IDENTITY THEFT 2010: CIVIL LIABILITIES AND REGULATORY RED FLAGS

DRI STRICTLY RETAIL SEMINAR
Chicago, Illinois
March 4-5, 2010

William F. Ray
Watkins & Eager, PLLC
400 East Capitol Street
Jackson, Mississippi 39201
Post Office Box 650
Jackson, Mississippi 39205-0650
Telephone: (601) 965-1900
wray@watkinseager.com

Introduction

"Identity theft" is a term that pervades popular culture and the collective consciousness. A Google® search of "identity theft" yields over 50,000,000 results (compared to about 11,000,000 for "Abraham Lincoln," 30,000,000 for "The Beatles," and 200,000 for "credit fraud").

Identity theft is not only part of the vernacular. It is part of everyday life. According to the Federal Trade Commission, as many as 9 million Americans have their identities stolen each year.[1] Other estimates are higher.[2] According to the United States Government Accountability Office (GAO),

> Identity theft occurs when individuals' identifying information is used without authorization in an attempt to commit fraud or other crimes. There are two primary forms of identity theft. First, identity thieves can use financial account identifiers, such as credit card or bank account numbers, to take over an individual's existing accounts to make unauthorized charges or withdraw money. Second, thieves can use identifying data, which can include such things as SSNs and driver's license numbers, to open new financial accounts and incur charges and credit in an individual's name, without that person's knowledge. This second form of identity theft is potentially the most damaging because, among other things, it can take some time before a victim becomes aware of the problem, and it can cause substantial harm to the victim's credit rating.

Personal Information: Data Breaches Are Frequent, But Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, GAO Report to Congressional Requesters, GAO-07-737, p. (June 2007) ("GAO Report" herein; copy provided in Appendix to this paper). GAO

[1] www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

[2] See, e.g., http://www.privacyrights.org/ar/idtheftsurveys.htm

documented and studied numerous large-scale data breaches,[3] including some with notoriety. GAO concluded that data breaches occur frequently, under varying circumstances, and with varying degrees of threat or risk. GAO further concluded that in the great majority of data security breaches, there is no clear evidence of actual identity theft or harm. This conclusion is consistent with inferences taken from case law, and from popular press regarding identity theft – while risks of data breaches are admittedly great, a severe breach does not necessarily lead to severe harm.

Before January 1, 2000, only five reported decisions by U.S. District Courts referred to "identity theft:" since then, over 1,000 such decisions have been rendered (with most in very recent years). Likewise, the first reference to "identity theft" in a published decision by a U.S. Court of Appeals was in 1993, when the Fourth Circuit considered a challenge to Virginia's voter registration laws. Virginia required voters to supply their social security numbers in order to become registered. Virginia further permitted public access to the voter information, including social security numbers. The Fourth Circuit struck the law based on constitutional grounds, because the Virginia rules "compel would-be voters in Virginia to consent to the possibility of a profound invasion of privacy when exercising the fundamental right to vote." In discussing its "privacy" concerns the Fourth Circuit stated as follows (the quote is long but worthwhile):

> Originated in 1936, a SSN is a nine-digit account number assigned by the Secretary of Health and Human Services for the purpose of administering the Social Security laws. *See* 42 U.S.C. § 405(c)(2)(B). SSNs were first intended for use exclusively by the federal government as a means of tracking earnings to determine the amount of Social Security taxes to credit to each worker's account. Over time, however, SSNs were permitted to be used for purposes unrelated to the administration of the Social Security system. For example in 1961, Congress

[3] "Although there is no commonly agreed-upon definition, the term "data breach" generally refers to an organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers." GAO Report at 2.

authorized the Internal Revenue Service to use SSNs as taxpayer identification numbers. Pub.L. No. 87-397, 75 Stat. 828 (codified as amended at 26 U.S.C. §§ 6113, 6676).

In response to growing concerns over the accumulation of massive amounts of personal information, Congress passed the Privacy Act of 1974. This Act makes it unlawful for a governmental agency to deny a right, benefit, or privilege merely because the individual refuses to disclose his SSN. In addition, Section 7 of the Privacy Act further provides that any agency requesting an individual to disclose his SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it." At the time of its enactment, Congress recognized the dangers of widespread use of SSNs as universal identifiers. In its report supporting the adoption of this provision, the Senate Committee stated that the widespread use of SSNs as universal identifiers in the public and private sectors is "one of the most serious manifestations of privacy concerns in the Nation." S.Rep. No. 1183, 93d Cong., 2d Sess., reprinted in 1974 U.S.Code Cong. & Admin. News 6916, 6943. In subsequent decisions, the Supreme Court took notice of the serious threats to privacy interests by the mass accumulation of information in computer data banks. For example, in *Whalen v. Roe*, 429 U.S. 589, 97 S.Ct. 869, 51 L.Ed.2d 64 (1977), in rejecting a privacy challenge to a New York statute that: (1) required doctors to disclose to the state information about prescriptions for certain drugs with a high potential for abuse and (2) provided for the storage of that information in a centralized computerized file, the Court observed:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of all criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.

Id. at 605, 97 S.Ct. at 879 (footnote omitted).

Since the passage of the Privacy Act, an individual's concern over his SSN's confidentiality and misuse has become significantly more compelling. **For example, armed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits or Social Security benefits, order new checks at a new address on that person's checking account, obtain credit cards, or even obtain the**

> **person's paycheck**. Elizabeth Neuffer, Victims Urge Crackdown on Identity Theft, BOSTON GLOBE, July 9, 1991, at 13, 20 (In Massachusetts, "[a]uthorities say that, with another person's Social Security number, a thief can obtain that person's welfare benefits, Social Security benefits, credit cards or even the victim's paycheck."); Michael Quint, Bank Robbers' Latest Weapon: Social Security Numbers, N.Y. Times, September 27, 1992, at 7 (SSN can be used to order new checks at a new address). (FN8) In California, reported cases of fraud involving the use of SSNs have increased from 390 cases in 1988 to over 800 in 1991. Y. Anwar, Thieves Hit Social Security Numbers, San Francisco Chronicle, August 30, 1991, A1, A2. Succinctly stated, the harm that can be inflicted from the disclosure of a SSN to an unscrupulous individual is alarming and potentially financially ruinous. **These are just examples, and our review is by no means exhaustive; we highlight a few to elucidate the egregiousness of the harm. . . .**
>
> **Other uses include unlocking the door to another's financial records, investment portfolios, school records, financial aid records, and medical records.**

Greidinger v. Davis, 988 F.2d 1344, 1352-54 (4th Cir. 1993).

The Fourth Circuit's decision was portentous regarding risks.

Courts, legislatures, regulators, and consumer advocacy groups have advanced the issue of identity theft to the front burner. Increasingly, businesses are expected to pay the economic and social costs of credit-related identity theft crimes. This paper provides a brief overview of legal theories that are used to make retailers and other businesses bear the costs of criminal acts of others. The paper then focuses on the "Red Flags Rule" promulgated by the Federal Trade Commission, and likely effects of that rule.

Fact Example: Missteps and Misappropriation

Guns & Butter, Inc. operates a national chain of boutique stores, specializing in firearms and gourmet dairy products. G&B provides online shopping as well as retail showrooms. G&B provides a "membership" based discount program, and also provides rebates and discounts through its store-branded credit card, which is offered through an arrangement with a major credit card company and bank.

Both online and at the cash register, customers are offered instant, one-time-only discounts in exchange for opening G&B credit card accounts. Customers complete physical or online applications, providing name and address, income, birth date and social security number, drivers license number and expiration date, and phone numbers.

Through its store-branded credit card program, its club membership, and through other sources – all of which involve voluntarily provision to G&B of information by customers – the company has collected detailed information on hundreds of thousands of customers. G&B's marketing department analyzes the information statistically, combined with purchasing and shopping patterns, to ensure that the company provides up-to-date goods and services to its customers.

Ellen Sharp, EVP of market analysis for G&B, has called a summit meeting with all regional marketing officers to discuss trends. Her laptop contains G&B's entire customer data base, with all available information. She routinely works with that information while traveling, and while conducting meetings with other highly placed marketing executives.

Ellen's trip to the summit meeting includes taxis, trains and planes. She arrives at her destination hotel late, and tired. Only when she awakens the next morning does she discover that her G&B-issued laptop – holding over 200,000 detailed customer records – has disappeared from her backpack.[4]

Meanwhile Lenny Lightfingers has had a good day. He has removed three wallets, two cell phones, four MP3 players, and one laptop – Ellen's – from the possession of their rightful owners. Lenny sells the devices to Freddy Fencer, who specializes in electronics.

---

[4] Laptop thefts are a major source of serious data breaches. See, e.g., the discussion at http://en.wikipedia.org/wiki/Laptop_theft which lists several significant data breaches resulting from laptop thefts and losses; see also http://www.consumeraffairs.com/news04/2006/03/laptop_thefts.html listing other significant breaches.

Freddy, in turn, has his own markets. He recognizes Ellen's laptop as an expensive, new, "corporate" model. He knows a buyer for high-end laptops. By the time Ellen discovers her loss, her laptop has been disassembled , the hard drive has been duplicated and destroyed, and the database has been emailed, in several discreet packets, to Eastern Europe. There, the database of Guns & Butter's customers will be split into parcels and sold to counterfeiters, immigration fraud, entrepreneurs and others.[5]

G&B consults counsel, and realizes that it must inform all affected customers of the data breach. The cost of notification is huge, including staffing of telephone hotlines, tracing unreturned mail notices, and legal fees associated with ensuring compliance with almost fifty jurisdictions' rules. While few customers have suffered actual economic losses, many are upset, and some have filed lawsuits, including one class action suit.

One thing leads to another. A month later, a later 6 foot tall blonde woman approaches a cash register at Lots of Big TVs. As she is preparing to purchase a television with a check, the store's employee offers a 10% discount, if the customer opens a store credit card account. The customer readily agrees, presenting her photo ID and other documentation. The new Big Lots of TVs affinity credit card account is opened in the name and personal identifiers of Manuela Diaz Garcia – who is in fact 5 feet tall, brunette, and a continuing victim of identity theft. Within six weeks, Ms. Garcia will receive her first collection call, inquiring why she is late with her monthly credit payment for the TV.

A combination of legal concepts apply. Some of G&B's customers are completely

---

[5] *Cf.* "Feds Charge 11 In Breaches at TJ Maxx, Office Max, DSW, Others," http://www.wired.com/threatlevel/2008/08/11-charged-in-m/ describing international ring of data pirates, including one who allegedly earned over $11 million selling stolen credit cards and magnetic stripe data.

unaffected (or would have been, had they never been notified of the breach). Others, like Ms. Garcia, have been directly victimized and injured. And when the impostor applied for and received credit at a second retailer, the next level of harm, and potential liability, began.

The Developing Law: Concepts of Duty, Liability, and Remedies

Courts, legislatures, regulators and litigators are grappling to apply old concepts to new issues - - or to invent new concepts entirely - - for identity theft cases. Most civil litigation over identity theft has applied old common-law concepts, or new statutory rules. Emerging technologies, concepts of privacy-based rights and duties, and highly-publicized crimes have generated thousands of articles and other publications. These range from ephemeral tweets and blogs, to thorough surveys of developing law, to scholarly works. I commend several excellent articles and sources to the reader who is building a knowledge base regarding civil liability for identity theft. Some of those sources are surveyed below.

Secondary Authorities

American Law Reports recently published a useful and timely annotation regarding civil claims for "future" identity theft. Annotation, *Liability for Risk of Future Identity Theft*, 50 A.L.R. 6th 33 (2009). The ALR annotation collected and discussed twenty-five decisions, focusing on *Ruiz v. Gap, Inc.*, 622 F.Supp.2d 908 (N.D. Cal. 2009), which is now on appeal in the Ninth Circuit and is discussed at some length below. The annotation collects cases "considering whether and under what circumstances there can be liability under state law for future or potential identity theft, where the private information of an individual or individuals has been stolen, left to public view, or otherwise compromised but where, to the knowledge of the parties, there have been no attempts to use the data." *Id.* at 40. This annotation is a thorough and concise collection of recent cases, and

I recommend review of the annotation and its future supplements, and the cases cited therein.

The A.L.R. annotation divides cases into the following categories:

1) Cases concluding that plaintiffs who cannot prove actual disclosure and use of their personal data nonetheless have standing to bring future identity theft cases;[6]

2) Cases concluding that such plaintiffs do not have standing;[7] and

3) Cases concluding that such plaintiffs have no viable claim because they cannot prove they had actual injuries or sustained compensable harm.[8]

These three categories are frequently acknowledged by courts and by scholarly articles, as referenced below.

Robert Sprague and Corey Chiocchietti recently published *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91 (2009) ("Sprague and Chiocchietti") hereinafter. Their article examines current practices in collection and use of personal identifying information, and "one of the greatest threats associated with data collection - unauthorized disclosure due to data breaches." *Id.* at 95. The paper reviews American law of privacy regarding collection of personal information, and current practices by online commercial enterprises. The authors note that common law provides little relief to individuals whose personal information is leaked through data security breaches absent cognizable harm, and that victims of actual identity theft frequently lack remedies against commercial creditors

---

[6]Citing *McLoughlin v. People's United Bank, Inc*., 2009 WL 2843269 (D. Conn. 2009), *Pisciotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir. 2007), and *Caudle v. Towers, Perrin, Forster & Crosby, Inc*., 580 F.Supp. 2d 273 (S.D. N.Y. 2008).

[7]Citing *Giordano v. Wachovia Securities*, LLC, 2006 WL 2177036 (D. N.J. 2006) and *Key v. DSW, Inc*., 454 F.Supp.2d 684 (S.D. N.Y. 2008).

[8]Citing numerous cases including *Ruiz*, *supra*, *Guin v. Brazos Higher Education Services Corp., Inc*., 2006 WL 288483 (D. Minn. 2006) and *Randolph v. ING Life Ins. and Annuity Co.*, 973 A.2d 702 D.C. 2009).

due to absence of a legal duty of care. *Id.* at 102-03. Sprague and Chiochietti review state legislative response to data breaches, noting that almost all states have followed California's example in passing legislation requiring businesses to notify state residents if their personal information has been disclosed through a data breach. *Id.* at 104-05. The authors describe and identify those state enactments, including states that provide encryption safe harbors (i.e., excusing companies from notifying people of breaches if the data is encrypted) and noting "the few states that do provide civil damages against a company that has had a data breach." *Id.* at 105-107, and nn. 67-74.

In 2008, Joseph Lazzarotti published a very helpful survey of federal and state data privacy laws. *Joseph J. Lazzarotti on State Data Privacy and Security Laws*, 2008 *Emerging Issues* 1879 (Matthew Bender 2008, updated through 2010) (available on Lexis). Lazzarotti reviews recent federal legislative efforts (both enacted and defeated), and acknowledges that in many ways state legislatures have made more progress:

> States have been aggressive in their enactments to protect the personal information of their residents. Key components of the "cocktail" approach employed by the states to prevent identity theft include (I) specific protections for Social Security numbers, (ii) notification of unauthorized breaches of personal information, (iii) affirmative obligations to safeguard personal information, and (iv) the proper destruction of records containing personal information that are no longer needed.

Lazzarotti, at n. 23. Lazzarotti then describes, and identifies, various state-law initiatives including 45 state data breach notification laws. Lazzarotti at n. 56 *et seq*. Lazzarotti's article is particularly helpful for companies and practitioners who are developing an understanding of the diverse national landscape of breach notification rules.

Vincent Johnson provided an excellent overview of civil liability of "database possessors" due to security breaches by hackers and thieves. V. Johnson, *Cybersecurity, Identity Theft, and the*

Limits of Tort Liability, 57 S.C.L. Rev.. 255 (Winter 2005).

> Hackers and other data intruders are subject to criminal and civil liability. Victims may sue, sometimes successfully, under a variety of tort theories, including conversion, trespass to chattels, and intrusion upon private affairs, as well as under the civil liability provisions of the federal Computer Fraud and Abuse Act. However, hackers, particularly those located in other countries, may be difficult to identify or subject to jurisdiction. Hackers may also be judgment-proof. A better target for a lawsuit - one easier to locate, more amenable to legal process, and perhaps more solvent - may be the database possessor who failed to prevent or reveal the security breach, rather than the intruder.
>
> Whether, and to what extent, courts can hold a database possessor liable for damages suffered by data subjects as a result of improper data access are questions of huge importance. On one hand, unless the courts impose some form of liability, the persons often in the best position to prevent the losses may have insufficient incentive to exercise care to avoid unnecessary harm. On the other hand, if liability is too readily assessed, it will have the power to bankrupt valuable enterprises because of the often vast numbers of potential plaintiffs and consequent extensive resulting damages. Obviously, courts must strike a balance that adequately protects the interests of individuals without discouraging the use of computer technology or driving important institutions out of existence.

Id. at 259-60. Johnson addresses "three key questions relating to database possessor liability for harm caused by data intruders:" (1) whether database possessors owe a duty to protect personal information from hackers; (2) whether database possessors owe a duty to disclose intrusions or breaches; and (3) how far the liability of a database possessor should extend in cases where the possessor has failed to exercise reasonable care to protect data or to disclose information about intrusion. *Id.* at 261-62. After surveying common-law theories and statute-based duties of care, and various remedies that might be available to individuals whose information is compromised, Johnson ultimately opines that a proper balance could be maintained by requiring businesses to disclose information about security breaches, in exchange for a limitation on liability for such breaches.

> One reasonable option would be to cap the database possessor's exposure to liability at the moment the database possessor reveals the breach to the subject data. Notification could serve as the pivotal factor in shifting further responsibility

> (beyond the damages cap) from the database possessor to the data subject. Once the database possessor provides notice of the security breach, the data subject is in a better position than the database possessor to monitor the risk of harm and to take action against threats to the data subject's credit and personal security.

Id. at 306-07. Johnson further suggests that the cap on damages could limit recovery "to an amount equivalent to the out-of-pocket costs of monitoring security and taking reasonably necessary steps to prevent identity theft and other losses."

Brendan Delany published an excellent student comment regarding liability for identity theft. Comment, *Identity Theft: The Fair Credit Reporting Act and Negligent Enablement of Imposter Fraud*, 54 CATH. U. L. REV. 553 (Winter 2005). Delany reviewed judicial interpretation of the Fair Credit Reporting Act regarding identity theft, and examined common-law negligence claims against creditors and credit bureaus in cases arising from identity theft. Delany's comment focused on *TRW, Inc. v. Andrews,* 534 U.S. 19 (2001) (establishing law regarding statute of limitation under FCRA) and *Smith v. Citibank, N.A.*, 2001 U.S. Dist. LEXIS 25047, 2001 WL 34079057 (W.D. Mo. 10/3/2001) (holding that bank issuer of credit card to identity thief owed no duty of care to non-customer victim in whose name the card account was opened). Delany also analyzed two other cases that have become icons of identity theft tort law: *Polzer v. TRW, Inc.*, 682 N.Y.S.2d 194 (App. Div. 1998) (no cause of action for bank's "facilitating" identity theft in issuing credit cards to imposters, due to lack of duty, in absence of "special relationship"); and *Huggins v. Citibank, N.A.*, 585 S.E.2d 275 (S.C. 2003) (holding South Carolina law did not impose duty on banks that issued credit cards to identity thief, despite lack of due care, because of inadequate relationship between victims and banks).

Finally, a recent article in the Yale Law Journal provides an interesting overview of American and European privacy laws, recent federal and state trends, and the role of federal

preemption. Schwartz, *Preemption and Privacy*, 118 Yale L. J. 902 (2009). The article presents interesting theoretical arguments about the "dual federal-state system for information privacy," and provides some useful discussion of the Fair and Accurate Credit Transaction Act (FACTA).

Common Theories of Liability and Defenses in Identity Theft Cases

Of course, an identity thief's liability to his victim is undisputed. Whether in conversion, fraud, intentional infliction of emotional distress, or other theories, the victim is clearly entitled to recover from the thief. Johnson, at 258-59. But the thief's civil liability is almost never the subject of judicial or legislative[9] attention, and for obvious reasons plaintiffs and their counsel seek recovery against deeper pockets.

Civil lawsuits therefore are almost always directed against banks, credit card issuers, credit reporting agencies, technology service providers, or related vendors. To date, plaintiffs seeking to impose civil liability on businesses for enabling identity theft have repeatedly stumbled over two hurdles: identification of a legal duty owed by each defendant to plaintiff, and damages or compensable harm.

Does a Common-Law Duty exist?

Duty of Reasonable Care/ Negligence Duty: Classic tort principles are repeatedly referenced by courts and commentators in evaluating identity theft claims. The landmark case of *Palsgraf v. Long Island RR Co.*, 162 N.E. 99 (N.Y. 1928) continues to influence negligence law, in defining the limits of duty. As Judge Cardozo wrote in the *Palsgraf* decision, a duty of care is owed only to plaintiffs who are reasonably perceived to be placed at risk by behavior, and who are "within the range of apprehension." For more than eighty years, *Palsgraf* has stood for the principal that

[9]But see 18 U.S.C. 1030(g), providing private right of action by victim whose customer information is obtained from financial institution or card issuer databases, via hacking or otherwise.

defendants are liable only to upon whom harm might reasonably be expected to fall. See e.g. *Restatement of the Law (Second) of Torts*, § 281, "the elements of a cause of action for negligence."

Another area of negligence common law is liability of a negligent person for "allowing" tortious or criminal acts of a third party. At common law, a criminal act was a "superseding cause" which prevented a negligent defendant from being liable to harm caused by the criminal – even when the defendant's negligence was a substantial factor leading to plaintiff's injuries. See *Restatement of Torts (Second)*, § 440. However, limits to that protection have long been recognized, especially where "there was a relationship between the plaintiff and the defendant." Johnson, at 273-74 (citing *Palsgraf* and *Kline v. 1500 Massachusetts Avenue Apt. Corp.*, 439 F.2d 477 (D.C. Cir. 1970) (imposing liability on a landlord for violent criminal acts against tenant).

An "early" identity theft case was *Huggins v. Citibank, N.A.*, 585 S.E.2d 275 (S.C. 2003). Plaintiff's suit against banks that allegedly "negligently issued credit cards" to an identity thief was dismissed based on absence of a duty owed by the banks to a non-customer. Based on black-letter tort law, the court held that "in order for negligence liability to attach, the parties must have a relationship recognized by law as the foundation of a duty of care. . . . The relationship, if any, between credit card issuers and potential victims of identity theft is far too attenuated to rise to a level between them". *Id.* at 277. Johnson analyzes the *Palsgraf*, *Kline*, and *Huggins* decisions as follows:

> Together, *Palsgraf*, *Kline*, and *Huggins* indicate that the strongest cases for imposing a common law duty to guard data from intruders will be those in which there is a business relationship between the defendant database possessors and the plaintiff data subject. This conclusion makes sense on economic as well as doctrinal grounds. Imposing a duty of care in these cases will force the database possessor, who benefits from the use of computerized information, to internalize losses relating to improperly accessed data as a cost of doing business. That duty will in turn create an incentive for database possessors to scrutinize whether their business methods are really worth

> the costs they entail. At the same time, the imposition of a duty in a business context gives the database possessor a means for distributing the loss by adjusting the price of the goods or services it sells to the class of persons that ultimately benefits from the defendant's business methods. That reallocation of losses will help ensure that the costs relating to improperly accessed data will not fall with crushing weight on either the data subject or the database possessor.

Johnson at 275-76.

Voluntary Undertaking of Duty: A common-law duty can certainly arise by way of voluntary undertaking, and assumption of duty. *Restatement of Torts (2nd)*, §§ 323, 324A. For example, a financial institution or creditor's account agreement or internal policies may impose a duty of care upon the institution to protect customer information. *See* Johnson, at 278-279.

Emerging Duty: Data Breach Notification Rules

"Laws requiring data security breach notifications began with California's Senate Bill 1386 [Cal. Civ. Code § 1798.29, 1798.82] in 2002." Schwartz at 917. As stated earlier, at least 45 American jurisdictions have now imposed a statutory duty upon database possessors to disclose breaches of security that expose personal information to outsiders, including hackers. Lazzarotti at n. 56. According to Sprague and Chiocchietti, the only states that had not adopted data breach notification laws by mid-2008 were Alabama, Kentucky, Mississippi, Missouri, New Mexico and South Dakota. Sprague and Chiocchietti at 104, n. 65.

The California Act expressly creates a private cause of action for data breaches. Cal. Civ. Code 1798.84(b). Under state security-breach notification statutes, private rights of action are also available to individuals whose information is disclosed in the states of Utah, Washington, Delaware, New Hampshire, and Louisiana; in other states, the Attorneys General may sue to recover actual damages and/or civil penalties. Lazzarotti at n. 101 *et seq.*; see also Johnson at 284-85 and nn. 193-201. Other state statutes are silent regarding private rights of action, or even imply that no private

right of action is created by the statute. Johnson at 271 (citing Arkansas & Texas statutes as unlikely to support private actions).[10]

While scholars and state legislatures seem to agree that mandatory breach notices are good policy, the GAO Report noted conflicting goals and interests associated with mandatory notifications. While benefits include incentives to improve data security, prevention of identity theft, and improvement of public awareness, there are significant costs associated with notices. A study of companies that experienced data breaches and then notified the subjects indicated that millions of dollars have been spent on individual efforts; notification costs as high as $79 per affected account have been documented. GAO Report at 34. And provision of free credit monitoring services – a standard remedy in the event of data breaches – costs, on average, between $20 and $40 per customer. *Id.* at 35.

Obstacle to Tort Recovery: The Economic-Loss Rule

Under the "economic loss rule" claims for negligence are generally not viable unless defendant's negligence results in "physical damage to the plaintiff's person or property." *See generally* O'Brien, *Limited Recovery Rule as a Dam: Preventing a Flood of Litigation for Negligent Infliction of Pure Economic Loss*, 31 ARIZ. L. REV. 959 (1989); Perry, *The Economic Bias in Tort Law*, U. ILL. L. REV. (2009). Johnson identifies three types of economic damages likely to be experienced in identity theft cases: (1) out-of-pocket expenses incurred to restore a credit rating; (2) personal time spent in repairing one's credit rating; and (3) lost opportunities resulting from bad

[10] Even where state statutes do not provide for private rights of action, common-law duties could also require companies to provide notification of breaches, either under general negligence principals or the law of misrepresentation. Security breach notification laws could, in theory, serve as "negligence *per se* grounds." Johnson at 283, 285-86. Since standard industry custom has long served as an indicator of a defendant's reasonableness, and since the overwhelming majority of jurisdictions have imposed notification requirements on data possessors, it would be unsurprising for courts or juries to reach this conclusion.

credit. "Viewed from the standpoint of public policy, the economic-loss rule serves three very different functions: avoidance of too broad a scope of liability; insistence that damages be proved with certainty; and definition of the doctrinal boundary between contract law and torts." Johnson at 296-99.

Of course, applying the "economic loss rule" does not diminish the importance or impact of identity theft on victims. Indeed, it is has been estimated that identity theft victims take an average of 44 months to resolve their cases, translating into approximately 175 hours spent. Delany at 55 and n. 11. Such losses are hardly trivial. The issue is not severity, but whether negligence law provides a remedy.

Obstacle to Tort Recovery: Lack of Duty to Non-Customer

In *Smith v. Citibank, N.A.*, 2001 WL 34079057 (W.D. Mo. 10/3/01), the court ruled that the card-issuing bank owed no duty to plaintiff, a non-customer. The same result was obtained in *Polzer v. TRW, Inc.*, 682 N.Y.S.2d 194 (App. Civ. 1998) and in *Huggins v. Citibank, N.A.*, 585 S.E.2d 275 (S.C. 2003). Delany criticizes these results, because "a negligent issuer of a credit card" can "better bear the loss incurred as a result of identity theft" than can an innocent customer. Delany at 585. Delany recognizes, however, that such an approach would adopt a "liability beyond the risk" theory of liability. Delany at 586.

Obstacle to Tort (or Other) Recovery: Lack of Compensable Damages

Some plaintiffs' cases have been dismissed, and rightly so, because they simply were not harmed by data breaches. For example, in *Guin v. Brazos Higher Education Services Corp., Inc.*, 2006 U.S. Dist. LEXIS 4846 (D. Minn. 2/2/2006), plaintiff sued a lender that lost a laptop containing plaintiff's personal information. Plaintiff could not present any evidence that his

personal information was actually accessed or used; plaintiff had not experienced any identity theft or other fraud involving his personal information. His negligence claim was therefore dismissed.

"The element of damages has been a particular problem for plaintiffs in" identity theft actions. Lazzarotti, at n. 111, citing *Rowe v. UniCare Life & Health Ins. Co.*, No. 1:09-cv-2286 2010 U.S. Dist. LEXIS 1576 (N.D. Ill. 1/5/2010); *Williams v. Manchester*, 888 N.E.2d 1 (Ill. 2008); *Pisciotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir. 2007), *Bell v. Acxiom Corp.*, 2006 U.S. Dist. LEXIS 72477 (E.D. Ark. 10/3/2006), *Key v. DSW, Inc.*, 454 F.Supp.2d 683 (S.D. Ohio 2006), *Stollenwerk v. Tri-West Healthcare Alliance*, 2005 U.S. Dist. LEXIS 41054 (D. Ariz. 9/6/2006) [*rev'd in part*, 254 Fed.Appx.664 (9th Cir. 2007)], and *Forbes v. Wells Fargo Bank*, 420 F.Supp.2d 1018 (D. Minn. 2006).

There are, of course, cases in which actual damages can be proven, or at least inferred. For example, in *Stollenwerk*, *supra*, two plaintiffs did not claim any actual harm from the data breach. The trial court and the Ninth Circuit rejected plaintiffs' claim for the cost of credit monitoring (in part because of insufficient evidence of exposure to risk, and in part because of evidence that adequate credit monitoring was available free of charge). *Stollenwerk v. Tri-West Healthcare Alliance*, 254 Fed.Appx. at 665. A third plaintiff, however, had experienced actual identity fraud incidents shortly after the data breach. That plaintiff testified that 1) he gave the defendant his personal information; 2) fraudulent accounts were opened in his name six weeks after the breach; 3) he had never before experienced any identity theft; 4) he did not transmit personal information over the internet; 5) he shredded mail that contained personal information; and 6) the only other incident of his losing personal information was a theft of his wallet five years before. The Ninth Circuit concluded that these facts were sufficient to present a jury question regarding whether the

data breach caused his identity theft losses. *Id*. at 667.

These common themes are recognized by courts, and by commentators (who, in scholarly fashion, frequently criticize the rules because they prevent recovery by plaintiffs). Plaintiffs continue to challenge these obstacles to recovery, as shown in recent and currently-pending litigation.

Current High-Profile Cases

The oft-cited cases mentioned above have laid the groundwork for a current generation of significant litigation. The doctrines that protect businesses from liability to uninjured, non-customer plaintiffs are alive and well, but are being tested in the following high-profile cases:

Amburgy v. Express Scripts

In *Amburgy v. Express Scripts, Inc.*, 2009 U.S. Dist. LEXIS 109100, 2009 WL 4067218, (U.S.D.C. E.D. Mo. 11/23/2009) (4:09-CV-705 slip op; docket doc. #53), the plaintiff filed a putative class action alleging the defendant pharmacy company's "inadequate security measures in relation to its computerized database system allowed unauthorized persons to gain access to confidential information of Express Scripts members contained in the database, with such information including names, dates of birth, Social Security numbers, and prescription information." The unauthorized parties then attempted to extort money from Express Scripts by threatening to publicize the confidential information. Plaintiff alleged that in the "extortion letter," the thieves included information about 75 individuals but claimed to have similar information on millions of customers. *Id*. at 1-2. Plaintiff's complaint asserted claims of negligence, breach of contract with respect to third-party beneficiaries, breach of implied contract, violations of "data breach notification laws" of various states, and violations of Missouri's Merchandising Practices Act. Plaintiff alleged

the class members

> have had their Confidential Information compromised, their privacy invaded, have been deprived of the exclusive use and control of their proprietary prescription information, have incurred costs of time and money to consistently monitor their credit card accounts, credit reports, prescription accounts, and other financial information in order to protect their Confidential Information, and have otherwise suffered economic damages.

Id. at 2-3. Plaintiff did not allege that he had personally undergone any out-of-pocket losses.

The court granted defendant's motion to dismiss, ruling as follows on each of defendant's arguments:

1) Lack of Standing: Defendant argued plaintiff lacked Article III standing due to absence of "injury in fact." After canvassing recent law on personal data security breaches, the court acknowledged a trend toward finding that standing exists for plaintiffs with possible future injuries, but declined to follow this "whim." *Id*. at 7. The court concluded that, since plaintiff could not demonstrate any "impending and immediate" harm, rather than "remote, speculative, conjectural, or hypothetical" injury, the likelihood he would be injured did not support a justiciable "case or controversy."[11]

2) Failure to state a claim of negligence: The court found that plaintiff's negligence claim failed because it did not assert any compensable damages, an essential element of a

---

[11] The court stated as follows:

> For plaintiff to suffer the injury and harm he alleges here, many "if's" would have to come to pass. Assuming plaintiff's allegation of security breach to be true, plaintiff alleges that he would be injured "if" his personal information was compromised, and "if" such information was obtained by an unauthorized third party, and "if" his identity was stolen as a result, and "if" the use of his stolen identity caused him harm. These multiple "if's" squarely place plaintiff's claimed injury in the realm of the hypothetical. If a party were allowed to assert such remote and speculative claims to obtain federal court jurisdiction, the Supreme Court's standing doctrine would be meaningless.

Id. at 10-11.

common-law negligence tort. The court also concluded that Missouri's new security breach disclosure act did not support a private cause of action for negligent failure to comply with the act. *Id.* at 13-16.

3) Failure to state a claim of breach of contract: Plaintiff asserted rights as a third-party beneficiary under contracts between Express Scripts and other providers, and also asserted rights under implied contracts. In the motion to dismiss, defendant did not dispute the breach of contracts (the nature of the contracts is unclear from the opinion), and the court found that plaintiff's allegations were sufficient to state a compensable claim – because Missouri law only required assertion of a contract, and its breach, at the pleading stage. *Id.* at 16-17. Nonetheless, the court dismissed the contract claims due to lack of Article III standing, and consequent lack of subject-matter jurisdiction. *Id.* at 17-18.

4) Lack of class representative standing to assert claims under other states' breach disclosure laws: Plaintiff asserted a class right to recover under statutory database breach disclosure laws of California, Delaware, District of Columbia, Hawaii, Illinois, Louisiana, Maryland, North Carolina, Rhode Island, Tennessee, and Washington. The court dismissed those claims because plaintiff, as a Missouri resident, had no personal claims under those statutes and could not represent residents of those jurisdictions regarding such claims. The court therefore did not reach the merits of those claims. *Id.* at 18-20.

5) Missouri Merchandising Practices Act: Finally, the court concluded the MMPA did not apply because plaintiff did not plead a sufficiently "ascertainable loss" associated with a "purchase or lease of merchandise" to meet the statute's requirements.

Cumis v. BJ's

Cumis Insurance Society, Inc. v. BJ's Wholesale Club, Inc., 455 Mass. 458, 918 N.E.2d 36 (Mass. 12/11/2009) is the most recent decision arising from the BJ's Wholesale Club data breach of 2003-04. In February 2004, Visa and MasterCard determined that thieves had gained access to the full magnetic stripe data, including various personal or proprietary data, from transaction records of about 9 million cardholder customers. Fraudulent cards were generated by criminals using the stolen data, and those cards were used to make purchases. After discovery of the breach, and investigation by authorities, the retailer was accused of failing to encrypt customer information, storing information too long and in easily accessible files, and otherwise failing to protect customer information.[12] This most recent court decision involves claims by credit unions that issued the compromised cards, and by their insurer, Cumis, which reimbursed some of the losses. Plaintiffs relied in part on agreements between BJ's and card-issuer banks, which allegedly required BJ's to treat the data with more caution.

> It was ultimately determined that the third-party transaction processing software used by BJ's was permanently storing the magnetic stripe data in transaction logs. The agreements between BJ's and Fifth Third contained a requirement that BJ's comply with Visa and MasterCard's regulations, including those prohibiting BJ's from storing any magnetic stripe data after a transaction was completed; the agreements among Fifth Third and Visa and MasterCard required Fifth Third to ensure that its merchants complied with the regulations. BJ's conceded that it was retaining the magnetic stripe data.

918 N.E. 2d at 42. Plaintiffs claimed they could recover as intended third-party beneficiaries for the alleged breach of contract. Plaintiffs also asserted claims based on fraud, negligence, negligent misrepresentation, and other claims. *Id.* at 40.

---

[12]See FTC Complaint against BJ's Wholesale Club, Inc., http://www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf, and FTC announcement of settlement with BJ's, http://www.ftc.gov/opa/2005/06/bjswholesale.shtm.

Trial judges dismissed the third-party contract claims based on express language excluding such claims, dismissed the negligence claims based on the economic loss doctrine, and dismissed fraud and negligent misrepresentation claims for lack of sufficient proof. On appeal, the Supreme Judicial Court of Massachusetts addressed these claims as follows:

1) Third-party contract beneficiaries: The court relied on express language in the Visa and MasterCard contracts, which disclaimed any intent to benefit third-party beneficiaries and excluded third parties from the right to enforce the agreements. The court rejected parol evidence and plaintiffs' argument that the contractual regulations were intended to benefit all participants in the transactions, giving precedence to the contracts' express language. *Id* at 45-46.

2) Negligence claims: The court relied on Massachusetts law that rejects tort claims for purely "economic loss." *Id.* at 46 ("the economic loss doctrine bars recovery unless the plaintiffs can establish that the injuries they suffered due to the defendants' negligence involved physical harm or property damage, and not solely economic loss."). Plaintiffs attempted to skirt the economic loss doctrine by arguing that "physical harm" indeed occurred, "because the plastic credit cards are tangible personal property and their damages included physical harm to the plastic cards that had to be canceled following the thefts." The court readily rejected that argument, stating that "the question here is not whether the credit cards are tangible property, but rather the nature of the damages sought by the plaintiffs" (that is, the cost of replacing and reissuing cards were also economic losses, not property damage). *Id.*[13]

[13] In support of this analysis, the court cited another case arising from the same data breaches, *Pennsylvania State Employees Credit Union v. Fifth Third Bank, 398 F. Supp. 2d 317, 330 (M.D. Pa. 2005)*, aff'd in part, *Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162, 176-178 (3d Cir. 2008)*. The *Sovereign Bank* case involved claims by a card-issuing bank against BJ's and Fifth Third Bank, which handled card transactions for BJ's. The Ninth Circuit reversed summary judgment in favor of Fifth Third, finding a genuine issue of fact regarding "whether Visa intended to give Sovereign the benefit of Fifth Third's promise to Visa to ensure BJ's compliance

3) Fraud and negligent misrepresentation claims: Plaintiffs' fraud claims were based on assertions that defendants "falsely represented that [they] would comply with the Card Operating Regulations," thus inducing the credit unions both to act as issuers and also to fail to take "additional steps to protect themselves." Plaintiffs' negligent misrepresentation claims[14] were based on allegations that some defendants "falsely represented" that BJ's was not storing magnetic stripe information. *Id.* at 47. But after discovery was completed, there was no evidence of direct representations by defendants to plaintiffs, and no evidence of reliance by plaintiffs on the underlying agreements containing the "representations" (for that matter, plaintiffs had not seen the agreements prior to the litigation). *Id* at 48. Plaintiffs also presented no evidence that they would have "acted differently with respect to their participation in the Visa and MasterCard organizations had they been aware of the defendants' breach of their contractual obligations to abide by the operating regulations." *Id*. at 49. Dismissal of the fraud and misrepresentation claims was affirmed for several reasons: lack of direct representation of some facts to plaintiffs; lack of reliance by plaintiffs; inability to base misrepresentation claims on breach of contractual promises absent lack of intent to perform when the promise is made; and lack of reasonableness of any supposed reliance, in light of plaintiffs' knowledge of circumstances.[15] *Id.* The summary judgments in favor of BJ's and others were affirmed.

---

with the provisions of the Visa-Fifth Third Member Agreement." *Id.* at 173. The Ninth Circuit affirmed dismissal of negligence claims, relying on the economic loss doctrine. *Id*. at 177-78.

[14]Unlike other negligence claims, the economic loss doctrine did not bar recovery for negligent misrepresentation under controlling law. *Id*. at 48.

[15]For example, the court noted that plaintiffs had actual notice of unrelated alerts from Visa and MasterCard about instances of improper storage of magnetic data. but plaintiffs did not take any action in response.

TJX v. Card Issuers

In Re TJX Companies Retail Security Breach Litigation/ Amerifirst Bank v. TJX Companies, Inc., 564 F.3d 489 (1st Cir. 2009) involved similar facts and claims to the *BJ's* case. In January 2007, TJX Companies, Inc., a major operator of discount stores, disclosed that its computer systems had been hacked and credit or debit card data for millions of customers had been stolen. "Harm resulted not only to customers but, it appears, also to banks that had issued the cards ("issuing banks"), which were forced to reimburse customers for fraudulent use of the cards and incurred other expenses." *Id*. at 491. As in the *Cumis v. BJ's* case discussed above, card issuers sued the retailer and the processing bank and relied on breaches of Visa and MasterCard rules as well as third-party beneficiary theories.

> AmeriFirst's complaint, seeking class action status for issuing banks, charged that both TJX and Fifth Third were variously at fault: that TJX and Fifth Third failed to follow security protocols prescribed by Visa and MasterCard to safeguard personal and financial information; that the breaches occurred from July 2005 onward but were discovered and disclosed only later; and that the issuing banks suffered losses from reimbursing customers for fraud losses, monitoring customers accounts, and cancelling and reissuing cards.

Id. at 492.

> The complaint alleged that Fifth Third has contracts with MasterCard and Visa that require compliance with operating regulations adopted by each credit card organization and that TJX and Fifth Third similarly have a contract that requires TJX to comply with such regulations. It further alleged that TJX and Fifth Third ignored security measures required by the operating regulations--for examples, that signatories deploy a firewall configuration, protect stored data, encrypt transmission of cardholder data, and track access to cardholder data and network resources.
>
> But although TJX and Fifth Third are charged in the complaint with misrepresentations, the plaintiffs' claim--as elaborated in their district court filings and brief on appeal--appears to rest (with one doubtful exception as to Fifth Third) on a flimsier foundation than actual misrepresentation. Rather, plaintiffs argue that by accepting credit cards and processing payment authorizations, defendants impliedly represented that they would comply with MasterCard and Visa regulations

and this was the negligent misrepresentation.

Id. at 494. The district court (without the benefit of the *Cumis* decision discussed above) declined to dismiss the negligent misrepresentation claim on a 12(b)(6) motion, and the First Circuit (also without the final *Cumis* decision) likewise left that claim alive – "but on life support" – because of the idea that some sort of "conduct" might have sufficed as a "representation." *Id*. at 495. The First Circuit stated that

> It would almost surely stretch Massachusetts law too far [**11] to say that merely doing credit card transactions with issuing banks, whether directly (Fifth Third) or indirectly (TJX), is a representation implied by conduct to third parties that the defendants were complying with detailed security specifications of Visa and MasterCard. The implication is implausible and converts the cause of action into liability for negligence – without the limitations otherwise applicable to negligence claims.

Id. at 494. The First Circuit also rejected the issuer banks' negligence[16] and third-party beneficiary contract claims, on the same grounds as discussed in *Cumis v. BJ's*. *Id*. at 498-99. Finally, the First Circuit affirmed the district court's denial of a late motion to amend plaintiffs' complaint to add a claim for conversion; the court briefly expressed mild skepticism about the merits of that claim. *Id*. at 500.

Ruiz v. Gap

Presently pending in the U.S. Court of Appeals for the Ninth Circuit is *Joel Ruiz v. Gap, Inc. and Vangent, Inc*., Case No. 09-15971. Plaintiff had applied for a job with retailer Gap, Inc. Vangent is a vendor that processes Gap job applications. On September 17, 2007, a thief broke into

[16]In attempting to avoid the economic loss doctrine, plaintiffs in the *TJX* case urged that the economic loss doctrine did not apply "because it had a property interest in the payment card information, which the security breach rendered worthless." The First Circuit rejected that argument as insufficient to meet the "physical destruction of property" requirement under Massachusetts law, just as the state court rejected the "loss of property" claim on the credit and debit cards themselves in the *Cumis* decision.

Vangent's offices in Chicago and stole two laptop computers. At the time, one of the laptops was downloading information about Gap job applicants; a Vangent employee planned to use the information to prepare a report about Gap hiring trends. At the time it was stolen, the laptop contained unencrypted private information, including Social Security numbers, of about 750,000 Gap applicants. *Ruiz v. Gap, Inc.*, 622 F.Supp.2d 908, 50 A.L.R. 6th 579, 582 (N.D. Cal. 2009).

Eleven days later, Gap sent a notification letter to the applicants whose information was on the computer, informing them of the breach and offering to provide them with twelve months credit monitoring, with fraud assistance, at no cost. Gap advised the recipients, including Ruiz, "to notify their banks and sign up for a free credit report from one of the three major credit reporting agencies."

Ruiz sued Gap in a putative class action, asserting theories of negligence, bailment, violation of California Business and Professions Code § 17200, et seq.; violation of the California constitutional right to privacy; and violation of California Civil Code §1798.85 (which requires "Confidentiality of Social Security Numbers"). The district court dismissed all of those claims except those resting in negligence and §1798.85, on the pleadings. *Ruiz v. Gap, Inc.*, 540 F.Supp.2d 1121 (N.D.Cal.2008). Plaintiff amended his complaint to add Vangent as a defendant, and to add a claim for breach of contract. The Court ultimately granted summary judgment and dismissed the case in its entirety.

First, the district court addressed Ruiz's Article III standing to bring the claims, recognizing the "irreducible constitutional minimum" requirement of injury in fact. The court then surveyed recent judicial analyses of standing in cases involving lost data. The court's discussion of those cases merits this lengthy quote:

> Some courts have held that plaintiffs in "lost-data" cases have not suffered an injury-in-fact sufficient to confer Article III standing. *See Randolph v. ING Life Ins.*

and Annuity Co., 486 F.Supp.2d 1, 6-8 (D.D.C.2007) (no standing where laptop computer stolen during burglary and plaintiffs pled increased risk of identity theft); *Bell v. Acxiom Corp*., No. 06-0485, 2006 WL 2850042, at *1-2 (E.D.Ark. Oct. 3, 2006) (class action dismissed for lack of standing where hacker downloaded information and sold it to marketing company); *Key v. DSW, Inc*., 454 F.Supp.2d 684, 690 (S.D.Ohio 2006) (class action dismissed for lack of standing where unauthorized persons obtained access to information of approximately 96,000 customers); *Giordano v. Wachovia Sec. LLC*, No. 06-476, 2006 WL 2177036, at *4 (D.N.J. July 31, 2006) (credit monitoring costs resulting from lost financial information did not constitute injury sufficient to give plaintiff standing).

However, the only circuit court to consider the question of standing in a lost-data case determined that the plaintiff did have standing to assert negligence and contract claims. *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir.2007). Old National Bancorp ("ONB") operated a marketing website where individuals seeking banking services could complete online applications. *Id.* at 631. The applications requested names, addresses, social security numbers, driver's license numbers, date of birth, mother's maiden name, and other information. *Id.* A third-party hacker obtained access to the information of tens of thousands of applicants. Id. The scope and manner of access suggested the intrusion was "sophisticated, intentional and malicious." *Id.* at 632. After ONB sent written notice to those affected, plaintiffs filed a putative class action asserting negligence and breach of contract claims and requesting compensation for credit monitoring services. Id. The Seventh Circuit held that plaintiffs had standing because "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions." *Id.* at 634.

Relying on *Pisciotta*, the District Court for the Southern District of New York determined that plaintiffs had standing in a lost-data case. *Caudle v. Towers, Perrin, Forster & Crosby, Inc*., 580 F.Supp.2d 273, 280 (S.D.N.Y.2008). In *Caudle*, an employee was notified that several laptop computers had been stolen, one of which contained the employee's personal information, including his social security number. *Id.* at 276. Although the Second Circuit has not decided whether the standing requirement can be satisfied by an increased future risk of identity theft, the Second Circuit has decided that standing exists where there is an increased future risk of harm based on exposure to environmental toxins or potentially unsafe food products. *See Baur v. Veneman,* 352 F.3d 625, 634 (2d Cir.2003); *LaFleur v. Whitman*, 300 F.3d 256, 270 (2d Cir.2002). Against this backdrop, the court determined the plaintiff alleged an adequate injury-in-fact for standing purposes. *Caudle*, 580 F.Supp.2d at 280.

Ruiz, 50 A.L.R. 6th at 584. Based on Ruiz's alleged increase in risk theft, and on the reasoning in

Pisciotta and *Caudle*, the district court ruled that Ruiz had constitutional "injury in fact" standing to assert the claims. *Id*. at 585.

The district court then addressed the merits of Ruiz's negligence claim. Plaintiff alleged that due to defendants' lack of due care, he and the plaintiff class had "been injured and harmed since Defendants' compromising of their [personal information] has placed them at an increased risk of identity theft." *Id*. at 585-56. Ruiz also alleged the plaintiff class had suffered damages, because they "have spent and will continue to spend time and/or money in the future to protect themselves as a result of Defendants' conduct." *Id*. at 585-86.

The district court observed that under California law, "appreciable, nonspeculative, present harm is an essential element of a negligence cause of action," and "the breach of a duty causing only speculative harm or the threat of future harm does not normally suffice to create a cause of action for negligence." *Id*. at 586. The district court then ruled that Ruiz's "risk of future identity theft" was inadequate under California law to satisfy the damages element of a negligence claim, stating that "While Ruiz has standing to sue based on his increased risk of future identity theft, this risk does not rise to the level of appreciable harm necessary to assert a negligence claim under California law." *Ruiz*, 50 A.L.R. 6th at 586.

The court distinguished toxic chemical exposure cases, in which the need for medical monitoring is deemed sufficient to satisfy the "harm" prong of a negligence claim, on three grounds. First, Ruiz presented no authority treating lost-data cases as analogous to medical monitoring cases. Second, Ruiz did not present sufficient evidence establishing a "significant exposure" of his personal

information, comparable to the burden in medical monitoring cases.[17] And third, Ruiz's failure to take advantage of Gap's offer of free credit monitoring for one year cast doubt on the contention that he would in fact incur such future costs. *Id*. at 587.

The district court cited other cases rejecting the mere release of personal information as sufficient to support a negligence claim. In *Pisciotta*, cited above, the Seventh Circuit held that naked allegations of increased risk of future identity theft were insufficient to support a negligence claim. 499 F.3d at 635-39. In *Caudle*, also cited above, the district court rejected a negligence claim absent actual evidence that plaintiff's data had been accessed and used as a result of the theft. The court in *Ruiz* continued:

> In *Melancon v. Louisiana Office of Student Financial Assistance*, the court noted that "the mere possibility that personal information may be at increased risk does not constitute actual injury sufficient to maintain a claim for negligence." 567 F.Supp.2d 873, 877 (E.D.La.2008). In *Kahle v. Litton Loan Servicing LP*, computer equipment was stolen that contained the personal information of 229,501 former customers of Provident bank. 486 F.Supp.2d 705, 706 (S.D.Ohio 2007). The court found that "without direct evidence that the information was accessed or specific evidence of identity fraud this Court can not find the cost of obtaining ... credit monitoring to amount to damages in a negligence claim." Id. at 713.
>
> In *Forbes v. Wells Fargo Bank, N.A.*, computers were stolen from a vendor of Wells Fargo Bank that contained unencrypted customer information. 420 F.Supp.2d 1018, 1019 (D.Minn.2006). The court granted summary judgment against the plaintiffs on their negligence claim because their expenditure of time and money monitoring their credit did not establish the essential element of damages. Id. at 1020-21. In *Guin v. Brazos Higher Education Service Corp.*, a laptop computer was stolen that contained unencrypted, nonpublic customer information. No. 05-668, 2006 WL 288483, at *1 (D.Minn. Feb. 7, 2006). The court held that the plaintiff could not sustain a claim for negligence because he had experienced no instance of identity theft. Id. at *6.

---

[17]The court cited an unpublished Ninth Circuit decision, *Stollenwerk v. Tri-West Health Care Alliance*, 254 Fed.Appx. 664, 665-67 (9th Cir.2007) as additional support. The court in *Stollenwerk* rejected a negligence claim in plaintiff's suit arising from theft of a laptop containing plaintiff's personal information; the Ninth Circuit rejected an argument based on the "medical monitoring" analogy because plaintiff could not provide analogous threshold proof comparable to significant toxic exposure required for medical monitoring under the law of Arizona, and other states.

Ruiz, 50 A.L.R. 6th at 587-88. The district court thus granted summary judgment on Ruiz's claims of negligence.

The court then turned to Ruiz's claims under California Civil Code §1798.85. The court determined that no technical breach of the statute had occurred (because the Social Security number was not required in order to "access any website"). Therefore, the court did not reach the question whether the statute created a private right of action. *Id.* at 590.

Finally, Ruiz alleged that he and other putative class members were third-party beneficiaries of an Employment Screening Services Agreement between Gap and Vangent. The agreement was allegedly breached by Vangent's failure to "employ commercially reasonable efforts to preserve the security and confidentiality of personal data under its control, and by failing to encrypt the data." *Id.* But once again, Ruiz's inability to show actual harm was fatal to the claim:

> Under California law, a breach of contract claim requires a showing of appreciable and actual damage. *See St. Paul Fire and Marine Ins. Co. v. American Dynasty Surplus Lines Ins*., 101 Cal.App.4th 1038, 1060, 124 Cal.Rptr.2d 818 (2d Dist.2002) ("An essential element of a claim for breach of contract are damages resulting from the breach.") (italics omitted); *Patent Scaffolding Co. v. William Simpson Const. Co.*, 256 Cal.App.2d 506, 511, 64 Cal.Rptr. 187 (2d Dist.1967) ("A breach of contract without damage is not actionable."). Because Ruiz has not been a victim of identity theft, he can present no evidence of appreciable and actual damage as a result of the theft of the two laptop computers.

Ruiz, 50 A.L.R. 6th at 590-91. The court dismissed the claims for third-party beneficiary contract breaches.

The district court's opinion in *Ruiz* was thorough and thoughtful. As stated above, Ruiz has appealed the case. Briefing is complete, and the case is set for oral argument before the Ninth Circuit on April 12, 2010. In his 62-page opening brief (copy provided in appendix to this paper), Ruiz attacks every aspect of the trial court's decision, arguing that he in fact demonstrated actual

injuries, and advocating for recognition of rights to recover under the California Constitution and statutes as well as common law. Gap and Vangent's 63-page appeal brief (provided in appendix) asserts that no instances of actual identity theft occurred as a result of the breach, whether to Ruiz or anyone else, and otherwise supports the district court's legal analysis.

Appellees are supported by a prospective *amicus curiae* brief submitted by the Chamber of Commerce of the United States and by the Retail Industry Leaders Association (RILA). The public policy and importance of the issue is nicely presented in their motion for leave to participate as *amici* which merits quoting at length:

> RILA is the world's leading alliance of retailers, and of those who provide products and services to retailers. The Association represents many of the largest retailers in California and throughout the United States. Worldwide, RILA's members collectively account for more than $1.5 trillion in annual sales, provide millions of jobs, and operate over 100,000 stores, manufacturing facilities, and distribution centers both domestically and globally. In addition to other services that it offers to its members, RILA represents its members' interests through advocacy with various arms of the government and through the filing of briefs in judicial proceedings.
>
> The Chamber and RILA have tens of thousands of members who, as businesses, routinely obtain electronic personal information of customers, employees, potential employees, and others. Members of the retail and business communities receive such electronic personal information for any number of reasons, aimed at increasing the efficiency and quality of their businesses and improving the experience of the customers they serve. These wholly legitimate purposes include screening job applicants (as occurred in this case); administering various human resources programs for employees; processing payment or shipping information from customers; running customer loyalty programs; and analyzing demographic trends involving marketing, consumers, products, and services. Without such information, most businesses would likely find it impossible to function in today's complex commercial world, which is increasingly dependent on electronic commerce and transactions.
>
> The members of the Chamber and RILA take seriously their responsibility to safeguard personal identifying information. Unfortunately, a stark reality of today's business world is the existence of criminals who target businesses and their property, including valuable equipment like computers and valuable information like

> personal identification data. Despite the best efforts of retailers and businesses to protect their property and their data, sometimes the thieves succeed.
>
> According to the arguments made by Mr. Ruiz, and properly rejected by the District Court, each and every one of these criminal acts places retailers and businesses at risk of automatic liability. Good corporate citizens can find themselves facing the burden of baseless litigation along with the risk of adverse jury verdicts, founded on the mere speculative fear that someone might misuse stolen personal information.
>
> . . .
>
> The brief proposed by the Chamber and RILA makes two points. First, the brief argues that plaintiffs such as Mr. Ruiz in essence seek to hold companies strictly liable for data breaches, and that as a result companies will provide no more notice than the existing notification laws clearly require. This is a risk because the individuals in the class that Mr. Ruiz seeks to lead reside in states that have the varied notice requirements. In fact, dozens of jurisdictions require notice to be given only when there is a reasonable likelihood that harm will result from a data breach. Holding companies strictly liable for data breaches would therefore give companies a disincentive to provide notice to individuals when the law does not require such notice. This point is not discussed in detail by the parties, and so will substantially assist this Court in deciding this case. The brief also includes a table of statutory language listing the jurisdictions that require notice only when there is a reasonably likelihood that harm will result from a data breach. Second, the brief argues that the fear of future data theft is so speculative that the current law of negligence in California and elsewhere does not recognize it as an actionable injury. It points out that a holding by this Court recognizing such a fear as an actionable injury would mark a fundamental change in the law of negligence.

Ruiz v. Gap, Inc., Motion of Chamber of Commerce of the United States and Retail Industry Leaders Association for Leave to File Brief *Amicus Curiae* in Support of Defendants-Appellees, docket entry # 30-2, Case 09-15971 in the U.S. Court of Appeals for the Ninth Circuit (11/16/2009) (provided in appendix).

***Hannaford Bros*.**

The *Hannaford Bros*. litigation also bears watching. Plaintiffs, customers of the grocery chain, allege that

> beginning December 7, 2007, third-party "wrongdoers obtained access to

> [Hannaford's] information technology systems and, until containment of this security breach on or about March 10, 2008, stole private and confidential debit card and credit card information, including up to an estimated 4.2 million debit card and credit card numbers, expiration dates, security codes, PIN numbers and other information belonging to [the] [p]laintiffs and other customers . . . who had used debit cards and credit cards to transact purchases at supermarkets owned or operated by [Hannaford]." The plaintiffs do not claim that wrongdoers acquired customer names from Hannaford. They say that credit card association Visa, Inc. notified Hannaford on February 27, 2008, that Hannaford's information technology system had been breached, and that Hannaford discovered the means of access on March 8, 2008, contained it and notified certain financial institutions on March 10, 2008, but made no public disclosure until March 17, 2008, and even then, made an inadequate disclosure.

In re Hannaford Bros. Co. Customer Data Security Breach Litigation, MDL Docket No. 2:08-MD-1954, 613 F. Supp. 2d 108, 116 (D. Me. 2009).

> There was no identity theft as such, but as a result of the data theft, a number of plaintiffs in this case initially suffered fraudulent and unauthorized charges to their credit card accounts or bank accounts. These plaintiffs spent time and effort identifying the fraudulent charges. They also expended time and effort convincing their banks and credit card companies that the charges were fraudulent and that the fraudulent and unauthorized charges should be reversed. All such charges were eventually reversed. Ultimately, no plaintiff had to pay the fraudulent charges, and none of the named plaintiffs claims specific expenses incurred to remove the fraudulent charges. The plaintiffs have not placed a monetary value upon the time and effort that they spent dealing with credit companies or banks regarding the reversal of the fraudulent charges to their accounts.

In re Hannaford Bros. Co. Customer Data Security Breach Litigation, MDL Docket No. 2:08-MD-1954, 2009 U.S. Dist. LEXIS 110091, *10 (D. Maine 11/24/2009).

After considerable litigation, on November 24, 2009 the MDL court certified key questions of law to the Supreme Judicial Court of Maine. The certified questions invoke the economic loss doctrine discussed in so many other cases. The questions of law certified by the MDL court are stated as follows:

> 1. In the absence of physical harm or economic loss or identity theft, do time and effort alone, spent in a reasonable effort to avoid or remediate reasonably foreseeable

harm, constitute a cognizable injury for which damages may be recovered under Maine law of negligence and/or implied contract?

> 2. If the answer to question # 1 is yes under a negligence claim and no under an implied contract claim, can a plaintiff suing for negligence recover damages under Maine law for purely economic harm absent personal injury, physical harm to property, or misrepresentation?

Id. at *14.

As stated above, these cases deserve close attention as the defenses available to retailers, creditors, and other data possessors continue to be attacked.

The Federal Trade Commission's Red Flags Rule

Against the backdrop of public interest in identity theft, large scale data breaches, and increasing litigation and legal analysis, the Federal Trade Commission's Red Flags Rule was developed and adopted. The legislative history and statutory basis of the Red Flags Rule begins with the Equal Credit Opportunity Act, 15 U.S.C. § 1691 *et seq*. The Equal Credit Opportunity Act defines "creditor" as "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit." 15 U.S.C. § 1691a(e). In 2003, Congress passed the Fair and Accurate Credit Transaction Act ("FACTA"), Pub. L. 108-159 (the Act is provided in the appendix to this paper.) FACTA famously regulated printed credit card receipts, requiring "truncation" of account numbers and deletion of expiration dates from receipts. Since FACTA provided for recovery of statutory damages and attorney fees for plaintiffs whose receipts were not truncated, a cottage industry of "truncation" class action suits quickly developed.

The legislative purposes of FACTA include "to prevent identity theft . . . ." H. R. Rep. No.

108-396, at 65-66 (2003) (House Conference Report). FACTA includes a mandate that the FTC, together with regulators of bank and credit unions, establish guidelines and prescribe regulations regarding identity theft, including identification of possible risks. Specifically, FACTA requires the FTC to

> (A) establish and maintain guidelines for use by each financial institution and each creditor regarding identity theft with respect to account holders at, or customers of, such entities, and update such guidelines as often as necessary;
>
> (B) prescribe regulations requiring each financial institution and each creditor to establish reasonable policies and procedures for implementing the guidelines established pursuant to subparagraph (A), to identify possible risks to account holders or customers or to the safety and soundness of the institution or customers . . .

15 U.S.C. § 1681m(e)(1), "Red Flag guidelines and regulations required."

The agencies are required to "identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft." *Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule*, 72 Fed. Reg. No. 217 (11/9/2007) p. 63719.[18]

From mid-2006 through November 2007, the agencies considered public comments to the regulations, and adjusted the proposed regulations in response to comments from consumers, financial institutions, and others. *Id.* at 63719. The regulations became final, but have never yet entered the enforcement stage. Meanwhile, FTC has published considerable information in an effort to inform the public and businesses about the Rule, and about FTC's interpretations.[19]

---

[18]The entire final rule, along with supplementary information published in the Federal Register, is provided in the appendix to this paper.

[19]For example, the FTC has published "Fighting Fraud with the Red Flags Rule: A How-to Guide for Business;" a copy is provided in the appendix to this paper. In that document, the FTC provides plain-language interpretation of the Rule, and advice for complying. It is noteworthy that in that document, the FTC defines

Basics of the Red Flags Rule

FACTA incorporated by reference the definition of "creditor" in Equal Credit Opportunity Act, *supra*. The Red Flags Rule covers financial institutions and "creditors" that offer or maintain "covered accounts."

> A covered account is (1) an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft.

72 Fed. Reg. at 63719.

Creditors covered under the Red Flags Rule must establish and maintain "Identity Theft Prevention Programs" to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or with any existing covered account. The Program must be tailored to the creditor's size, and to the complexity and nature of its business.

Before delving into the details of the FTC's final Red Flags Rule, a business should first determine whether it is a "creditor," and whether it offers or maintains "covered accounts." Clearly, if a retailer regularly offers store-branded credit cards, and "arranges" for customers to apply for and obtain those cards, the retailer will be considered a "creditor" by the FTC.

The next question is whether a business entity offers or maintains "covered accounts" within the scope of the Red Flags Rule. A "covered account" is defined in 16 CFR 681.2(b)(3), and reaches virtually all consumer accounts that permit "multiple payments or transactions."

Details of the Red Flags Rule

For purposes of the Red Flags Rule, "identity theft" means "**a fraud committed or**

"creditor" to include "retailers that offer financing or help consumers get financing from others, say, by processing credit applications." *Id.* at 10. Fortunately, the FTC further states that "simply accepting credit cards as a form of payment does not make you a 'creditor' under the Red Flags Rule."

attempted using the identifying information of another person without authority." 16 CFR 681.2(b)(8), incorporating 16 CFR 603.2(a). "Identifying information" means "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person . . . ." "Identifying information" can include the person's name, social security number, birthdate, driver's license or government identification card number, passport number, taxpayer identification number, fingerprint, voice, retina or iris image, telecommunication identifying information, etc. "Thus, under the FTC's regulation, the creation of a fictitious identity using any single piece of information belonging to a real person falls within the definition of 'identity theft' because such a fraud involves 'using the identifying information of another person without authority.'" 72 Fed. Reg. at 63723.

Establishment of an Identity Theft Prevention Program

The fundamental requirement of the Red Flags Rule is establishment of an identity theft prevention program. The elements of an Identity Theft Prevention Program must include reasonable policies and procedures to:

(1) Identify relevant Red Flags[20];

(2) Detect Red Flags;

(3) Respond appropriately to any Red Flags that are detected; and

(4) Ensure that the program is updated periodically.

16 CFR 681.2(d), "Establishment of an Identity Theft Prevention Program."

[20]The regulation defines "Red Flag" as "a pattern, practice or specific activity that indicates the possible existence of identity theft." 16 CFR 681.2(b)(9).

Administration of an Identity Theft Prevention Program

"Administration of the program" is regulated under 16 CFR 681.2(e). The FTC requires a high-level review and approval process for a creditor's Identity Theft Prevention Program. Under 16 CFR 681.2(e), the following measures are mandated:

(1) the company must obtain approval of its initial Identity Theft Prevention Program from either the company's board of directors, or an appropriate committee of the board of directors.

(2) the company must involve its board of directors, an appropriate committee of the board, or a designated employee at the level of senior management "any oversight, development, implementation and administration of" the company's Identity Theft Prevention Program.

(3) every covered creditor must "train staff, as necessary, to effectively implement the" Identity Theft Prevention Program.

(4) every covered creditor must "exercise appropriate and effective oversight of service provider arrangements."

Regulatory Guidelines

The FTC and the other "Red Flags Agencies" promulgated "Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation," 72 Fed. Reg. at 63773. Each creditor that implements an Identity Theft Prevention Program "must consider the guidelines . . . and include in its Program those guidelines that are appropriate." 16 CFR 681.2(f).

Guidelines on Identifying Relevant Red Flags: The regulatory guidelines state that creditors "should consider particular factors in identifying relevant Red Flags. Those factors include the types

of accounts offered, the methods provided to open accounts, the methods provided to access accounts, and the company's previous experiences with identity theft." According to the Guidelines, a company's Identity Theft Prevention Program should "incorporate" relevant Red Flags from sources "such as" prior incidents of identity theft experienced by the creditor, "methods of identity theft" that reflect changes in risks, and "applicable supervisory guidance."

Categories of Red Flags: The Guidelines describe specific "categories" of Red Flags, and state that a creditor's Identity Theft Prevention Program should include "relevant Red Flags" from the categories:

(1) alerts or notifications from reporting agencies, service providers, fraud detection services, etc.;

(2) "the presentation of suspicious documents";

(3) "the presentation of suspicious personal identifying information such as a suspicious address change":

(4) the unusual use of, or other suspicious activity related to, a covered account; and

(5) notice from customers, victims, law enforcement, or others regarding possible identity theft in connection with the company's covered accounts.

Detecting Red Flags: The Guidelines state that a creditor's Identity Theft Prevention Program should address the "detection of Red Flags" in connection with opening accounts, and with existing accounts, "such as by" obtaining sufficient identifying information and verification of a person, and authenticating customers, monitoring transactions, and verifying the validity of change of address requests.

Preventing and Mitigating Identity Theft: The Guidelines state that an Identity Theft

Prevention Program "should provide for appropriate responses to Red Flags." The Guidelines list examples of Red Flag situations, and responses, including monitoring an account; contacting the customer; changing passwords; changing account numbers; declining to open or closing an account; refraining from collection efforts, or sale of a covered account subject to a Red Flag detection; or notifying law enforcement.

The Guidelines also (thankfully) note that "determining that no response is warranted under the particular circumstances" may be an appropriate response.

Updating the Program: According to the Guidelines, program updates should "reflect changes in risks" from identity theft, based on factors such as experiences with identity theft, changes in methods of identity theft, and in detection methods; changes in the types of accounts that the creditor offers or maintains; and changes in business arrangements of the creditor such as mergers, alliances, and service provider arrangements. 72 Fed. Reg. at 63773.

Methods for Administering the Identity Theft Prevention Program: As stated above, the FTC mandates involvement by the board of directors or a board committee in approving the initial Program. The Guidelines describe specific activities that should be included in ongoing administration, including assignment of responsibility, review of reports, high-level approval of material changes, and oversight of service provider arrangements.

Guidelines Supplement: 26 Examples of Red Flags

The FTC promulgated detailed examples of "Red Flags" as a supplement to the Red Flag Rules Guidelines. 72 Fed. Reg. at 63774. Those examples are divided into five categories: (1) alerts, notifications or warnings from a consumer reporting agency; (2) suspicious documents; (3) suspicious personal identifying information; (4) unusual use of or suspicious activity related to, the

covered account; and (5) notice from customers, victims, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

The 26 examples are included in the Federal Register pages provided in the appendix to this paper. Caution is warranted regarding these examples. It would be tempting to "drag and drop "many of those examples directly into a company's mandated Identity Theft Prevention Program – in order to demonstrate to the FTC that the company is serious about complying. However, with respect to the 26 examples and to any other aspect of a written program, companies should proceed with caution.

As described in this paper, and in the articles previously cited, courts have been slow to impose a duty of care in favor of some identity theft victims. Furthermore, industry standards have sufficed, for the most part, to establish the standard of care in dealing with personal information and with people who use credit accounts.

The Red Flags Rule will force businesses to commit in writing concerns, concepts, and proposals for dealing with an ever-changing landscape. A company's mandated Identity Theft Prevention Program will likely be the first document requested by plaintiff's counsel in an "identity theft" civil lawsuit. Creditors and their counsel must therefore be thoughtful and pragmatic in their initial drafting and revision of Programs. Otherwise, companies may incorporate "Red Flags" and responsive policies that do not fit their business models or abilities, only to be skewered with those policies when a criminal defrauds the company – unpredictably, and uncontrollably.

ABA v. FTC, and Thoughts on the Current State of the Red Flags Rule

In August 2009, the American Bar Association sued the FTC, seeking a declaratory judgment and injunction related to the Red Flags Rule. During the two years since the FTC had finalized the

Red Flags Rule, the agency had voluntarily delayed the date on which enforcement would begin. During that period, the FTC published numerous articles, aids, and publications notifying the public of the rules, and providing information about FTC interpretation. The Red Flags Rule was originally scheduled to take effect on January 1, 2008, with a mandatory compliance date of November 1, 2008. But the commission cited "confusion by entities as to whether they were subject to the Rule." *American Bar Association v. FTC*, 2009 U.S. Dist. LEXIS 111407 (D. D.C. 12/1/2009).

On April 30, 2009, the FTC published a document entitled "FTC Extended Enforcement Policy: Identity Theft Red Flags Rule, 16 CFR 681.1." ABA at *11. In that document, the FTC stated its belief that attorneys and other professionals "who bill their clients after services are rendered" are subject to the Red Flags Rule. *Id.* at * 12. In a detailed opinion, the U.S. District Court for the District of Columbia ruled that the FTC's extension of the Red Flags Rule to attorneys was unreasonable, was inconsistent with the enabling legislation, and was erroneous. The court based its decision on several fundamental conclusions. First, FACTA's regulation of "financial institutions and creditors" and focus on "identity theft with respect to account holders or customers" indicated, according to the court, that FACTA was "created to apply to entities involved in banking, lending, or financial related business." *Id.* at * 26. Second, FACTA's references to "account holders" and "customers" and its amendment to the Equal Credit Opportunity Act did not indicate a congressional intent to regulate the legal profession. *Id.* at * 27. Third, the statutory definition of "creditor" did not apply to mere delayed billing by attorneys. A final judgment was entered on December 28, 2009, enjoining FTC from enforcing the Red Flags Rule against practicing attorneys. Under F.R.A.P. 4(a)(1)(B) the FTC has sixty days in which to appeal, i.e. until February 26, 2010.

The FTC has now extended its deferral of enforcement of the Red Flags Rule again, this time

until June 1, 2010. According to the FTC, this delay is "at the request of several members of Congress." See FTC Extended Enforcement Policy: Identity Theft Red Flags Rule, provided in appendix to this paper.

Until the FTC begins enforcement of the Red Flags Rule, it is impossible to predict, with any certainty, the ultimate scope of the regulations. Certainly, the FTC has indicated it will attempt to give the Red Flags Rule the broadest conceivable application (see discussion of American Bar Association litigation, below). Therefore, retailers who take any action in assisting customers who establish or maintain credit accounts – from "house accounts" to indirect-lending bank loans, to store-branded credit card accounts – must be advised to comply with the Red Flags Rule by June 1, 2010. In light of the ABA lawsuit and congressional action, and in light of the FTC's continuing delay, we cannot know - - even at this late juncture - - exactly when, how, and in what form the Red Flags Rule will eventually be enforced. Nonetheless, until further notice creditors, including retailers as discussed above, must be prepared to comply.

Conclusion

Case law, state statutes, and federal legislation are proceeding frenetically in an effort to adjust to the new types of harm that can be inflicted – or threatened – by way of modern technology. Some of this attention may be misdirected; a candid observer might conclude that the level of attention to "identity theft" exceeds its true social impact. At present, the courts are generally refraining from precipitous changes in the law. Legislatures, Congress, and regulators may feel a more immediate need to respond to public concerns. The burdens on businesses of data breaches have been heavy, but generally manageable, in civil litigation. But the burdens of breach notification laws, or of Red Flags Rule compliance, are likely to be much heavier. Businesses,

including retailers who possess large volumes of personal information about their customers and employees, will be well served to dedicate resources to data security and – when necessary – determined defenses designed to preserve established and sound legal doctrines.

William F. Ray
Watkins & Eager PLLC
Jackson, Mississippi
www.watkinseager.com

Appendix of Supplemental Materials