Washington Journal of Law, Technology & Arts

Volume 2 | Issue 2 Article 1

10-24-2005

The FACT Act of 2003: Securing Personal Information in an Age of Identity Theft

Terrance J. Keenan

Constitutional & Regulatory
Cite as: Terrance J. Keenan, *The FACT Act of 2003: Securing Personal Information In an Age of Identity Theft*, 2 Shidler J. L. Com. & Tech. 5 (Oct. 24, 2005), *at* <http://www.lctjournal.washington.edu/Vol2/a005Keenan.html>

THE FACT ACT OF 2003: SECURING PERSONAL INFORMATION IN AN AGE OF IDENTITY THEFT

By Terrance J. Keenan[1]

ABSTRACT

The Fair and Accurate Credit Transactions Act of 2003 ("FACT Act") makes incremental progress toward its goal of improving the protection of consumers and businesses in an age of increasingly sophisticated scams and cons. Congress enacted the FACT Act in order to further address the problems of identity theft, improve resolution of disputes over consumer credit information, enhance accuracy of consumer credit records, further regulate use of credit information, and broaden consumer access to credit information. The FACT Act imposes new business practices on companies that handle personal consumer information by requiring them to share with consumers information about data that has been collected and reported about them, as well as how and when that data is being used. Consumers and businesses may benefit from these changes if some harm has already occurred and, in any case, consumers should find that the accuracy and accessibility of their credit information has improved. However, they will find that prevention of future acts of identity theft was not the principal aim of the FACT Act and that other legislation and initiatives are necessary to adequately address these crimes.

Table of Contents

INTRODUCTION

<1> Incidence of identity theft is on the rise. In 2004, the Federal Trade Commission ("FTC") received 15% more identity theft-related complaints than in the prior year,[2] representing a nearly seven-fold increase since 2000.[3] Indeed, 39% of complaints received in 2004 by Consumer Sentinel, the FTC-maintained consumer complaint database, were related to identity theft.[4] While some of this growth may be attributable to more thorough and accurate reporting by the FTC and other organizations, the increase is nevertheless dramatic. As the incidence of identity theft continues to increase annually, state legislatures and Congress have struggled to provide consumers and businesses with tools to fight the growing problem.

<2> The Fair and Accurate Credit Transactions Act of 2003[5] ("FACT Act") is the latest in a series of federal legislative efforts aimed principally or in part at reducing consumers' vulnerability to identity theft and consumer fraud, and minimizing the harm once the theft or fraud has occurred. The FACT Act provides a variety of concrete tools that should enhance the accuracy and accessibility of consumer credit information and help consumers resolve personal credit issues once an incident has occurred. However, it does not significantly reduce the vulnerability that enables identity thieves to commit crimes in the first place. Even as provisions of the FACT Act are implemented by businesses and utilized by consumers, both groups will demand stronger fraud prevention and law enforcement efforts to stem the tide of growing personal and economic costs. In anticipation of consumer demand and the increasing possibility of liability for harm, businesses should not only adopt the business practices required under the FACT Act but should focus on emerging practices that might further protect against identity theft.

IDENTITY THEFT ON THE RISE

<3> Identity theft is a crime in which someone wrongfully obtains and uses another person's personal information in some way that involves fraud or deception, typically for economic gain.[6] Personal information that is valuable to identity thieves includes Social Security numbers, driver's license or identification card numbers, financial account numbers, credit or debit card numbers, and personal passwords or unique identifiers used to verify identity or gain access to information via telephone or on-

line services.[7] Once identity thieves are in possession of this information, they may use it to perpetrate a wide variety of fraudulent activities. The FTC reported that in 2003 the most common identification theft complaints were related to credit card fraud, followed by phone or utility fraud, bank fraud, employment-related fraud, government document or benefit fraud, and loan fraud.[8]

<4> Although identity theft has occurred in various forms for decades, the speed of technological advancement and widespread use of information technology have provided identity thieves with new, more readily-available sources of personal information. Indeed, the relative ease with which an aspiring identity thief can develop the technological skills necessary to carry out a crime enables even minors to perpetrate crimes of such scope as would have been unthinkable in the recent past. For example, in 2003, the FTC charged a minor with violations of two federal laws when he sent out e-mails that appeared to be sent from the "AOL Billing Center" in order to fraudulently collect personal information which he later used to make various online purchases.[9] This offense is an example of a relatively new phenomenon known as "phishing," which is the act of sending an e-mail falsely claiming to be from an established legitimate enterprise in an attempt to scam the recipient into surrendering private information that will be used for identity theft.[10] Today, phishing is a commonly employed method of collecting personal data. In the U.S. alone, over 57 million adults have been reached by phishing attacks compromising some 122 well-known corporate brands.[11]

<5> In a related phenomenon known as "pharming,"[12] the identity thief takes advantage of vulnerabilities in the domain name system (DNS) server software that directs Internet traffic to servers where websites reside. The DNS server directs traffic by translating commonly used web addresses, which are entered into the web browser by a user, into the IP addresses of the servers where the websites reside (e.g., the address www.ftc.gov is translated into IP address 321.654.0.0). By changing this translation, the identity thief is able to redirect an unsuspecting user to his fraudulent website where he collects the user's personal data in a manner similar to that used in phishing scams. Since the translation from the user-entered web address to the IP address is invisible to the user, she is not aware that the website is fraudulent.

<6> Some aspects of identity theft crimes make them especially difficult to discover and prosecute. Therefore, these crimes present complex challenges for victims, law enforcement

officials, and legislators. For example, victims are rarely aware of the commission of identity theft until long after the crime has occurred, rendering them unable to provide helpful information to law enforcement. Given what can be extremely complex cases, law enforcement officials often lack sufficient resources to perform adequate investigations of individual incidents as well as the training and information necessary to fight crimes across multiple jurisdictions. Furthermore, individual cases of identity theft are typically not significant enough for federal prosecution; indeed, it has been suggested that the lack of prosecution is the key reason why identity theft has become so widespread.[13] Legislators are challenged to enact laws that enable victims and law enforcement officials to fight and recover from identity theft.

DEVELOPMENT OF CONSUMER PROTECTION

<7> Congress first addressed identity theft problems at a time when today's statistics, with nearly 1 in 8 adults in the U.S. having fallen victim to this crime over a recent five year period,[14] would have been unfathomable. However, the swift pace of technological advancement and the adoption of computer technology by businesses and consumers alike have recently outpaced the legal infrastructure intended to provide safeguards against identity theft. The foundation for this legal infrastructure is comprised of a number of laws, foremost among them the Federal Trade Commission Act ("FTC Act").[15]

<8> In 1970, Congress enacted the Fair Credit Reporting Act[16] ("FCRA") in part "to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit . . . in a manner which is fair and equitable to the consumer with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information . . . ."[17] The FCRA imposed a broad range of legal obligations on, and consumer rights of action against, consumer reporting agencies, those who furnish consumer data to the agencies, and those who use data provided by the agencies. Correspondingly, the FCRA provides for damages where legal liability is established, whether for generally or willfully negligent violations.

<9> From the late 1990's through today, Congress has enacted various laws in an effort to quell the rapid growth of identity theft crimes. The Identity Theft and Assumption Deterrence Act,[18] which provided the preeminent federal identity theft statute, was enacted in 1998 to close a loophole in the 1982

federal criminal fraud statute. This earlier statute addressed only the fraudulent creation, possession, use, or transfer of identification documents, and not the theft or criminal use of the underlying personal information. Therefore, the enactment of the Identity Theft Act made it possible to prosecute fraudulent use of personal information whether or not the information was contained in a physical document. This distinction is critical in an age when an estimated 80 percent of corporate assets are digital.[20]

<10> In 1999, Congress passed the Gramm-Leach-Bliley Financial Modernization Act ("GLB Act").[21] The GLB Act articulates the policy that financial institutions—a broadly defined group of businesses under the Act—are duty-bound to respect their customers' privacy and to protect the confidentiality and security of their nonpublic personal information.[22] Nonpublic information includes personally identifiable information provided by a consumer to a financial institution or obtained by the institution by other means, including through a transaction with the consumer.[23] Furthermore, the Act tasks various federal and state agencies with insuring the privacy and confidentiality of consumer information, and protecting consumers against anticipated threats and unauthorized access that could cause them harm or inconvenience. Additionally, the GLB Act makes it a crime to use false, fictitious, or fraudulent statements or representations to obtain customer financial information from a financial institution, or to solicit another individual to do so.[24]

THE FACT ACT OF 2003

<11> In 2003, Congress responded to the dramatic increase in identity theft and consumer fraud by enacting the FACT Act as an amendment to the FCRA. Congress recognized that the protections provided by the 35-year-old statute were not sufficient to address the dramatic increase of fraud and theft of personal information.

<12> Generally, identity theft statutes either provide for prosecution of identity theft offenses or aim to assist victims in repairing their credit histories.[25] The FACT Act emphasizes the latter, by placing additional responsibilities on businesses to cooperate more fully with consumers through enhanced communication and more accurate recordkeeping. It focuses on the legal obligations of consumer reporting agencies, furnishers of consumer data, and users of consumer data, while significantly expanding the rights of consumers. While this enhancement of consumer rights will help to minimize the harm

once an identity theft has occurred, the FACT Act does little to reduce vulnerability to fraud.

Minimization of Harm

<13> Supporters of the FACT Act claim that the law provides consumers with more opportunities to minimize harm to themselves once a risk has been exposed or incident has occurred and to insure that records are more accurate and complete on an on-going basis. Indeed, the real strength of the FACT Act is the increased power it provides to consumers with regard to credit reporting. Congress has taken a pragmatic approach: requiring businesses to provide a greater quantity of accurate information to individual consumers, thereby educating consumers to more effectively monitor and manage their own credit-related affairs. By helping consumers understand what their rights are under the FACT Act, and making interactions with the credit reporting agencies, data furnishers, and data users more efficient and effective, some harm minimization might be achieved.

<14> In the spirit of enhanced communication and accountability to consumers, the FACT Act calls for cooperation between the credit bureaus and the FTC to define and communicate to consumers a statement of their rights in the event that a theft or fraud occurs. The Act calls upon the FTC to prepare a model summary of consumers' rights to remedy the effects of identity theft or fraud.[26] The model summary, published in November 2004, describes consumers' rights with respect to consumer reporting agencies, data furnishers, and data users. Under the FACT Act, the credit reporting agencies are required to provide consumers with this model summary or a substantially similar version.[27]

<15> By requiring enhanced communication and cooperation, these FACT Act provisions substantially affect credit reporting agencies. For example, the FACT Act requires the three largest agencies to provide free credit reports once per year to any consumer, and must provide consumers with a single point of contact to submit his or her request. This service was rolled out across the country between December 1, 2004, and September 1, 2005.[28] It also requires agencies to make consumers' credit scores available, a service for which a fee may be charged. Agencies are prohibited from reporting transactions resulting from an identity theft once the victim has provided a police report or other evidence of fraud or theft.[29]

<16> The FACT Act prohibits furnishers of data from providing

data to credit reporting agencies which they know or have reasonable cause to believe is inaccurate.[30] If incorrect or incomplete information has been furnished to consumer reporting agencies by a data furnisher, the furnisher must notify the agencies of required corrections and provide only accurate and complete information in the future.[31] Additionally, the Act clarifies the duties of data furnishers to respond to disputes initiated by consumers or credit reporting agencies. The Act permits consumers to dispute credit information directly with the furnisher[32] or, as was permitted under prior law, request that credit reporting agencies contact the furnisher to lodge a dispute on her behalf. In either case, a "reasonable" reinvestigation of the information by the furnisher must commence free of charge.[33] If the data furnisher determines that the disputed information is incomplete or inaccurate it is obligated to modify, delete, or permanently block the information for purposes of reporting to consumer reporting agencies.[34]

<17> Users of consumer data must notify a consumer if they have made a decision adverse to the consumer's interests based on information provided by a credit reporting agency,[35] a third party that is not a credit reporting agency,[36] or an affiliate of the data user.[37] For example, denial of credit, insurance, or employment based on credit information may be adverse actions under the statute.[38] Such notification must include the relevant contact information of the reporting agency that furnished the information. Additionally, the FACT Act imposes a number of obligations on consumer data users when alerts for fraud or active military duty have been included in a credit report.[39]

Reduction of Vulnerability

<18> Critics of the FACT Act claim that it does not go far enough to prevent identity theft from occurring in the first place. These critics assert that it mandates security solutions already in place, does not impose sufficient restrictions on businesses, does not impose sufficient penalties against companies that violate the law and report incorrect information,[40] and does not apply new powers to a sufficiently broad group of consumers. For example, a centerpiece of the law—the requirement that credit and debit account numbers are truncated to not more than the last five digits on sales receipts[41] —had been implemented by major credit card processors[42] and many merchants[43] prior to any legislative mandate. Furthermore, the ability of a consumer to place a block on his or her account is

afforded only to active duty military service members serving overseas,[44] a relatively small portion of the population of potential victims.

<19> Critics also point to federal preemption provisions as evidence that Congress is failing to protect consumers fully. Most new federal preemptions relate to identity theft provisions, and consumer and credit score disclosures.[45] In order to enforce national standards on the credit reporting agencies and providers and users of credit information, the FACT Act extends various preemptions that were already effective under the FCRA and imposes new preemptions, thereby reducing (but not eliminating entirely) the states' authority to enact more stringent laws.[46] Critics of preemption argue that the FACT Act prevents states from enforcing stricter laws to protect their citizens. Given that more expansive privacy protections implemented by some leading states have been or may be preempted, such as those provided by California's Financial Information Privacy Act,[47] the critics' arguments may be well-founded.

<20> The FACT Act does impose new responsibilities on businesses, aimed at reducing fraudulent acquisition and use of consumer data. For example, the law required the FTC to devise, in cooperation with various federal agencies, standards for the disposal of consumer report information and records.[48] Although the standards laid out in the FTC's final regulation are sufficiently flexible to accommodate businesses of all sizes and data of varied sensitivity, it is critical that businesses ensure that the disposal practices they adopt are reasonable for each situation in order to avoid liability. This nebulous reasonableness standard will require businesses to be diligent in assessing the sensitivity of the information, the costs and benefits of different disposal methods, and relevant changes in technology over time.

<21> In a positive sign that Congress is responding to criticism from consumers and businesses, the FACT Act was followed by the Identity Theft Penalty Enhancement Act.[49] This 2004 Act, enacted a mere six and a half months after the FACT Act, further amended the 1982 federal criminal fraud statute to establish penalties for the crime of aggravated identity theft. By putting potential identity thieves on notice that more severe penalties may be imposed, Congress is demonstrating that it understands the need to eliminate, rather than simply minimize, the costs of these crimes. If inadequate punishment of identity theft is tantamount to "tacit encouragement" to commit further crimes, as some critics assert and the United States House of Representatives Committee on the Judiciary acknowledges,[50]

then this legislation might serve as a deterrent against future crimes.

MORE LEGISLATIVE ACTION IS NECESSARY

<22> New technological change will continue apace, and efforts to manipulate and use technological developments for fraudulent purposes are bound to move just as quickly. The courts wish for legislators to respond to issues of fraud on consumers and financial institutions through the development of new laws. While the FACT Act provides consumers and businesses with substantially more power to respond in the face of identity theft once it has been committed, legislators must now take action to build upon the FACT Act. Enhancement of consumers' ability to combat identity theft was a primary objective of the Act. Now, Congress must do more to provide consumers and businesses alike with weapons to preempt the damage and prevent fraud from occurring in the first place.

No Claim for "Negligent Enablement"

<23> While new legislative solutions will continue to be advanced, the judiciary has generally rejected victims' tort claims against businesses that are accused of enabling identity thieves. Indeed, the claim of "negligent enablement of an imposter" has been recognized only by the courts of Alabama,[51] while such a tort claim has been soundly rejected in many other states' courts.[52] Most courts have rejected such negligence claims based on the "banker's privilege", a doctrine under which non-customer third parties are owed no duty of care by a bank.[53] Indeed, even where a bank's customer defrauds a third party through the use of the bank's services, the victim can make no claim against the bank because there is no direct relationship between the bank and the victim.[54]

<24> The Alabama Supreme Court's decision in *Patrick v. Union State Bank* held that, where a bank opens an account in a person's name using his identification, the bank owes a duty of reasonable care to that person to ensure that the individual opening the account and presenting the credentials is not an imposter.[55] Although the court found for the plaintiff, it is notable that the majority was comprised only of a plurality of three justices concurring in the opinion and a fourth in the result. A dissenting justice agreed with the defendant that a "special relationship" between the plaintiff and defendant is required to impose liability and, since no such relationship existed, no duty to protect the plaintiff could be imposed. [56]

Furthermore, the dissenting justice claimed that under the plurality's holding in *Patrick* "banks are now required to foresee criminal acts in all banking transactions." The dissent's observation indicates why the reasoning of *Patrick* is likely never to be adopted, and the claim of "negligent enablement of an imposter" may never be accepted, outside of Alabama.

<25> The prevailing judicial view that consumer protection matters should be addressed by legislators rather than by judges is reflected in most courts' unwillingness to recognize a new cause of action in this context. This viewpoint was recently expressed by the South Carolina Supreme Court in *Huggins v. Citibank, N.A.*[57] In its decision addressing the liability of banks in instances of credit card fraud, the court paid deference to the legislative branch when it asserted that "the legislative arena is better equipped to assess and address the impact of . . . fraud on victims and financial institutions alike."[58] The *Huggins* court declined to recognize the tort of negligent enablement of imposter fraud.[59]

Looking Ahead: Early Warning and Prevention

<26> Even before Congress enacted the FACT Act, myriad proposals for supplemental identity theft legislation were waiting in the wings and continue to be considered by Congress.[60] Senator Dianne Feinstein proposed perhaps the most promising among these. The Notification of Risk to Personal Data Act ("NRPD Act"),[61] modeled on California's Security Breach Information Act,[62] attempts to provide victims of identity theft with early warning of a potential crime by requiring government agencies and businesses to notify an owner or licensee of personal information in the event that security of unencrypted data has been compromised.[63] This will serve consumers by enabling them to respond earlier to possible fraudulent activity. Establishment of a national notification standard, especially determination of the particular development or event that will trigger the notification, is a key legislative issue. Also, while critics of such an approach, including the Bush Administration, claim that confidentiality for corporate victims of computer crimes must be guaranteed in order to ensure cooperation with law enforcement,[64] advocates argue that the corporate victims owe a supervening duty of care to protect their digital assets from internal and external security threats.[65] They believe that this duty will be reinforced when a strict notification standard has been enacted.

<27> Furthermore, Congress made explicit in the FACT Act its

desire that businesses use more advanced technology to combat the security weaknesses permitted by our current technological environment. Section 157 of the FACT Act provides that "the Secretary of the Treasury shall conduct a study of the use of biometrics and other similar technologies to reduce the incidence and costs to society of identity theft by providing convincing evidence of who actually performed a given financial transaction."[66] Although it is not clear whether Treasury's study will extend beyond a basic report of how technology is used by business today, this provision is notable because it demonstrates Congress' willingness to involve the federal government in evaluating current and emerging security solutions. Whether such a study is intended to provide the basis for further legislation mandating the use of certain technologies and business practices is not known.

CONCLUSION

<28> The FACT Act aims to reduce vulnerability of consumers to identity theft and consumer fraud, and to minimize the harm once the theft or fraud has occurred. The Act enhances the ability of consumers to resolve personal credit issues once an incident has occurred; however, it does little to reduce consumers' vulnerability to identity theft and fraud. Even as provisions of the FACT Act are implemented by businesses and utilized by consumers, further legislative action is expected. In response to consumer demand and the increasing possibility of liability for harm, businesses should adopt the business practices specifically enumerated in the FACT Act as well as continue to assess other practices that might provide additional consumer protection.

PRACTICE POINTERS

- Ensure that business practices comply with the FACT Act's enumerated requirements that apply to consumer reporting agencies, those who furnish data to the agencies, and those who use data provided by the agencies.
- Adopt reasonable business policies for the disposal of consumer report data based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology.
- Keep all business records containing sensitive information in secure locations to prevent unauthorized disclosure, and shred (preferably with a

cross-cut shredder), pulp, or burn all documents that contain identity information that the business is not required by law or policy to retain.[67]

- Define reasonable operating procedures to assure that information about individuals is maintained and reported with maximum possible accuracy.
- Monitor legislative developments in the identity theft arena, since today's legislators are swift to respond to constituent demands for greater protection even at the expense of legislative effectiveness.[68]
- Watch for trends toward business liability in federal and state court decisions; while there is a clear trend against allowing common law causes of action, Alabama has held a bank liable for "facilitating" an identity thief's commission of a crime.

<< Top

Footnotes

1. Terrance J. Keenan, University of Washington School of Law, Class of 2006. Thank you to Nicole Nyman and Professor Jane Winn for their input and encouragement.
2. Fed. Trade Comm'n, National and State Trends in Fraud and Identity Theft: January – December 2004 4 (2005), *at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf (Oct. 8, 2005).
3. U.S. Dep't of Justice & Can. Solicitor Gen., Public Advisory: Special Report for Consumers on Identity Theft (May 2003), *at* http://www.usdoj.gov/opa/pr/2003/May/publicadvisory1.pdf (last visited Jan. 10, 2005).
4. Fed. Trade Comm'n, *supra* note 2, at 4.
5. Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. §§ 1681a-1681x, 20 U.S.C. §§ 9701-08, 31 U.S.C. § 5318 (2005).
6. U.S. Dep't of Justice & Can. Solicitor Gen., *supra* note 3.
7. The Notification of Risk to Personal Data Act, S. 1350, 108th Cong. § 2(4) (2003).

8. Fed. Trade Comm'n, *supra* note 2, at 4.
9. Press Release, Federal Trade Commission, Identity Thief goes "Phishing" for Consumers' Credit Information (July 21, 2003), *at* http://www.ftc.gov/opa/2003/07/phishing.htm (last visited Jan. 10, 2005).
10. *E.g.*, http://www.webopedia.com/TERM/P/phishing.html (last visited Jan. 10, 2005).
11. *Experts: 'Phishing' More Sophisticated*, Jan. 20, 2005, *at* http://www.cnn.com/2005/TECH/internet/01/20/tech.phishing.reut (last visited Jan. 23, 2005).
12. *E.g.*, http://en.wikipedia.org/wiki/Pharming (last visited May 19, 2005).
13. Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, United States Attorneys' Bulletin, Mar. 2001, at 14, 15, *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usab4902.pdf (last visited Jan. 10, 2005).
14. *FTC: Identity Theft Strikes 1 In 8 Adults*, Oct. 29, 2003, *at* http://www.cnn.com/2003/TECH/ptech/09/04/id.crime/ (last visited Feb. 10, 2005).
15. Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2005).
16. Fair Credit Reporting Act, Pub. L. No. 91-508, tit. 6, 84 Stat. 1114, 1127 (codified as amended at 15 U.S.C. §§ 1681-1681x (2005)).
17. 15 U.S.C. § 1681 (2005).
18. 18 U.S.C. § 1028 (2005).
19. Hoar, *supra* note 13, at 14, 16.
20. *Identity Theft: Hearing Before the Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and Census of the House Comm. on Gov't Reform*, 108th Cong. 4-5 (2004) (statement of Jody R. Westby, Esq., Managing Director, PricewaterhouseCoopers LLP), *available at* 2004 WL 2112321.
21. Gramm-Leach-Bliley Financial Modernization Act, 15 U.S.C. §§ 6701-6910 (2005).

22. 15 U.S.C. § 6801(a) (2005).
23. 15 U.S.C. § 6809(4)(A) (2005).
24. 15 U.S.C. §§ 6821(a)-(b) (2005).
25. Hoar, *supra* note 13, at 14, 16.
26. 15 U.S.C. § 1681g(c)(3) (2005).
27. 15 U.S.C. § 1681g(c)(1) (2005).
28. Fed. Trade Comm'n, FTC Facts for Consumers: Your Access to Free Credit Reports 2 (2004), *at* http://www.ftc.gov/bcp/conline/pubs/credit/freereports.pdf (last visited January 23, 2005).
29. Lawrence A. Young, *The FACT Act: Fair and Accurate Credit Transactions Act of 2003 (H.R. 2622) and Related Developments*, 58 Consumer Fin. L.Q. Rep. 36, 36 (2004).
30. 15 U.S.C. § 1681s-2(a)(1)(A) (2005).
31. 15 U.S.C. § 1681s-2(a)(2) (2005).
32. 15 U.S.C. § 1681s-2(a)(8) (2005).
33. 15 U.S.C. § 1681i(a)(1)(A) (2005) (although reinvestigation of disputes was required prior to enactment of the FACT Act, the reasonableness requirement was added by the Act).
34. 15 U.S.C. § 1681s-2(b)(1)(E) (2005).
35. 15 U.S.C. § 1681m(a) (2005).
36. 15 U.S.C. § 1681m(b)(1) (2005).
37. 15 U.S.C. § 1681m(b)(2) (2005).
38. Michael F. McEneney & Karl F. Kaufmann, *Fair Credit Reporting Act Developments*, 59 Bus. Law. 1215 (2004).
39. 15 U.S.C. § 1681c-1(h) (2005).
40. Young, *supra* note 29, at 37.
41. 15 U.S.C. § 1681c (2005).
42. *Visa The Clear Winner Of Card News' PR And Marketing Awards*, Card News, July 22, 2004, *available at* 2004 WLNR 5238701.
43. Mary Hunt, *A New Federal Law Could Help Protect*

Your Credit, St. Paul Pioneer Press, Mar. 31, 2004, *available at* 2004 WLNR 3535757.

44. 15 U.S.C. § 1681c-1 (2005).

45. Tony Hadley, *The FACT Act of 2003*, *at* http://www.privacyassociation.org/docs/sum04/406Hadley.pdf (last visited Jan. 10, 2005).

46. Young, *supra* note 29, at 37.

47. *See, e.g.*, Cal. Fin. Code § 4053(b)(1) (West 2005) (preempted by American Bankers Ass'n. v. Gould, 412 F.3d 1081 (9th Cir. 2005)).

48. Press Release, Federal Trade Commission, FTC Issues Final Regulation on Consumer Information and Records Disposal (Nov. 18, 2004), *at* http://www.ftc.gov/opa/2004/11/factadisposal.htm (last visited Jan. 10, 2005).

49. Identity Theft Penalty Enhancement Act, 18 U.S.C. §§ 641, 1028-1028A (2005).

50. H.R. Rep. No. 108-528, at 5 (2004).

51. *E.g.*, Patrick v. Union State Bank, 681 So.2d 1364 (Ala. 1996) (holding that "a bank owes a duty of reasonable care to the person in whose name, and upon whose identification, an account is opened to ensure that the person opening the account and to whom checks are given is not an imposter").

52. *E.g.*, Huggins v. Citibank, N.A., 355 S.C. 329 (2003) (holding that South Carolina does not recognize the tort of negligent enablement of imposter fraud).

53. David A. Szwak, *Update on Identity Theft and Negligent Enablement*, 58 Consumer Fin. L.Q. Rep. 66, 70 (2004).

54. *E.g.*, Eisenberg v. Wachovia Bank, N.A., 301 F.3d 220, 227 (4th Cir. 2002).

55. *Patrick*, 681 So.2d at 1371.

56. *Id.* at 1372.

57. 355 S.C. 329 (2003).

58. *Id.* at 334.

59. *Id.*

60. Young, *supra* note 29, at 37.

61. The Notification of Risk to Personal Data Act, S. 1350, 108th Cong. (2003).

62. Cal. Civ. Code § 1798.29 (West 2003).

63. *Identity Theft: Hearing Before the Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and Census of the House Comm. on Gov't Reform*, 108th Cong. 4-5 (2004)
(statement of Jody R. Westby, Esq.,
Managing Director, PricewaterhouseCoopers LLP),
available at 2004 WL 2112321.

64. Young, *supra* note 29, at 37.

65. *Identity Theft: Hearing Before the Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and Census of the House Comm. on Gov't Reform*, 108th Cong. 4-5 (2004)
(statement of Jody R. Westby, Esq.,
Managing Director, PricewaterhouseCoopers LLP),
available at 2004 WL 2112321.

66. 117 Stat. 1952, § 157.

67. Hoar, *supra* note 13, at 14, 21-22.

68. Young, *supra* note 29, at 37.

<< Top