

Records Disposal and the Law: Trends to Watch in 2006

Charles H. Kennedy
Counsel, Morrison & Foerster, LLP

INTRODUCTION AND SUMMARY

2005 was a momentous year for the law of records management, and 2006 promises to be equally lively.

The most important development of 2005 was the Federal Trade Commission's ("FTC") Disposal Rule, which took effect on June 1, 2005.¹ The Disposal Rule implements certain provisions of the Fair and Accurate Credit Transactions Act ("FACTA"), which requires "any person that maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose to properly dispose of such information or compilation."² Under the new FTC Rule, all covered entities must implement and comply with "policies that require the burning, pulverizing, or shredding of papers concerning consumer information so that the information cannot practicably be read or reconstructed."³ The Rule also requires businesses to exercise "due diligence" in selecting records disposal companies, including the obtaining of references and consideration of any third-party certifications the disposal company has obtained.⁴

As covered in the Iron Mountain white paper entitled "If You Don't Think the FACTA Disposal Rule Applies to You, Think Again!," the impact of the Disposal Rule will extend to every private and governmental organization in the country. The FTC will move aggressively to enforce the Rule, and other agencies – both state and federal – will take the Rule as their template for enforcement of their own consumer protection authority against organizations that fail to dispose properly of records containing personal information. At the same time, lawyers representing plaintiffs in class-action lawsuits will look to the Rule as establishing a "standard of care" against which juries can measure the document disposal efforts of corporate defendants.

In addition to the Disposal Rule, individual states have adopted disposal requirements that, in some cases, are even more exacting than those of the FTC. As of January 1, 2006, nine (9) states now require companies doing business in those states, or maintaining records that include personal information of residents of those states, to take reasonable measures to prevent the unauthorized disclosure of personal information contained in such records when they are undergoing disposal.⁵ Most of those statutes specifically require that paper documents containing personal information be *shredded*. Burning and other methods of destruction of paper documents do not comply with the laws of these states.⁶

Finally, 2005 saw a proliferation of state laws that require companies to give notice to consumers of any breach in the security of their systems or data involving personal information. These "breach notification" laws started in California and now have been adopted in 22 other states.⁷ Under those laws, failure to notify consumers of a data security problem – even one that does not result in identity theft or other tangible harm – is an offense in itself. These laws severely restrict the ability of companies to conceal the results of inadequate records disposal practices.

The legal requirements for proper document destruction will continue to evolve in the coming year. As this white paper details, businesses should monitor important developments in the following areas:

- Enactment of new state laws requiring secure data disposal.
- Enactment of a federal breach-notification law.
- New class-action suits against companies that lose or inadvertently disclose consumer information.
- Increased enforcement activity at the state and federal level.

Charles H. Kennedy has taught cyberlaw and communications law for the past ten years at the Columbus School of Law, Catholic University of America, and is an author of four books on the law of electronic communications. He is Of Counsel to Morrison & Foerster, LLP, where he can be reached at ckennedy@mofo.com.

I. NEW STATE LAWS REQUIRING SECURE DATA DISPOSAL

A. State Disposal Laws Already on the Books

The records disposal laws adopted to date by nine states, including high population states like New Jersey, Texas and California, will have an impact far beyond the borders of those jurisdictions.⁸ In fact, we can expect those states to enforce their laws against any company, wherever located, that maintains information containing those states' residents.

Among other things, the nationwide reach of state disposal laws makes shredding the only prudent option for disposal of paper records that contain personal information. With one exception, all of the state statutes specify the same three disposal methods: "shredding," "erasing," or otherwise "modifying the personal information in the records" to make it unreadable or undecipherable.⁹ Two of these prescribed methods – "erasing" or "modifying" personal information – can effectively be applied only to electronically-stored data. This leaves only "shredding" as a permissible disposal method for paper records. Accordingly, the eight state laws that require companies to shred, erase or modify personal data are often referred to, quite accurately, as "must-shred" laws as they apply to paper records.

The only exception to the "must-shred" approach is North Carolina, which defines reasonable disposal measures to include "[i]mplementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing personal information so that the information cannot practicably be read or reconstructed."¹⁰

North Carolina's permitted alternative disposal methods of "burning" and "pulverizing," however, are not practical options for companies that have – or will obtain – personal information of residents of Arkansas, California, Colorado, Georgia, Montana, New Jersey, Texas, or Washington. If a company maintains personal information of residents of those states – and companies with a national marketing footprint almost certainly *will* have such data – it must shred paper records containing that information or face possible enforcement action. Accordingly, national companies that wish to comply with all applicable state disposal laws have two options: they can undertake the pointless task of using different disposal methods for information concerning residents of different states, or they can shred all of their paper documents that contain personal information. In effect, "must shred" is now the national standard for disposal of sensitive paper records.

B. State Disposal Legislation Introduced in 2005

The proliferation of state records disposal laws shows no sign of abating and likely will continue in the 2006 sessions of the various state legislatures.

Bills introduced in 2005 confirm this trend, and a number of those bills specify or endorse shredding as a proper or prescribed method for disposing of records that contain personal information. For example, a bill introduced in the Illinois General Assembly would provide that "each agency's program for efficient management of records [must] require shredding as the means of destroying or disposing of personal records unless otherwise required by the act."¹¹ Similarly, a bill introduced in the New York State Assembly would require "any medical business, tax preparation business or other business person to properly dispose of records containing personal information through one or more of the following means: shredding, destruction, modification, or other reasonable action to ensure that no unauthorized person will have access to the personal information..."¹² Other bills that mandate proper disposal of paper documents containing personal information were introduced in the legislatures of Maryland and Pennsylvania.¹³

In light of the continuing public and political concern with breaches of data security, many more states can be expected to adopt document disposal legislation in the coming year.

II. PROSPECTS FOR A FEDERAL BREACH NOTIFICATION LAW

Since 2003, when California adopted the first law requiring businesses to notify consumers of breaches of network security involving stored personal information, 22 other states have enacted similar legislation. As a result, U.S. businesses must monitor and comply with a wide variety of breach notification obligations, and the compliance burden this situation imposes is likely to increase as more states adopt breach notification laws in the New Year.

In 2005, Congress discovered that breach notification laws are popular with the public and moved accordingly. Several breach notification bills were introduced in the House and Senate, and although none of those bills became law, a new federal statute may be passed in 2006.¹⁴ If such a federal law is not enacted, or if that law fails to preempt more restrictive state statutes, American business will continue to be burdened with the task of compliance with dozens of breach notification laws.

A. State Breach Notification Laws

The state breach notification laws already on the books create a crazy quilt of obligations for U.S. business. All of those statutes require business and/or public organizations to report certain occurrences involving defined categories of personal information, and all of those statutes impose penalties for failure to comply. The laws vary widely, however, in significant ways, including the entities to which they apply, the types of information they are intended to protect, and the level of the security breaches that give rise to a duty to report.

For example, some of the state laws apply to all persons or businesses within the state that own or license personal information (although they may exempt financial and healthcare organizations already subject to federal data security regulations).¹⁵ Other states limit their breach notification requirements to specially-defined entities, such as “information brokers”¹⁶ and “data collectors.”¹⁷ Still other laws apply to state agencies and political subdivisions.¹⁸

Equally confusing is the range of “personal information” categories to which the breach notification laws apply. For example, most of the statutes apply to “computerized” personal data; but North Carolina’s law requires notification of breaches of the security of “personal information in any form (whether computerized, paper, or otherwise).”¹⁹ Therefore, businesses that experience security breaches involving only paper records must report those incidents if North Carolina residents will be affected. (Businesses also must be aware that failure to report an incident involving paper records may be challenged by the FTC and state authorities as an unfair trade practice – and may form the basis of private lawsuits by affected consumers.)

Similarly, most of the statutes define the “personal information” to which they apply as including a person’s name combined with one or more standard items, such as a Social Security number, driver’s license number, or financial account numbers and access codes.²⁰ Some laws, however, cover additional categories of data, such as date of birth, mother’s maiden name, medical history and digital signatures.²¹

Even more confusing are the states’ different definitions of the circumstances that constitute reportable security breaches. This element of the statutes is especially important to both businesses and consumers. At one extreme, consumers will not benefit from (and will learn to ignore) repeated notices of trivial system incidents that create no real risk of identity theft or other harm. At the other extreme, notifications that are withheld until harm to consumers is confirmed may be “too little, too late” to prevent losses. Ideally, breach notification laws will strike a balance between these extremes, by only requiring companies to give notice of breaches that create a significant, if less than certain, risk that personal information has gotten into the wrong hands and will be misused.

Most of the notification laws now on the books resolve this dilemma by erring on the side of more notice rather than less. The typical statute borrows from California, which requires disclosure of “any breach of the security of the system following discovery or notification of the breach in 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.”²² “Breach of the security of the system,” in turn, is defined by California and most other states as “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.”²³

Under this “California” standard, the duty to notify is triggered whenever there is a risk that an unauthorized person has *acquired* personal data, even if there are no specific facts to suggest that the information will be used to harm consumers. For example, a company might discover the theft of a laptop computer that contains unencrypted personal information. The company might have no reason to believe that the thief was interested in the stored information. Nevertheless, if the laptop contains personal information of residents of California, or of any of the other states that have adopted the California approach, notification of the incident likely would be required simply because an unauthorized person – knowingly or not – now has access to the information stored in the laptop’s hard drive.

Some states, however, let businesses decide not to disclose certain breaches that might have resulted in unauthorized acquisition of personal information. Specifically, a few states have adopted “risk of harm” statutes that require notice only if the breach is reasonably likely to result in criminal activity or other harm to consumers.²⁴ A company in such a “risk of harm” state might, for example, choose not to disclose the theft of a laptop that was promptly recovered from a local pawnshop, on the assumption that the thief was simply looking for quick cash and had neither the time nor the motivation to acquire and misuse the personal data stored on the machine. (Of course, if the thief later turns out to have downloaded the data and turned it over to an identity theft ring before pawning the laptop, the company’s decision will be liberally second-guessed by affected consumers and state authorities.)

More state breach notification laws were proposed in 2005, and more will be enacted in 2006.²⁵ For at least two reasons, however, 2005 saw a strong movement in Congress to pass a federal notification law. One set of pressures came from consumer groups that want to replace or reinforce the patchwork of state laws with a universal, California-type notification requirement. Other pressures came from business interests that prefer a federal “risk of harm” law that preempts more restrictive state obligations. These contradictory demands produced a number of bills and no definitive action, but the battle to craft a national breach notification law will continue in 2006.

B. The Push for A Federal Breach Notification Law in 2006

1. Who Will Be Covered By The Proposed Federal Notification Law?

First, and fundamentally, Congress must decide who will be subject to the federal notification law. Some of the bills introduced in 2005 would have covered all U.S. businesses engaged in interstate commerce, and some would have applied to governmental bodies.²⁶ Other bills covered only financial institutions, credit reporting agencies or “information brokers.”²⁷

The choice of entities that will be covered by a new law will have several implications. Notably, if a federal statute fails to cover entities that are subject to one or more state notification laws, those entities may continue to be subject to multiple state obligations even if Congress elects to preempt state laws that cover entities subject to the federal law. Similarly, if Congress elects to cover credit reporting agencies, financial institutions, healthcare institutions or other entities that already are subject to federal data security regulations, it must ensure that the new law does not weaken or otherwise conflict with existing obligations. Finally, Congress’s definitions of the categories of businesses subject to the new law must be clear enough to preclude confusion about which companies are covered and which are not.

2. When Will Companies Have An Obligation To Give Notice?

The greatest challenge of drafting a security breach notification bill is deciding when notice of a breach will be required. In testimony given before Congress in 2005, business interests warned that if companies must report every system incident, including those that pose no plausible risk of harm, consumers will be deluged with “false alarm” notices that they probably will learn to ignore. Accordingly, the business witnesses urged Congress to adopt a “risk of harm” standard rather than a statute that follows the lead of California’s notification law. Consumer groups, not surprisingly, testified that letting businesses decide when breaches of their systems pose a reportable risk of harm would put the fox in charge of guarding the henhouse. The consumer groups, along with the attorneys general of several states, therefore urged Congress to adopt a California-type standard or, at least, decline to preempt state laws that include that standard.

The bills introduced in 2005 take a wide variety of approaches to this balancing act. At one extreme, some of the bills give companies great latitude to investigate security incidents and decide, on the basis of their own assessment of the risk involved, whether notice to consumers is required. For example, H.R. 3997, the Financial Data Protection Act of 2005, provides as follows:

- (a) Security Policies and Procedures - Each consumer reporter shall have an affirmative obligation to implement, and a continuing obligation to maintain, reasonable policies and procedures to protect the security and confidentiality of sensitive financial personal information relating to any consumer that is maintained, serviced, or communicated by or on behalf of such consumer reporter against any unauthorized use that is reasonably likely to result in substantial harm or inconvenience to such consumer.
- (b) Investigation Requirements-
 - (1) INVESTIGATION REQUIRED - Whenever any consumer reporter determines or becomes aware of information that would reasonably indicate that a breach of data security has or may have occurred or is reasonably likely to be about to occur, or receives notice under subsection (d), the consumer reporter shall immediately conduct a reasonable investigation to --
 - (A) assess the nature and scope of the potential breach;
 - (B) identify the sensitive financial personal information involved; and
 - (C) determine if the potential breach is reasonably likely to result in substantial harm or inconvenience to any consumer to whom the information relates.
 - (2) SCOPE OF INVESTIGATION - An investigation conducted under paragraph (1) shall be commensurate with the nature and the amount of the sensitive financial personal information that is subject to the breach of data security.
 - (3) FACTORS TO BE CONSIDERED - In determining the likelihood under this section that sensitive financial personal information that was the subject of a breach of data security has been or will be misused, the consumer reporter shall consider all available relevant facts, including whether the information that was subject to the breach was encrypted, redacted, required technology to use that is not generally commercially available, or is otherwise unreadable or unusable.

- (c) Investigation Notices and System Restoration Requirements - If a consumer reporter determines after commencing an investigation under subsection (b) that a potential breach of data security may result in substantial harm or inconvenience to any consumer to whom the sensitive financial personal information involved in such potential breach relates, the consumer reporter shall --
- (1) promptly notify the United States Secret Service;
 - (2) promptly notify the appropriate functional regulatory agency for the consumer reporter;
 - (3) notify as appropriate and without unreasonable delay --
 - (A) any entity that owns or is obligated on a financial account that may be subject to unauthorized transactions as a result of the breach, to the extent the breach involves related sensitive financial account information, including in such notification information reasonably identifying the nature and scope of the breach and the sensitive financial personal information involved;
 - (B) each nationwide consumer reporting agency, in the case of a breach involving sensitive financial identity information relating to 1,000 or more consumers; and
 - (C) any other appropriate critical third parties --
 - (i) whose involvement is necessary to investigate the breach; or
 - (ii) who will be required to undertake further action with respect to such information to protect such consumers from resulting fraud or identity theft;
 - (4) to the extent possible and practicable, take reasonable measures to repair the breach and restore the security and confidentiality of the sensitive financial personal information involved to limit further unauthorized use of such information; and
 - (5) take reasonable measures to restore the integrity of the affected data security safeguards and make appropriate improvements to data security policies and procedures.²⁸

Other bills do not permit companies to rely upon their own investigations as a basis for nonreporting. For example, S.1332, the Personal Data Privacy and Security Act of 2005, simply states that notice is required “following the discovery of a security breach of its system or databases in its possession or control when such security breach impacts sensitive personally identifiable information.”²⁹ A “security breach,” in turn, is defined in S. 1332 as “compromise of the security, confidentiality, or integrity of computerized data through misrepresentation or actions that result in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personally identifiable information.”³⁰

The choice Congress makes between these different reporting thresholds will significantly affect the risk to business that a new federal breach-notification statute will pose. If Congress chooses a standard like the one set out in S.1332, businesses will be required to report any security breach that they reasonably believe to have resulted in unauthorized access to personal information – including, presumably, cases in which the unauthorized access is unlikely to cause harm. Those notifications may have little benefit for consumers, but they will undermine the affected businesses’ public image and alert the FTC, and other enforcement agencies, to possible defects in those businesses’ data protection practices. If, on the other hand, Congress adopts a standard like the one set out in H.R. 3997, companies might fail to remedy lax procedures that eventually *will* cause harm to the public.

Finally, even if Congress passes a bill with the more business-friendly approach of H.R. 3997, it is by no means certain that Congress will preempt more restrictive state laws. If Congress elects not to preempt, and important states like California continue to require notice of even “harmless” breaches, companies that do business nationally will be forced to comply.

3. Will Congress Preempt the States’ Breach Notification Laws?

In the testimony and debates concerning the federal breach notification bills introduced in 2005, business interests urged Congress to preempt the breach notification laws of the states. Such preemption would have created a single breach notification regime for all U.S. companies, regardless of where they did business and where their customers were located.³¹

The states and the consumer protection groups generally opposed preemption, arguing that state laws with more stringent notification requirements should continue to be enforced.³² Under this approach, for example, a new federal law that permitted companies to forego notification when their own investigations of a breach showed no risk of actual harm to consumers would not relieve those companies of the obligation to notify consumers in California and other states that have less permissive laws. This result would effectively leave business interests no better off than they were before federal legislation was passed.

The preemption issue promises to remain highly contentious in 2006. If Congress fails to include clear language on the issue of preemption, we could see a repeat of the lengthy and inconclusive challenges to state “do-not-call” requirements that resulted from the ambiguous preemption language of the 1991 federal telemarketing statute.³³ As that experience has shown, unless Congress expresses its intention to preempt in unmistakable language, the states will continue to enforce their breach notification laws aggressively.

Finally, it is by no means certain that new federal legislation will emerge from the debate that resumes in 2006. The competing interests affected by breach notification may produce a continuing deadlock. Also, a number of congressional committees can legitimately claim jurisdiction over this issue, and such turf battles are a frequent source of inaction on Capitol Hill. If a new federal law does not emerge this year, businesses must continue to monitor the state capitols for new – and perhaps inconsistent – notification obligations. As is always the case when states make rules for nationwide businesses, the most restrictive state law is likely to become the standard.

III. NEW CLASS-ACTION SUITS

2005 will be remembered as the year plaintiffs’ lawyers discovered data security. The first major event, but by no means the only one, was the fallout from Choicepoint, Inc.’s disclosure of personal information of more than 500,000 people to representatives of dummy companies that posed as legitimate Choicepoint customers. Starting with a claim filed in Los Angeles on February 18, 2005 – only three days after the data breaches were disclosed – a number of class-action suits have been brought on behalf of individuals who claim that their personal information was compromised.³⁴ Only the following month, a shareholders’ suit against Choicepoint alleged that the company harmed actual and potential investors by failing to disclose the inadequacy of its security practices.³⁵

Choicepoint has not been the only target of private lawsuits arising out of data security breaches. CardSystems Solutions, Inc. is the defendant – along with VISA, Mastercard and one bank – in a class-action suit arising out of the theft of information concerning some 40 million credit card accounts.³⁶ Similarly, after the FTC brought its action against BJ’s Wholesale Club for loss of unsecured bank card data that was used to make fraudulent purchases, a number of card issuers sued BJ’s for the cost of reimbursements to cardholders and cancellation and reissuance of compromised accounts.³⁷ Also, a class-action complaint was filed against LexisNexis, Reed Elsevier Inc. and Seisint for alleged, unauthorized disclosures of credit reports and other personal information.³⁸

The success of these complaints is by no means assured, and one court already has dismissed a class-action claim for lack of evidence that a health insurance manager's loss of a computer hard drive containing beneficiaries' personal information caused any actual harm to the plaintiffs.³⁹ A proper case, however, brought by defendants who have suffered identity theft or other actual harm because of careless handling of personal data, could result in crippling damage awards against corporate defendants. Companies that store personal data should watch the progress of the pending class-action claims closely. They should expect more such claims to be brought as companies continue to issue the breach notifications required by state (and, perhaps, federal) breach reporting requirements.

IV. INCREASED REGULATORY ENFORCEMENT

As detailed in the Iron Mountain white paper entitled "If You Don't Think the FACTA Disposal Rule Applies to You, Think Again!," the FTC has a history of looking for enforcement targets when Congress passes a new law for that agency to enforce. Such enforcement action sends a signal to industry that the Commission is serious about the new law and demonstrates to Congress that the agency makes good use of the authority entrusted to it.

As noted earlier, in 2005 the FTC took the critical step that will permit it to enforce the records disposal requirements of the Fair and Accurate Credit Transactions Act. By adopting a specific Disposal Rule, the Commission sent a signal to businesses that maintain personal information that they must follow reasonable disposal practices or face adverse action.

The likelihood of new enforcement activity is underscored by recent FTC initiatives in the privacy and consumer protection areas. On December 1, 2005, the Commission announced its settlement of an action against DSW Inc., which allegedly had allowed hackers to gain access to bank card and checking account information of more than 1.4 million customers. Among the Commission's charges against DSW was that the company failed to dispose of duplicate customer files that no longer were needed in its business operations.⁴⁰ Although the FTC did not specifically cite its new Disposal Rule, the specific reference to failure to dispose of sensitive records demonstrates the Commission's awareness of this issue.

Another emerging element of the FTC's enforcement program is its increased tendency to demand significant monetary damages, as well as consent decrees, against companies that violate consumers' rights. The most dramatic demonstration of this new emphasis is the December, 2005 settlement between the Commission and DirecTV, which agreed to pay \$5,335,000 for making unlawful sales calls to residential telephone numbers of the national Do Not Call Registry.⁴¹ Against this background, businesses should not be surprised if enforcement actions against violators of the FTC Disposal Rule are accompanied by demands, not only for the defendant's agreement to a lengthy consent decree, but for payment of substantial penalties as well.

Finally, it should be remembered that the FTC is not the only source of consumer protection enforcement, including actions against companies that suffer loss or compromise of consumer data. The states are equally aggressive in this area, and many of the states' attorneys general look to the FTC and emulate the enforcement priorities of that agency.

CONCLUSION

2005 brought data security to the forefront of public and political awareness, and the fallout from those events is still building. Businesses that store personal information should be aware that the attention given to this issue is not a fad and will not soon subside. Proper management and disposal of records is a high-level corporate governance issue that will be with us for years to come.

FOOTNOTES

- 1 16 C.F.R. Pt. 682.
- 2 *Fair and Accurate Credit Transactions Act of 2003*, Pub.L. 108-159, 111 Stat. 1952, 15 U.S.C. § 1681w(a)(1).
- 3 16 C.F.R. Pt. 682, § 682.3(b)(1).
- 4 *Id.* § 682.3(b)(3).
- 5 *Arkansas Code Annotated* §§ 4-110-103 et seq.; *California Civil Code* §§ 1798.80 et seq.; *Colorado Revised Statutes* § 6-1-713; *Official Code of Georgia Annotated* §§ 10-15-1 et seq.; *Montana Code Annotated* § 30-14-1702; *New Jersey Statutes* §§ 56:8-161 et seq.; *North Carolina General Statutes* § 75.61 et seq.; *Texas Business & Commercial Code* § 48.102; *Revised Code of Washington* § 19.215.
- 6 See, e.g., *Arkansas Code Annotated* § 4-110-104(a); *California Civil Code* § 1798.81; *Official Code of Georgia Annotated* § 10-15-2; *Montana Code Annotated* § 30-14-1703; *New Jersey Statutes* § 56:8-162; *Texas Business & Commercial Code* § 48.102(b); *Revised Code of Washington* § 215.010(2).
- 7 *Arkansas Code Annotated* §§ 4-110-103 et seq.; *California Civil Code* § 1798.82; *Connecticut Senate Bill S.B. 650* (2005, effective Jan. 1, 2006); *6 Delaware Code* §§ 101 et seq.; *Florida Statutes* § 817.5681; *Official Code of Georgia Annotated* §§ 10-10911 et seq.; *815 Illinois Code* § 530/10(a); *Louisiana Revised Statutes* §§ 51:3073 et seq.; *Sec. 1.10 Maine Revised Statutes Annotated* ch. 210-B §§ 1347 et seq.; *Minnesota Statutes* § 325E.61; *Montana Code Annotated* § 30-14-1704; *Nevada Revised Statutes* Sec. 17, Title 52, § 24; *New Jersey Statutes* § 56:8-163; *New York Consolidated Law Service General Business* § 899aa; *North Carolina General Statutes* § 75-65; *North Dakota Century Code* § 51-30-02; *Pennsylvania Senate Bill No. 712*, Session of 2005, *Breach of Personal Information Notification Act* (effective July 1, 2006); *Rhode Island General Laws* § 1-49.2-3; *2005 Tennessee Public Acts* 473, amending Title 47, Chapter 18, Part 21 of *Tennessee Code Annotated*; *Texas Business & Commercial Code* § 48.103; *Revised Code of Washington* § 19.255.010.
- 8 If a company is a financial institution, medical business or tax preparation business, it also is subject to Wisconsin's "must-shred" law. *Wisconsin Statutes* § 895.505. Some of the state disposal statutes also apply to governmental agencies. See, e.g., *Colorado Revised Statutes* § 6-1-713(1) (applies to "each public and private entity in the state"); *New Jersey Statutes* § 56:8-162 (applies to any "business or public entity"); *Revised Code of Washington* §§ 19.215.020(1), 19.215.010(2) (applies to any "entity," defined to include "a sole proprietor, partnership, corporation, limited liability company, trust association, financial institution, governmental entity, other than the federal government, and any other individual or group, engaged in a trade, occupation, enterprise, governmental function, or similar activity in this state, however organized to operate a profit." Accordingly, government agencies, no less than private businesses, should be aware of their obligations under the records disposal laws of their states.
- 9 *Arkansas Code Annotated* § 4-110-104(a).
- 10 *North Carolina General Statutes* § 75.64(b).
- 11 *Illinois General Assembly*, House Bill HB 4229, synopsis as introduced, available at http://www.ilga.gov/legislation/BillStatus_pf.asp?DocNum=4229&DocTypeld=HB&Legl.
- 12 *New York Assembly Bill A08456*, <http://assembly.state.ny.us/leg/?bn=A08456>.
- 13 *Maryland House bill 1588* introduced March 8, 2005 by Delegate Moe, summarized at *State Net Maryland Bill Tracking*, 2005 *Bill Tracking MD H.B. 1588*; *General Assembly of Pennsylvania House Bill No. 1921*, Session of 2005, referred to Committee on Commerce August 18, 2005.
- 14 See, e.g., S.1332, *Personal Data Privacy and Security Act of 2005*; S.1789, *Personal Data Privacy and Security Act of 2005*; S.1216, *Financial Privacy Breach Notification Act of 2005*; S.1594, *Financial Privacy Protection Act of 2005*; S.768, *Comprehensive Identity Theft Prevention Act*; S.1408, *Identity Theft Prevention Act*; S.751, *Notification of Risk to Personal Data Act*; S.115, *Notification of Risk to Personal Data Act*; H.R. 3997, *Financial Data Protection Act of 2005*; H.R. 3140, *Consumer Data Security and Notification Act of 2005*; H.R. 3374, *Consumer Notification and Financial Data Protection Act of 2005*; H.R. 3375, *Financial Data Security Act of 2005*; H.R. 1069, *Notification of Risk to Personal Data Act*.
- 15 See, e.g., *Minnesota Statutes* § 325E.61(1)(a); *Texas Business & Commercial Code* § 48.103(b); *Arkansas Code Annotated* § 4-110-105.

- 16 An “information broker” is defined in Maine as “a person who, for monetary fees or duties, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties.” Maine Revised Statutes Annotated 210-B § 1347(3). See also Official Code of Georgia Annotated § 10-1-911(2).
- 17 In Illinois, a data collector “may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.” Illinois H.B. 1633, Public Act 94-36, § 5.
- 18 See, e.g., California Civil Code § 1798/29(a); Burns Indiana Code Annotated 4-1-11-5(a); Minnesota Statutes § 13.055(2); Ohio Revised Code Annotated § 1347.12(B)(1).
- 19 North Carolina General Statutes § 75-65(a). Businesses should be aware that breaches of the security of paper records, although not technically covered by the breach notification laws of most states, must be disclosed if any North Carolina residents are affected. Also, failure to report a breach of paper records may be challenged by the FTC or the states as an unfair trade practice, and may form the basis of private lawsuits by affected consumers.
- 20 See, e.g., California Civil Code § 1798.29(e); 6 Delaware Code § 101(4); Florida Statutes § 817.5681(5); Texas Business & Commercial Code § 48.002(2)(defining “sensitive personal information”).
- 21 See, e.g., Arkansas Code Annotated § 4-110-103(7); North Carolina General Statutes § 75-65(a); North Dakota Century Code § 51-30-01(2).
- 22 California Civil Code § 4-110-105(b).
- 23 *Id.* § 1798.82(d).
- 24 See, e.g., Florida Statutes § 817.5681(10); North Carolina General Statutes § 75-61(14); Revised Code of Washington § 19.255.010(10)(d).
- 25 See, e.g., Alaska House Bill 270 (introduced Apr. 15, 2005); Massachusetts Senate Bill 2058 (2005).
- 26 S.1332, the Personal Data Privacy and Security Act of 2005, and S.1789, would have covered all “business entities,” including nonprofits, and all agencies; S.768, the Comprehensive Identity Theft Prevention Act, would have applied to all “commercial entities;” see also S.751 and S.115.
- 27 See H.R. 3997 (“consumer reporter”); H.R. 3140 (financial institutions and “unregulated information brokers”); S.1594 (“financial services providers”); S.1408 (“consumer credit reporting agencies”); H.R. 3374 (“financial institutions”); H.R. 3375 (“consumer reporters”); H.R. 1069 (“financial institutions”).
- 28 H.R. 3997 § 630(b).
- 29 S.1332 § 421(a).
- 30 *Id.* § 3(10).
- 31 See Testimony of Oliver Ireland, Morrison & Foerster LLP, before House Subcommittee on Financial Institutions and Consumer Credit, Nov. 9, 2005 (2005 Federal News Service); Testimony of Randy Lively, American Financial Services Association, before House Subcommittee on Financial Institutions and Consumer Credit, Nov. 9, 2005 (2005 Federal News Service).
- 32 See, e.g., Testimony of Evan Hendricks, Privacy Times, before House Subcommittee on Financial Institutions and Consumer Credit, Nov. 9, 2005 (2005 Federal News Service); Testimony of Julie Brill, National Association of Attorneys General, before House Subcommittee on Financial Institutions and Consumer Credit (2005 Federal News Service).
- 33 See, e.g., Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, Report and Order, 18 FCC Rcd 14014 ¶83.
- 34 *Goldberg v. Choicepoint, Inc.*, No. BC329115 (Los Angeles Superior Court, filed Feb. 18, 2005). Three other class-action complaints were brought against Choicepoint in California, and a similar suit was filed against the company in Georgia. *Harrington et al. v. Choicepoint, Inc.*, CV05-1294; *Salladay et al. v. Choicepoint, Inc.*, CV05-1683; *Cloy v. Choicepoint, Inc.*, CV05-1993 (all consolidated in the U.S. District Court for the Central District of California); *Wilson, et al. v. Choicepoint, Inc.*, No. 05-1604 (U.S. District Court for the Northern District of Georgia).

- 35 *Perry v. Choicepoint, Inc.*, CV-05-1644 (U.S. District Court for the Central District of California, filed Mar. 4, 2005).
- 36 *Parke, et al. v. CardSystems Solutions, Inc. et al.*, CGC 05 44264 (California Superior Court, San Francisco).
- 37 *In the Matter of BJ's Wholesale Club, Inc.*, File No. 0423160 (Federal Trade Commission, Agreement Containing Consent Order, HYPERLINK "<http://ftc.gov/os/caselist/0423160/050616agree0423160.pdf>" <http://ftc.gov/os/caselist/0423160/050616agree0423160.pdf>; see, e.g., *Banknorth. N.A. v. BJ's Wholesale Club, Inc.*, No. 05 CV 0021 P S, 2005 WL 1610654, at *6 (U.S. District Court for District of Maine, July 8, 2005).
- 38 *James Syran v. LexisNexis Group, et al.*, No. 05-909 (U.S. District Court for Southern District of California).
- 39 *Sollenwerk v. TriWest Healthcare Alliance*, No. CIV 03-0185-PHX-SRB (U.S. District Court for District of Arizona)(unpublished decision, Sep. 6, 2005).
- 40 FTC Press Release, "DSW Inc. Settles FTC Charges" (Dec. 1, 2005).
- 41 FTC Press Release, "DirecTV to Pay \$5.3 Million Penalty for Do Not Call Violations" (Dec. 13, 2005).

© 2006 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated. All other trademarks are the property of their respective owners.



745 Atlantic Avenue
Boston, Massachusetts 02111
(800) 899-IRON

Iron Mountain operates in major markets worldwide, serving thousands of customers throughout the U.S., Europe, Canada, Latin America, and the Pacific Rim. For more information, visit our Web site at www.ironmountain.com.