), in Section 313.3 (k)(2)(x), provides examples of what constitutes a “financial institution” for purposes of the regulations to include those entities providing “real estate settlement services”:

(x) An entity that provides real estate settlement services is a financial institution because providing real estate settlement services is a financial activity listed in CFR 225.28 (b)(2)(viii) and referenced in Section 4(k)(F) of the Bank Holding Company Act. [Emphasis added]

It is important to note that CFR 225.28 (b)(2)(viii) *specifically excludes* “providing title insurance as principal, agent, or broker” from its definition of “real estate settlement services” and no mention is made in these regulations of other escrow related services (See footnote (4) of CFR 225.28 (b)(2)(viii)).

However, Section 4(k)(F) of the Bank Holding Company Act (BHCA) does bring escrow services rendered by a UTC back into the definition of “real estate settlement services” (and thus within the definition of “financial activities” of a

“financial institution”) via its reference to Federal Reserve Bulletin Orders. Section 4 (k)(F) of the BHCA reads:

*(F) Engaging in any activity that the Board has determined, by **order** or regulation that is in effect on the date of the enactment of the Gramm-Leach-Bliley Act, to be so closely related to banking or managing or controlling banks as to be a proper incident thereto (subject to the same terms and conditions contained in such order or regulation, unless modified by the Board.) [Emphasis added]*

In three separate Bulletin Orders (81 FRB 805 (August 1993), 79 FRB 517 (May 1993), 76 FRB 1058 (Dec, 1990)), the Federal Reserve Board determined that “real estate settlement services” included just about all escrow activities conducted by a UTC.

Thus, through the BHCA Section 4 (k)(F) and the aforementioned Federal Reserve Board Bulletin Orders, the escrow related functions provided by UTCs fall within the definition of “real estate settlement services.” (See attached summary of activities defined to be “real estate settlement services” by the Federal Reserve Board in their Bulletin Orders.)

C. Do UTCs handle “nonpublic personal information” as set forth in the GLBA and related regulations?

1) Define the types of information gathered and used:

It is essential to ascertain the type or types of information a UTC handles in its course of business to determine what provisions of the GLBA affect them.

To properly conduct this analysis, it is important to determine several things:

- (a) What information that UTCs collect is from a public source such as county records?
- (b) What types of information are collected from the consumer directly from sources other than public information (such as a Statement of Identity form)? And
- (c) To what extent, if any, are the public and personal information commingled to provide a given product, service, or generate a database?

These questions are important because all of the restrictions and requirements within GLBA flow from *the goal of protecting nonpublic personal information, NOT public information.*

D. Public records v. “nonpublic personal information”

The GLBA (Section 6809 (4)(B)) defines “nonpublic personal information” to exclude public documents:

*(B) Such a term does not include **publicly available information**; as such term is defined by the regulations prescribed under Section 6804 of this title. [Emphasis added]*

In addition, *lists* derived solely from public records (arguably, such things as farm packages) are specifically excluded from the definition of “nonpublic personal information” in GLBA Section 6809 (4)(C)(ii).

Thus, the definition of “nonpublic personal information” does **not** include publicly available information (e.g. public records, telephone books, well-distributed lists, etc.) or “any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information.”

However, it is important to acknowledge that the GLBA also undercuts this public document exemption for *groupings* of consumers if there is a commingling of information both from a public source and from **any** nonpublic personal information derived directly from the customer. GLBA Section 6809 (4)(C)(i) states that the definition of “nonpublic personal information” **does** include the following:

*...any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using **any** nonpublic personal information other than publicly available information... [Emphasis added]*

While the GLBA discusses the commingling or “tainting” of groupings of information that contain both public and nonpublic personal information, it intimates that any commingling of these two sources may cause a UTC problems in relying solely upon the “public record” exemption.

E. What other exclusions exist within the GLBA relevant to UTCs?

- 1) Information handled by UTCs “necessary to effectuate transaction” exempt from Opt-Out Notice provisions of the GLBA:

The phrase “necessary to effect, administer, or enforce the transaction” is defined within the GLBA Section 6809 (7) (A) to mean:

(A) The disclosure is required, or is a usual, appropriate, or acceptable method, to carry out the transaction or the product or service business of which the transaction is a part, and record or service or maintain the consumer’s account in the ordinary course of providing the financial service or financial product, or to

administer or service benefits or claims relating to the transaction or the product or service business of which it is a part...

The “necessary to effect, administer, or enforce the transaction” is also defined within the Opt-Out Notice provisions of the GLBA to specifically include exchange of customer information for the purposes of insurance underwriting (Section 6809 (7) (C)), and for billing and handling accounts (Section 6809 (7)(D)).

Certainly, any information sharing, databases, etc., used by UTCs to conduct real estate settlement services falls into the definition of “necessary to effect, administer, or enforce the transaction” and they are exempt from the Opt-Out Notice Provisions. This is in addition to the above arguments regarding the fact that they are using only public records that do not fall within the definition of “nonpublic personal information” within the GLBA.

- 2) UTCs are exempt from the requirement to provide an Annual Notice of Privacy Policy

Under the GLBA, all “financial institutions” handling “nonpublic personal information” are required to provide a notice, at least annually, to the consumer explaining how they compile, store, use, and share “nonpublic personal information” with other companies and affiliates. (Section 6803)

Within the FTC Regulations (16 CFR, Chapter 1, Part 313) UTCs and title insurers are defined as having a “continuing” “customer relationship” with their customers pursuant to Section 313.3 (i)(2), subparagraphs (C) & (K).

However, for purposes of the Annual Privacy Notice required by the GLBA, UTCs are exempt from continually providing the annual notice pursuant to Section 313.5 (b)(1) because the customer relationship is found to have been “terminated” in 313.5 (b)(2)(vi) once the settlement service provider has executed all of its functions and recorded the necessary documents.

Presumably, the GLBA assumes some sort of notice –though not annually—will be provided to the consumer, probably some time during the escrow process by the UTC. Arguably, this notice would only address those pieces of information that were not derived from the public records but from other sources, such as the Statement of Interest Forms and other escrow documents not recorded within a public record database, such as the county recorder.

- F. In summary, are UTCs subject to the Opt-Out Notice and Annual Privacy Notice requirements as set forth in the GLBA?

Not to the extent the exceptions provided in the GLBA apply.

UTCs, as “financial institutions,” are certainly subject to the GLBA as discussed above. As discussed above, UTCs are probably considered “financial institutions” because of their direct association with the title insurer (who are also “financial institutions”) and also because they conduct a number of activities that fall within the definition of “real estate settlement service provider.” That point seems indisputable.

However, if UTCs handle only “nonpublic personal information” (i.e. public records) in conducting a title search and generating a title policy, they are –in theory-- exempt from almost all provisions of the GLBA, including the Opt-Out Notice and Annual Privacy Notice requirements as set forth in Sections 6802 and 6803, respectively. In other words, the exemption flows from the source of the information: if you use public records exclusively you’re essentially exempt from most of the GLBA. *The GLBA seeks to protect nonpublic personal information, NOT information contained within public records.*

However, the FTC Regulations seem to assume that UTCs, as settlement service providers, do in fact handle some information that is personal in nature and does not fall within the public records exclusions (i.e. information publicly available) within the GLBA. Obviously, some information contained within the Statement of Identity Forms and other escrow documents such as payoff amounts (which are not recorded) would probably fall within the definition of “nonpublic personal information.”

Therefore, the commingling public information (such as county records) with personal information provided by the consumer from such things as a Statement of Identity may “taint” the overall nature of the information. This is clearly stated in Section 6809 (4)(C)(i) when lists are generated and the aggregate information is not derived solely from a public record source. Title companies generating farm packages, mailing lists, etc., would be wise to ascertain exactly how these lists are generated and if they contain any nonpublic personal information to avoid having to provide a notice on with whom that information is shared and an opportunity to opt-out!

As discussed above, there is an exemption from the Opt-Out Notice provisions of the GLBA if the information exchange is “necessary to effect, administer, or enforce the transaction” initiated by the consumer. Thus, even if some of the information is being shared with real estate professionals, the title insurer, the escrow company, lender, etc., involve some personal information derived from the consumer or their financial institution, it is exempt from the Opt-Out Notice provisions of the GLBA.

In summary, UTCs are financial institutions subject to the GLBA. Most, if not all, of the information they collect, use, store, etc., is derived from public sources and is not subject to the Opt-Out Notice and Disclosure of Institution Privacy Policy requirements of the GLBA. *However, to the extent that UTCs collect any other information that contains “nonpublic personal information” from escrow documents, statements of identity, etc., it is subject to the Disclosure of Institution Privacy Policy requirements set forth in the GLBA in Section 6803. Assuming this to be true your policy of disclosure and sharing of any files, databases, website access portals, etc., containing this nonpublic personal information would need to be addressed in the disclosure. However, there does not need to be any opt-out option provided if the information is not shared with a third party or is only shared in the context of effectuating a transaction.*

- G. The FTC recently adopted new regulations dealing with “Standards for Safeguarding Customer Information” (16 CFR Part 314) on May 23, 2002. How do those recently enacted regulations affect UTCs?

As discussed above, the FTC already enacted regulations dealing with the “Privacy of Consumer Financial Information” (16 CFR Part 313) on May 24, 2000. These regulations dealt with the “Opt-Out Notice” (Sections 313.4 – 313.9) and the “Privacy Disclosure Notice” (Sections 313.10 –313.12).

In addition, the FTC, on May 23, 2002, enacted **new regulations** pursuant to the authority granted in the GLBA to specifically require “financial institutions” to develop and maintain security measures and safeguards to protect databases, computer files, paper documents, etc., containing “nonpublic personal information” as defined within the GLBA. The new regulations are entitled “Standards for Safeguarding Customer Information” and were codified in FTC regulations 16 CFR Part 314, published on May 23, 2002 in the Federal Register.

The Internet link to these new regulations can be found at the following FTC website: www.ftc.gov/os/2002/05/safeguardfrn.pdf

- 1) What is the purpose of these regulations?

Recently, the FTC enacted new regulations for “Standards for Safeguarding Customer Information” for those entities subject to the GLBA. These regulations seek to ensure the security and confidentiality of customer records and information; protect against any anticipated threats to those records; and protect against other potential harm to consumers resulting from an unauthorized release of that information.

- 2) What records are supposed to be protected?

All “customer information” is to be protected. “Customer information” is defined to be “nonpublic personal information” as defined in 16 CFR 313.3 (n). In other words, public records and publicly available information would be excluded (as it is in the GLBA) from this definition.

- 3) Are UTCs subject to these new regulations?

Not with respect to solely public information since it would not be “customer information” as defined within the new regulations.

However, to the extent UTCs generate, compile, use, or share “nonpublic personal information” (perhaps gleaned from Statement of Identity Forms, escrow documents, etc.) they would be subject to these new regulations in regards to how they handle that information.

In essence, whatever information UTCs may possess that is “customer information” under the GLBA would be subject to the safeguard requirements as outlined in these new regulations.

- 4) In brief, what would the new regulations require?

UTCs, to the extent they possess nonpublic personal information, would be required to establish what is called an "Information Security Program" as defined within Section 314.3 of the new regulations.

This program would contain administrative, technical, and physical safeguards that are "appropriate to the size, complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue" (Section 314.3 (a)). Nonpublic personal information contained within computer files, paper, or other form would be required to be protected (Section 314.2 (b)).

In addition, one or more employees would be required to coordinate the program (Section 314.4 (a)) and it would need to be designed to protect against foreseeable internal and external risks (Section 314.4(b)). The necessary training, software expenditures, etc., must be undertaken (Section 314.4).

- 5) Do they apply to nonaffiliated third parties with whom a UTC contracts?

Yes. However, there is a two year grandfathering of nonaffiliated third party service contracts from that part of the regulation which requires you to require your service providers to implement and maintain such safeguards.

- 6) When are these new regulations effective?

Under the FTC regulations, companies have one year from the date published in the Federal Register (May 23, 2002) to implement the information security program.

III. **FTC Rule on Disposal of Consumer Report Information and Records** (ALTA Summary)

**AMERICAN
LAND TITLE
ASSOCIATION**

Washington Update

June 20, 2005



Disposing of Consumer Report Information? New FTC Rule Tells How

In an effort to protect the privacy of consumer information and reduce the risk of fraud and identity theft, a new federal rule is requiring businesses to take appropriate measures to dispose of sensitive information derived from consumer reports.

Any business or individual who uses a consumer report for a business purpose is subject to the requirements of the Disposal Rule. The Rule requires the proper disposal of information in consumer reports and records to protect against “unauthorized access to or use of the information.” The Federal Trade Commission, the nation’s consumer protection agency, enforces the Disposal Rule.

According to the FTC, the standard for the proper disposal of information derived from a consumer report is flexible, and allows the organizations and individuals covered by the Rule to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology.

Although the Disposal Rule applies to consumer reports and the information derived from consumer reports, the FTC encourages those who dispose of any records containing a consumer’s personal or financial information to take similar protective measures.

Who must comply?

The Disposal Rule applies to people and both large and small organizations that use consumer reports. Among those who must comply with the Rule are:

- Consumer reporting companies
- Lenders
- Insurers
- Employers
- Landlords
- Government agencies
- Mortgage brokers
- Automobile dealers
- Attorneys or private investigators
- Debt collectors
- Individuals who obtain a credit report on prospective nannies, contractors, or tenants
- Entities that maintain information in consumer reports as part of their role as service providers to other organizations covered by the Rule

What information does the Disposal Rule cover?

The Disposal Rule applies to consumer reports or information derived from consumer reports. The Fair Credit Reporting Act defines the term consumer report to include information obtained from a consumer reporting company that is used – or expected to be used – in establishing a consumer’s eligibility for credit, employment, or insurance, among other purposes. Credit reports and credit scores are consumer reports. So are reports businesses or individuals receive with information relating to employment background, check writing history, insurance claims, residential or tenant history, or medical history.

What is ‘proper’ disposal ?

The Disposal Rule requires disposal practices that are reasonable and appropriate to prevent the unauthorized access to – or use of – information in a consumer report. For example, reasonable measures for disposing of consumer report information could include establishing and complying with policies to:

- burn, pulverize, or shred papers containing consumer report information so that the information cannot be read or reconstructed;
- destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed;
- conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the Rule. Due diligence could include:
 - reviewing an independent audit of a disposal company’s operations and/or its compliance with the Rule;
 - obtaining information about the disposal company from several references;
 - requiring that the disposal company be certified by a recognized trade association;
 - reviewing and evaluating the disposal company’s information security policies or procedures.

The FTC says that financial institutions that are subject to both the Disposal Rule and the Gramm-Leach-Bliley (GLB) Safeguards Rule should incorporate practices dealing with the proper disposal of consumer information into the information security program that the Safeguards Rule requires (ftc.gov/privacy/privacyinitiatives/safeguards.html).

The Fair and Accurate Credit Transactions Act, which was enacted in 2003, directed the FTC, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, and the Securities and Exchange Commission to adopt comparable and consistent rules regarding the disposal of sensitive consumer report information. The FTC’s Disposal Rule became effective June 1, 2005. It was published in the Federal Register on November 24, 2004. ([69 FR 68690](http://www.federalregister.gov))