

THE REVIEW OF
**BANKING & FINANCIAL
SERVICES**
A PERIODIC REVIEW OF SPECIAL LEGAL DEVELOPMENTS
AFFECTING LENDING AND OTHER FINANCIAL INSTITUTIONS

Vol. 20 No. 7

July 2004

PRIVACY AND SECURITY LITIGATION DEVELOPMENTS

New Federal and State Statutory Protections for Consumer Privacy and Security Have Spawned Litigation Over Commercial Uses of Motor Vehicle Records, Adverse Actions Based on Credit Reports, and Failures of Consumer Information Security. The Authors Review the Cases and Suggest Steps that Financial Institutions Should Take to Minimize Exposure to Litigation.

By James R. Tuite & [Cynthia T. Andreason](#)*

As the Internet, with its seemingly boundless capacity to collect, sort, and disseminate information, has become a fact of life, so also has public concern over the privacy and security of personal information. That concern has brought to businesses that deal with consumer personal information not only significantly increased obligations to protect that information, but also the specter of litigation over their handling of it. The volume of litigation against banks and insurers concerning consumer information privacy has slowly but steadily increased over the last several years, and, while it is early to make predictions concerning the future of such litigation, it is safe to say that statutes, rather than common law causes of action, are becoming the focal point of consumer privacy litigation. As Congress, and where not precluded, the States, continue to enact new statutes aimed at protecting consumer privacy, new questions and issues concerning the meaning

and scope of such statutes will arise, some of which will inevitably result in litigation. It is also safe to say that security breaches involving consumer information are, and will remain, a major source of litigation.

The good news is that, as discussed below, there are a number of steps companies can take to minimize their exposure to privacy and security litigation. Taking these steps well in advance of, rather than after, being sued is the best defense available to financial institutions that do not relish being repeatedly named as defendants in this litigation.

THE STATUTORY SCENE

Title V of the Gramm-Leach-Bliley Act (“GLB”)¹ was not the first statutory attempt to protect consumer information privacy. Nor, as 2003 has demonstrated, was it

*JAMES R. TUIITE is Associate General Counsel at State Farm Mutual Automobile Insurance Company in Bloomington, IL. CYNTHIA T. ANDREASON is a partner at Wiley Rein & Fielding LLP in Washington, D.C.. Their email addresses are, respectively, jim.tuite.awn7@statefarm.com and candrea-son@wrf.com.

1. 15 U.S.C. §§ 6801-6809.

IN THIS ISSUE

- **Privacy and Security Litigation Developments**

the last. Privacy statutes already abounded in November 2000,² when GLB became effective. However, most were fairly narrow in scope and had been honored primarily in the breach. That effectively ended with the passage of GLB, as financial institutions, in their efforts to comply with GLB's completely new requirements, became sensitized to the other, preexisting state and federal statutes relating to consumer privacy.

Congress continues to grapple with consumer information privacy and security issues, most recently by enacting the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"),³ the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN SPAM Act"),⁴ and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act").⁵

2. Federal statutes in force prior to 2000 include, but are not limited to: the Drivers Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725; Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506; the Family Educational Rights and Privacy Act, 20 U.S.C. §§ 1232 et seq.; the Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227; the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108; the Video Privacy Protection Act, 18 U.S.C. §§ 2701-2711; and the Health and Human Services Privacy and Security Rules implementing the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191.
3. P.L. 108-159.
4. P.L. 108-187, codified at 15 U.S.C. §§ 7701 et seq.
5. P.L. 107-56.

The FACT Act amended a number of the consumer privacy provisions of the Fair Credit Reporting Act ("FCRA").⁶ Among other things, the FACT Act reauthorized FCRA's 1996 preemption provisions, confirming the continuation of national uniform standards in information sharing by credit reporting agencies.⁷ The FACT Act requires creditors to provide "risk-based pricing notices" where creditors use credit reports to assess an applicant's eligibility for credit, and then offer terms that are "materially less favorable than the most favorable terms available to most of its customers."⁸ It also addresses identity theft, giving consumers free access to their credit reports and a new means of repairing damage resulting from identity theft, as well as placing new obligations on credit reporting agencies and financial institutions when identity theft is an issue.⁹ In addition, the FACT Act provides for consumer opt-out of affiliate information sharing if the information is used to make a solicitation for marketing purposes, but carves out a broad exception for preexisting business relationships with consumer customers.¹⁰

It is apparent that legislative action concerning privacy and security reflects public concern about these issues. As public concern over identity theft and credit scoring con-

6. 15 U.S.C. § 1681 et seq.
7. E.g., 15 U.S.C. § 1681t.
8. 15 U.S.C. § 1681m (h).
9. E.g., 15 U.S.C. §§ 1681c-1 and 1681m.
10. 15 U.S.C. § 1681s-3.

Standard & Poor's

The Review of Banking & Financial Services is a periodic supplement of the *The Review of Securities & Commodities Regulation*, which is published 22 times a year by Standard & Poor's, a division of The McGraw-Hill Companies. Executive Office 55 Water Street, New York, New York 10041. Editorial Office, 299 Park Avenue 16th floor, New York, New York 10171. Subscription rates: \$1075 per year in U.S., Canada and Mexico; \$1140 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and universities. For subscription information and customer service, please call (800) 852-1641. General Editor: Michael O. Finkelstein. Associate Editor: Sarah Strauss Himmelfarb. Copyright © 2004 by Standard & Poor's. ISSN: 1051-1741. Reproduction in whole or in part prohibited except by permission. All rights reserved. Officers of The McGraw-Hill Companies: Harold W. McGraw III, Chairman, President and Chief Executive Officer; Kenneth M. Vittor, Executive Vice President and General Counsel; Robert J. Bahash, Executive Vice President and Chief Financial Officer; Frank D. Penglase, Senior Vice President, Treasury Operations. Information has been obtained by *The Review of Banking & Financial Services* from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, *The Review of Banking & Financial Services* does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or for the results obtained from the use of such information.

The McGraw-Hill Companies

General Editor
Michael O. Finkelstein

Associate Editor
Sarah Strauss Himmelfarb

Board Members
Roland E. Brandel
Morrison & Foerster
San Francisco, CA

H. Rodgin Cohen
Sullivan & Cromwell
New York, N.Y.

Joseph Diamond
Consultant
New York, N.Y.

Carl Felsenfeld
Professor of Law
Fordham Law School
New York, N.Y.

Ralph Ferrara
Debevoise & Plimpton
Washington, D.C.

Connie M. Friesen
Sidley Austin Brown &
Wood LLP
New York, N.Y.

David L. Glass
Clifford Chance Rogers
& Wells LLP
New York, N.Y.

Robert Kurucza
Morrison & Foerster
Washington, D.C.

C. F. Muckenfuss, III
Gibson, Dunn & Crutcher
Washington, D.C.

Morris Simkin
Winston & Strawn
New York, N.Y.

Brian W. Smith
Mayer, Brown Rowe & Maw
Washington, D.C.

Thomas Vartanian
Fried, Frank, Harris, Shriver
& Jacobson
Washington, D.C.

tinues to rise, it is likely that litigation over these issues will increase, and thus we can expect to see more cases involving these issues in the near future.

RECENT LITIGATION

Drivers Privacy Protection Act

Several recent cases have alleged violations of the Drivers Privacy Protection Act (“DPPA”).¹¹ The DPPA, enacted in 1994, is an example of a consumer information privacy statute that has been on the books for a number of years, but which has not, until recently, been utilized in litigation. The DPPA was enacted in response to the murder of actress Rebecca Schaeffer, who was killed by a stalker who had obtained her address from state motor vehicle records. It imposes civil liability on “persons”¹² who knowingly obtain, use, or disclose “personal information”¹³ from state motor vehicle records for any purpose not permitted by the DPPA.¹⁴ Permitted purposes under the DPPA include use with the express written consent of the consumer,¹⁵ and

use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only

- to verify the accuracy of personal information submitted by the consumer to the business or its agents, employees, or contractors; and,
- if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purpose of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the consumer.¹⁶

Such information may also be used

by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.¹⁷

Locate.Plus.Com v. Worldwide Info. Inc.,¹⁸ involved a plaintiff corporation that was in the business of reformatting motor vehicle and driver’s license information obtained from the Iowa Department of Transportation (“Iowa DOT”) onto computer disks for sale to law enforcement agencies. Although in the past the plaintiff routinely had been allowed access to the information it needed for its business, in 1999 the Iowa DOT denied plaintiff access, citing the DPPA as its authority. The plaintiff sued, but the Iowa DOT won. On appeal, the Iowa Supreme Court affirmed the ruling in favor of the Iowa DOT on the grounds that the plaintiff was not an authorized user under the DPPA, and that the purpose for which the plaintiff sought the information was not a permissible purpose under the DPPA.

In *Sloan v. South Carolina Dep’t of Pub. Safety*,¹⁹ a consumer sued the South Carolina Department of Public Safety (“SC DPS”), alleging that it had improperly disclosed personal information about her to an entity that used such information for a purpose generally similar to that of *Locate.Plus.Com*. In *Sloan*, however, the court reached the opposite result because at the time of the sales in question, South Carolina state law expressly permitted such sales. The law in South Carolina has since changed, and the outcome would likely be different under the current law.

Levine v. ChoicePoint, Inc.,²⁰ is a class action filed on behalf of a group of consumers not against a state motor vehicle agency, but against ChoicePoint, Inc., its subsidiary, ChoicePoint Public Records, and Reed Elsevier Inc., the parent company of LexisNexis. Plaintiffs allege that the defendants obtained information from the Florida Department of Highway Safety and Motor Vehicle records and then sold it to third parties in violation of the

11. 18 U.S.C. §§ 2721-2725.

12. The DPPA defines “person” as an individual, organization or entity, not including a State or agency thereof. 18 U.S.C. § 2725(2).

13. The DPPA defines “personal information” as information that identifies an individual, including an individual’s photograph, social security number, driver identification number, name, address (but not 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver’s status. 18 U.S.C. § 2725(3).

14. 18 U.S.C. § 2721 (b).

15. 18 U.S.C. § 2721(b)(13).

16. 18 U.S.C. § 2721(b)(3).

17. 18 U.S.C. § 2721(b)(6).

18. 650 N.W.2d 609 (Iowa 2002).

19. 586 S.E.2d 108 (S.C. 2003).

20. No. 03-80491 (filed in S.D. Fla. May 30, 2003).

DPPA due to the fact that Florida has not revised its state law to incorporate the DPPA. Florida still permits third parties to obtain and resell motor vehicle records, and still uses an opt-out, as opposed to opt-in system, as required by the DPPA. The case is pending.²¹

While use of information from state motor vehicle agencies by insurers appears to be a permissible purpose under the DPPA, other financial institutions are well advised to determine, if they do not already know, whether they possess and use any information that originated from state motor vehicle agency records. Insurers may feel the impact of the DPPA rulings in a different way, in that entities named as defendants in DPPA cases are beginning to request that their insurers provide defense of and coverage for such claims.

Fair Credit Reporting Act

In recent FCRA cases, unlike the DPPA cases, courts have taken a more balanced approach, very possibly because FCRA is a statute that expressly aims at balancing consumer interests in information privacy and security and the needs of business for such information.²² For example, in *Ausherman v. Bank of America*,²³ the plaintiffs alleged that the defendants violated FCRA when one defendant, Bank of America Auto Finance Corp. (“BAAF”), improperly obtained their credit reports from a credit reporting agency at a time when the plaintiffs did not have and were not seeking a financial relationship with BAAF. The Fourth Circuit affirmed the lower court’s grant of summary judgment to the defendants, holding that BAAF’s corporate parent was not liable to the plaintiffs. It further held that because there had been internal employee confusion concerning access to credit reports, the plaintiffs could not show that BAAF knowingly and intentionally committed an act of conscious disregard to the plaintiffs, a requirement for liability under FCRA. Financial institutions confronted with allegations that they have violated FCRA will do well to keep in mind the balancing nature of the statute.

As noted above, two central issues in the debate over the FACT Act were continuation of FCRA’s preemption

of state law, and the expansion of the requirement that users of credit reports taking adverse action against consumers based on the consumer’s credit report notify the consumer of that fact via a “risk based pricing,” or “adverse action” notice. Several recent FCRA cases address these issues.

Preemption

At issue in *Davenport v. Farmers Ins. Group*,²⁴ was FCRA’s preemptive power. In *Davenport*, the plaintiffs filed a putative class action alleging that Farmers violated a Minnesota state statute that required businesses to obtain a consumer’s written consent before obtaining the consumer’s credit report. Farmers contended that the state statute was preempted by FCRA. The court granted Farmers’ motion to dismiss, without, however, addressing the preemption issue. Rather, the court held that because the state statute permitted disclosure of personal information without written authorization if another law permitted such disclosure, there was no need to determine whether or not the state statute was preempted.

While the preemption issue was sidestepped in *Davenport*, there will likely be more litigation concerning the scope of the FCRA preemptions, especially since the FACT Act not only made the FCRA preemptions permanent, it also expanded them into areas not previously preempted.

Oregon “Adverse Action” Cases

Another major question in connection with the passage of the FACT Act was the necessity vel non of more specifically articulating the adverse action notice requirements for credit transactions. That question was ultimately answered in the affirmative by the addition of Section 311.²⁵ Section 311 does not address the adverse action notice requirements for non-credit transactions. However, the adverse action notice requirements for insurers have recently been hotly contested in a group of cases in Oregon, two of which are currently on appeal to the Ninth Circuit.

In the Oregon cases, a plaintiffs’ law firm filed nine separate actions in federal court in Oregon, each alleging that

21. See also *Fresco v. Automotive Directions, Inc.*, No. 03-61063-Civ-Martinez/Dube (filed in S.D. Fla. Aug. 11, 2003).

22. 15 U.S.C. § 1681.

23. 352 F.3d 896 (4th Cir. 2003).

24. Civil File No. 03-1180 (PAM/JSM), 2003 U.S. Dist. LEXIS 14429 (D. Minn., Aug. 12, 2003).

25. Codified at 15 U.S.C. § 1681m (h).

plaintiffs have been harmed in some manner because various insurance companies have allegedly taken adverse action against them based on their consumer reports without providing adverse action notices as required by FCRA. In each of the cases decided so far, the court has ruled against the plaintiff.

In the first case, *Razilov v. Nationwide Mut. Ins. Co.*,²⁶ Razilov, who was insured by a Nationwide subsidiary, alleged, *inter alia*, that Nationwide (as opposed to its subsidiary that insured Razilov) took adverse action against him based on information in his credit reports, without providing an adverse action notice as required by FCRA. The court dismissed Razilov's claims against Nationwide. Based on the dictionary definition of "take," the court held that the FCRA adverse action notice requirement only applies to the entity that actually takes the action, i.e., the insurer that is party to the insurance contract. Participation in a decision that leads to an adverse action does not trigger the notice requirement. The court addressed and rejected substantively similar claims in *Ashby v. Farmers Ins. Group*,²⁷ and *Spano v. Safeco Ins. Co.*²⁸

In *Mark v. Valley Ins. Co.*,²⁹ the same plaintiffs' firm presented a slightly different "adverse action" notice issue to the court. Plaintiff Gustafson, a first-time applicant to Valley, alleged that Valley took an adverse action under FCRA against him when, based on his credit report, it charged him its "standard" rather than its "preferred" rate, and that Valley had violated FCRA by not providing him with a FCRA adverse action notice. The court rejected Gustafson's argument. The court held that FCRA's definition of "adverse action" for insurers³⁰ required that an adverse action notice be given only in the specific circum-

stances set forth therein, i.e., a denial of coverage, a cancellation of coverage, an increase in any charge for insurance, or an adverse or unfavorable change in the terms or amount of insurance coverage. Addressing the only one of these circumstances that was even potentially applicable, i.e., an increase in the charge for insurance, the court held that "[a]n insurer cannot 'make greater' something that did not exist previously."³¹ Therefore, according to the court, because the rate Valley gave to Gustafson was the first rate it provided to him, it was not an "increase" because there was no preexisting rate to increase, and therefore there was no adverse action. The court reached a similar result in *Rausch v. Hartford Fin. Servs. Group, Inc.*,³² and *Willes v. State Farm Fire and Cas. Co.*³³ It is significant that the FTC has filed amicus briefs in support of the plaintiffs in both *Rausch* and *Willes*.

In contrast, a Kentucky court in dicta reached the opposite conclusion. At issue in *Scharpf v. AIG Marketing*³⁴ was not whether the defendant insurer had taken an adverse action against the plaintiff, but rather, whether the defendant had a "permissible purpose," as set forth in 15 U.S.C. 1681b, for obtaining the plaintiff's credit report. While the plaintiff was on the telephone with her credit card company, she agreed to be transferred to an AIG agent to receive a free insurance quote. The agent obtained her credit score and used it to provide her with a quote. The court held that the insurer had a FCRA "permissible purpose", and therefore dismissed the plaintiff's claim. It went on to note in *dicta*, however, its belief that a FCRA adverse action had occurred, as an insured's adverse action notice obligations were not preconditioned on the existence of an application for insurance.

The outcome of these cases is of great significance to insurers. Despite the FTC's protestations to the contrary, it is far from clear what FCRA's adverse action notice requirements for insurers actually are. In the event that the FTC's interpretation prevails, insurers face the prospect of massively broadening their current adverse action notice practices, at significant expense, and consumers face the prospect of increased premiums to cover the cost of the notices. Given the laudable, but limited, purpose of the adverse action notice requirement, the

26. 242 F. Supp. 2d 977 (D. Or. 2003).

27. 261 F. Supp. 2d 1213 (D. Or. 2003) (attorney-in-fact of insurer who took adverse action against plaintiffs based on their credit reports without providing adverse action notices was not liable, because attorney-in-fact could not "take" any of the actions described in 15 U.S.C. § 1681a(k)(1)(B)(i)).

28. 215 F.R.D. 601 (D. Or. 2003) (reinsurer of insurer which took adverse action against insured was not obligated to give adverse action notices to insureds; although the reinsurance agreement contemplated that the reinsurer would collect premiums, adjust losses, and provide some direction concerning underwriting and rating for the direct insurers, ultimate control over underwriting decisions remained with the insurers and thus the reinsurer could not have taken adverse action against insureds).

29. 275 F. Supp. 2d 1307 (D. Or. 2003).

30. 15 U.S.C. § 1681a(k)(1)(B)(i).

31. 275 F. Supp. 2d at 1316.

32. CV 01-1529-BR (D. Or., July 31, 2003), (*appeal pending*).

33. CV 01-1457-BR (D. Or. July 31, 2003 and Sept. 9, 2003) (*appeal pending*).

34. 242 F. Supp. 2d 455 (W.D. Ky. 2003).

question arises whether the FTC's broad interpretation is actually in the best interest of consumers.

Information Security

Over the past couple of years there have been a series of widely publicized security failures, as a result of which personally identifiable consumer information was not protected in accordance with a company's promises that it would keep such information secure. While most of these security failures have in actuality been very limited in scope, they serve as cautionary tales as to what can happen despite a company's best efforts to protect consumer information.

In re Pharmatrak Inc. Privacy Litigation,³⁵ involved sales by Pharmatrak of a service to pharmaceutical companies that allowed the companies to collect website traffic and usage information. Despite Pharmatrak's assurances that it would not collect data, it inadvertently did so, apparently as a result of two of the subscribing companies changing the method they used to retrieve the information from Pharmatrak. The plaintiffs were the 232 Internet users whose data Pharmatrak collected. They sued Pharmatrak and pharmaceutical companies, alleging violations of the Electronic Communications Privacy Act ("ECPA").³⁶ The district court ruled in Pharmatrak's favor. On appeal, the First Circuit reversed, holding that the district court had incorrectly interpreted "consent," as defined in ECPA, and that Pharmatrak "intercepted" communications under ECPA.

In October 2003, after an investigation confirmed allegations that consumer information, including name, address, telephone number, and items ordered, was inadvertently accessible on Victoria's Secret's website for a period of several months, the New York Attorney General and Victoria's Secret reached an agreement that Victoria's Secret would compensate New Yorkers whose personal information it inadvertently left available to the public, and would implement specified reforms to improve the security of its website.³⁷

In re Ziff Davis Media was another New York Attorney General investigation, again involving inadvertent disclo-

sure of consumer information, including credit card numbers, as a result of computer programming errors. When the investigation confirmed that anyone with web access could read the site Ziff Davis used to accept magazine orders and gather its customer information base, Ziff Davis agreed with the New York and other Attorneys General that it would pay \$500 to each consumer whose data was exposed, implement various security protections, and train its employees concerning such protection.³⁸

These cases demonstrate the need for companies to continually test their own information security operations, and to update them as necessary to accommodate changes in their own operations and in the operations of entities with which they share consumer information.

What to Do

Financial institutions have significant statutory obligations to protect the privacy and security of consumer information. Identity theft concerns and other new privacy law standards will impact how federal and state security guidelines are interpreted in determining what safeguards are adequate to protect customer personal information.

Financial institutions and the business community generally must reach out for preventive law strategies as they strive to find benchmarks for what will be deemed acceptable in industry compliance programs. Defensive strategies must be considered so that preventive risk assessment approaches and strategies can be developed to address future litigation trends.

New actions are likely to surface based upon uninformed and careless information collection, sharing, and use practices within and among the enterprise, its agents, branches and vendors. Customers have been generally informed under the notice required under the GLB Act of the collection, use, and sharing practices of the enterprise. But in an era of personal identity theft, new concerns will likely focus on how information is shared both within the enterprise and with third parties to whom companies have entrusted customer personal information to perform services for their customers, and in many situations, to carry out the primary business function. Modern business enterprises provide services through many functional ser-

35. 329 F.3d 9 (1st Cir. 2003),

36. 18 U.S.C. §§ 2510-2520.

37. http://www.oag.stat.ny.us/press/2003/oct/oct21b_03.html.

38. http://www.oag.stat.ny.us/press/2002/aug/aug28a_02.html.

vice layers, many of which are outside the enterprise itself. Contracts with vendors must provide not only for confidentiality, but also for the need to safeguard customer information.

This means:

- Make privacy and security protection a core corporate and enterprise values.
 - Within the enterprise, coordinate utilization of IT functions and all elements of the enterprise that use customer information; viz., advertising, marketing, sales, service, claim handling, operations, public relations, etc.
 - Have in place decision trees and recovery plans to deal with security breaches, identity theft, and loss or wrongful disclosure of consumer personal information.
 - Undertake regular self-assessments, including privacy and security audits and evaluation of the effectiveness of the enterprise's recovery plans.
 - Focus on customer relations. A customer who is unhappy is more likely to sue. Mistakes will occur, despite best efforts to avoid them. Courteous and professional treatment of customers at all times, and especially after a mistake has been made, is an important defensive measure.
- Address breaches quickly, appropriately, and immediately. A delayed response is no response.
 - Reach out to media and adopt a media or public relations strategy so that your story can be told to the media, your customers, and the general public. Similarly, reach out to your regulators, and have in place decision trees and procedures for communicating with them concerning privacy and security issues that may arise.
 - Implement regular, documented enterprise training in privacy and security for all relevant employees.
 - Involve lawyers inside and outside the enterprise in building this better defense model. Not only is there is a great deal of law concerning consumer information security and privacy, but also the law in these areas is dynamic and subject to considerable regulatory change. ■