OHIO'S "AGGRESSIVE" ATTACK ON MEDICAL IDENTITY THEFT

STANLEY C. BALL[*]

I. INTRODUCTION

We all think we are the foremost authority when it comes to our personal health. We are consciously selective in what we tell our doctors, we confidently use WedMD.com to self-diagnose illnesses, and we even think we are savvy enough to

[*] Cleveland-Marshall College of Law, '11. I would like to thank Dr. Luther J. Blackwell, Jr. But for your guidance, I would have spent the next thirty years pushing papers around a cubical in the basement of some human resources company. I would also like to thank Professor Carolyn Broering-Jacobs. I cannot thank you enough for the kindness and support that you have shown me throughout my legal education.

make the medical determination of whether we should receive a flu shot each fall. We feel assured knowing that no one knows or can alter our medical identity without our consent or at least our knowledge. But what if someone can?

In 2009, Brandon Sharp, a 37-year-old manager at an oil and gas company in Houston, Texas,[1] was creating his version of the American dream. He was about to get married, buy his first home, and was in perfect physical condition.[2] Before applying for a mortgage, Mr. Sharp requested a copy of his credit report.[3] Much to his chagrin, his credit report revealed several collection notices under his name for emergency room visits throughout the country and a $19,000 bill for a life flight service.[4]

Mr. Sharp, like an increasing number of Americans, had fallen victim to a crime known as medical identity theft. The crime, defined as the theft or unauthorized use of another's personal information to obtain medical goods and services,[5] is dangerous because it alters the victim's medical identity without the victim's knowledge and may never be detected.[6] Additionally, because there is no national centralized repository for medical records, every time a thief uses the victim's medical identity, a record is created that could be easily mistaken for the victim's medical record.[7]

This note explains the severity of medical identity theft and the state and federal legislative reactions to the problem. Specifically, the note discusses data breach notification statutes that require healthcare providers to notify consumers when the systems holding customer personal information are breached.[8] The note concludes that Ohio's data breach notification statute, which does not expressly cover healthcare providers,[9] should be amended to protect residents from medical identity theft and provide redress when healthcare providers[10] violate state law.

---

[1] Walecia Konrad, *Medical Problems Could Include Identity Theft*, N.Y. TIMES, June 13, 2009, at B1, *available at* http://www.nytimes.com/2009/06/13/health/13patient.html.

[2] *Id.*

[3] *Id*.

[4] *Id.*

[5] Pat Curry, *How to Prevent and Cure Medical ID Theft*, CREDITCARDS.COM (Dec. 29, 2008), http://www.creditcards.com/credit-card-news/how-to-prevent-medical-id-identity-theft-1282.php.

[6] *Id.* Generally a victim will never know he is a victim of medical identity theft, unless he receives notice of an unpaid medical bill for treatment he has never received. *See id.*

[7] *See id.*

[8] *See* Sasha Romanosky et. Al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, CARNEGIE MELLON UNIV., at 1 (May 2008), http://www.heinz.cmu.edu/research/241full.pdf.

[9] OHIO REV. CODE ANN. § 1349.19(F)(2) (LexisNexis 2010). *See also* Department of Health and Human Services General Administrative Requirements, 45 C.F.R. § 160.103 (2010).

[10] For purposes of this note, the term "healthcare providers" will be used interchangeably with the term "HIPAA Covered Entities."

Section II of this note describes the nationwide problem of medical identity theft. It begins with an overview of data breach and general identity theft. The section then explains the difference between general identity theft and medical identity theft, and why the latter is more harmful to the victim.

Section III illustrates the federal legislative response to data breaches in the healthcare industry. The section also explains how all healthcare providers are subject to the requirements of the Health Insurance Portability and Accountability Act of 1996 (hereinafter "HIPAA"). The section explains the Act's 2009 amendments, known as the Health Information Technology for Economic and Clinical Act. Lastly, the third section illustrates the interaction between state and federal law, and how federal legislation allows for state regulations regarding data breaches.

Section IV provides an overview of the current Ohio law on data breach notification. The section articulates how and when the Ohio law applies. And most importantly, it explains that Ohio's data breach notification statute does not apply to healthcare providers.

Lastly, Section V provides several suggestions that will ensure Ohio is better able to protect its residents from medical identity theft through an amended data breach notification statute. Specifically, the section offers four proposals: (1) Ohio should make its data breach laws applicable to healthcare providers; (2) healthcare providers doing business in Ohio should not have any discretion when it comes to notifying patients when their data systems have been breached; (3) Ohio's data breach legislation should require healthcare providers to destroy patient's personal information when they dispose of it; and (4) Ohio's legislation should provide a mechanism for victims of medical identity theft to have access to monetary penalties from healthcare providers who violate the amended state law.

While it is undisputed that medical identity theft is a fast growing and fairly complex crime, there is no justifiable reason why Ohio should punt its ability to protect Ohio residents from medical identity theft to the federal government. As this note dictates, there are several concerns that favor and disfavor state laws that address consumer protection from medical identity theft. After weighing these concerns, however, the state legislature should be a driving force rather than a complacent participant in the fight against medical identity theft.

II. DATA BREACH, IDENTITY THEFT, AND MEDICAL IDENTITY THEFT

There are three actions that involve the unauthorized acquisition or misuse of an individual's personal information that may harm an individual. The first is the breach of an organization's information storage system containing consumer data. The second is identity theft. The third is a more severe form of identity theft known as medical identity theft. This section distinguishes the three actions and further explains the severe effects of medical identity theft.

A. Data Breach

The heart of data breach is personal information. In general terms, personal information is any data that identifies a particular person.[11] Organizations collect

[11] *See* Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91, 93 (2009). This includes social security numbers, mothers' maiden names, employment addresses, home addresses, and other personally identifiable information. *See id.*

this personal information because it creates an efficient way to provide goods and services.[12] At the same time, this collection creates a prime target for identity thieves.[13]

The unauthorized acquisition of, or access to, records containing an individual's personal information constitutes a security breach. [14] Often times, data breaches result in unauthorized access to only a small number of records. For example, in 2008, a 38-year-old Avon Lake, Ohio man spent a measly $115 for a spyware program that enabled him to view details of medical procedures, diagnostic notes, and other confidential information of 62 hospital patients.[15] Data breaches can also result in access to an enormous amount of personal information. For example, a laptop containing the social security numbers of approximately 2,000 current and former school employees from Springfield City Schools in Ohio was stolen from a state auditor's car, which was parked in his home garage.[16]

Just as data breaches can occur in numerous sizes, they also occur in several forms. For instance, hackers can use the Internet illegally to retrieve information stored in computer systems.[17] Individuals can also physically steal computers, data storage equipment, and paper files.[18] Additionally, personal information can be improperly displayed or thrown away, allowing sensitive data to be viewed by those who should not have access.[19] And finally, a disgruntled or opportunistic employee may also be the source of data breach.[20]

---

[12] *See id.* at 95.

[13] *See id.* Since 2005, over 345 million records containing personal information have been involved in security breaches in the United States. *See Chronology of Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/data-breach (last updated Sept. 6, 2010).

[14] *See* Neal G. Walters, *Into the Breach: Security Breaches and Identity Theft*, AARP PUB. POLICY INST. (July 2006), http://www.aarp.org/technology/privacy-security/info-2006/dd142_security_breach.html.

[15] *See* Robert McMillan, *Misdirected Spyware Infects Ohio Hospital*, PCWORLD (Sept. 17, 2009), http://www.pcworld.com/businesscenter/article/172185/misdirected_spyware_infects_ohio_hospital.html. The spyware gave the man access to the information when the person he sent the software to opened it on a hospital computer. *See id.* "He was also able to obtain e-mail and financial records of four…hospital employees." *Id*.

[16] *See* Andrew McGinn, *Laptop with City School Employees' Information Stolen*, SPRINGFIELD NEWS-SUN (Mar. 16, 2007), http://www.springfieldnewssun.com/hp/content/oh/story/news/local/2007/03/16/sns031707laptop.html.

[17] *See* Walters, *supra* note 14.

[18] *Id*.

[19] *See id*. [F]or example, printing Social Security numbers on address labels, inadvertently making sensitive personal information accessible on Internet sites that can be viewed by the general public, or not properly disposing of files containing sensitive personal information." *Id.*

[20] *See* Jonathan J. Darrow & Stephen D. Lichtenstein, *"Do You Really Need My Social Security Number?" Data Collection Practices in the Digital Age*, 10 N.C. J. L. & TECH. 1, 15-16 (2008).

When a data breach occurs, it can be costly to the individual whose information has been compromised, as well as to the company that had its data system breached.[21] The individual may have to monitor his credit for years, if not a lifetime.[22] The organization, in many cases, must bear the cost of notifying the individuals whose information has been stolen. When a publically traded company is involved, there is a significant, negative effect on the company's stock price.[23] The company may also be liable for damages if a customer brings a successful civil action based on common law principles or violations of federal and state data breach notification statutes.[24] Even if the suit is unsuccessful, the litigation cost alone can be an unexpected and substantial expenditure. Overall, a data breach's effect can be considerable, but in many cases it is just the tip of the iceberg.

B. Identity Theft

While data breaches pose a serious threat to the privacy of personal information, most people fear what happens after a data breach has occurred. A data breach exposes personal information that is lawfully used by many organizations to open new accounts, verify information, and make changes to existing accounts. Identity theft occurs when an individual uses another person's identifying information, without permission, to commit fraud or other crimes.[25]

An identity thief uses the personal information in a variety of ways. He may open a new credit card account in the victim's name or change the billing address on a victim's account, while accumulating charges[26] on the credit line.[27] Identity thieves

---

[21] Joseph J. Lazzarotti, *Emerging Technology and Employee Privacy: Symposium: The Emergence of State Data Privacy and Security Laws Affecting Employers*, 25 HOFSTRA LAB. & EMP. L.J. 483, 485 (2008). The average laptop contains data worth $972,000 and according to a Federal Bureau of Investigation Computer Crime Survey, the average annual cost of computer security incidents in the U.S. is $67.2 billion. *Id*.

[22] Chad Pinson, *New Legal Frontier: Mass Information Loss and Security Breach*, 11 SMU SCI. & TECH. L. REV. 27, 31-32 (2007).

[23] *See* Sasha Romanosky et. al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, CARNEGIE MELLON UNIV., at 4 (May 2008), http://www.heinz.cmu.edu/research/241full.pdf.

[24] *See* Pinson, *supra* note 22, at 37. "[I]ndividuals whose information has been compromised have sought legal redress against organizations from which their information was taken using a variety of statutory and common law theories." *Id*. at 32. "These cases may prove to be the leading edge in an effort to set new standards for the care and safeguarding of personal information." *Id.*

[25] *See About Identity Theft*, FTC, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html, (last visited Jan. 21, 2010). "The [Federal Trade Commission] estimates that as many as 9 million Americans have their identities stolen each year." *Id*.

[26] *See id.* "While fraudulent charges on a victim's credit card are the most common form of financial fraud, such charges are easily removed from a victim's bill." Robert Lemos, *Stolen Lives*, YOURSECURITYSOURCE.COM (Aug. 26, 2009), http://www.robertlemos.com/journalism/2009/08/index.html (follow "Symantec's YourSecurityResource" hyperlink).

[27] *See* FTC, *supra* note 25.

may also create counterfeit checks using the victim's name and account number, or take out a loan in the victim's name.[28] An identity thief may even get a driver's license or official ID card in the victim's name with the thief's picture on it.[29] In 2009 alone, the number of identity theft victims in the United States increased 12 percent from the previous year to 11.1 million people.[30] In 2008, the Federal Trade Commission reported that 8,237 Ohioans were identity theft victims.[31]

The number of identity theft victims is increasing because committing the crime is relatively simple, while catching and prosecuting identity thieves is extremely difficult.[32] The difficulty begins with discovering whether the crime has even occurred. In many cases, "the victim may not realize that her identity has been stolen until months or years after the fact."[33] This delay between the crime's commission and its discovery makes it nearly impossible for law enforcement to find the criminal.[34] Even though identity theft causes the victim financial harm, the victim in most cases is able to rectify the event by working with creditors and credit monitoring agencies.[35] On average, the victim is made whole after twenty-one hours of working with law enforcement and creditors to clean up the effects of identity theft.[36] While the effects of identity theft are inconvenient for the victim, the

---

[28] *Id*.

[29] *Id*. Children's identities are increasingly at risk. *See* Lemos, *supra* note 26. Criminals prefer using children "because parents are less likely to monitor their children's financial information." *Id.*

[30] *See Javelin Study Finds Identity Fraud Reached New High in 2009, but Consumers Are Fighting Back*, PR NEWSWIRE (Feb. 10, 2010), http://www.prnewswire.com/news-releases/javelin-study-finds-identity-fraud-reached-new-high-in-2009-but-consumers-are-fighting-back-83987287.html. Javelin Strategy & Research and leading companies in financial services and identity fraud prevention technology and resolution produced this comprehensive identity fraud survey. *See id.* "The survey is the nation's longest-running study of identity fraud, with more than 29,000 U.S. respondents over the past seven years." *Id.*

[31] *See* Letter from Richard Cordray, Ohio Attorney General, to Ted Strickland et al., Governor et al. (Nov. 1, 2009), *2009 Identity Theft Annual Report*, at 1, *available at* http://www.ohioattorneygeneral.gov/getattachment/dc78834d-4df5-4a91-b180-291f07f5efde/2009-Identity-Theft-PASSPORT-Program-Report.aspx. This is up 20 percent from the two previous years. *See id.* It places Ohio in the middle of the pack of all states in the number of annual identity theft incidents. *See id.*

[32] *See* Darrow & Lichtenstein, *supra* note 20, at 25.

[33] *Id*.

[34] *See id*. It is estimated that over 90% of identity thieves are never caught or convicted. *See id.*

[35] *See* PR NEWSWIRE, *supra* note 30. Generally it takes a consumer around 21 hours or over half a workweek to straighten out creditors when their identity has been stolen. *See id.*

[36] *See* Tiffany Hsu, *Identity Fraud on the Rise – Up 12% to 11.1 Million Adults Affected in 2009*, LOS ANGELES TIMES (Feb. 10, 2010), http://latimesblogs.latimes.com/money_co/2010/02/identity-fraud-on-the-rise-up-12-to-111-million-adults-affected-in-2009.html. The twenty-one hours represents the individual hours it will take a person to clean up the effects of having his identity stolen. *See id.* It does not mean twenty-one hours in the sense of within twenty-one hours after discovering the theft, the victim's information will be cleared. *See id*. In addition to the twenty-one hours it takes to

financial industry and law enforcement have become increasingly effective at assisting consumers to correct instances of identity theft.[37] There is, however, an area of identity theft where the victim's complete recovery is not as simple or even guaranteed.

C. Medical Identity Theft

While identity theft receives a great deal of media coverage, few realize that there are separate and distinct forms of the crime. Every year, three percent of all identity theft victims, or approximately 330,000[38] people, fall victim to medical identity theft.[39] "Medical identity theft refers to the misuse[40] of an individual's personally identifiable information"[41] "such as a name, date of birth, social security number, or insurance policy number to obtain or bill for medical services or medical goods."[42] An alarming example of medical identity theft is the situation that occurred to Anndorie Sachs.[43] A hospital notified Sachs that her newborn baby "tested

---

clear up a case of identity theft, the victim, on average, will spend $373 in out-of-pocket expenses, unreimbursed losses, legal fees, and time taken off work. *See id.*

[37] *See* PR NEWSWIRE, *supra* note 30. In 2009, it was estimated that the time it takes to correct the effects of identity theft decreased 30% from the previous year. Hsu, *supra* note 36.

[38] Based on the 2009 estimate of 11.1 million identity theft victims. *See* PR NEWSWIRE, *supra* note 30.

[39] Synovate, *Federal Trade Commission-2006 Identity Theft Survey Report*, 21 (Nov. 2007), http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

[40] Booz Allen Hamilton, *Medical Identity Theft Environmental Scan*, 4 (Oct. 15, 2008), http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_850701_0_0_18/HHS%20ONC%20MedID%20Theft_EnvScan_101008_Final%20COVER%20NOTE.pdf.

Id. at 5. For example, a consensual misuse is when a family member uses another family member's health information to get a drug prescription. *See id.* The term "misuse" includes both consensual and nonconsensual forms of medical identity theft. *See id.* This article only focuses on nonconsensual misuse of medical information because the information is obtained through data breaches, which by definition are nonconsensual. *See id.*

[41] Personally identifiable information is "any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual." OFFICE OF MGMT. & BUDGET, EXEC OFFICE OF THE PRESIDENT, OMB M-06-19, REPORTING INCIDENTS INVOLVING PERSONALLY IDENTIFIABLE INFORMATION AND INCORPORATING THE COSTS FOR SECURITY IN AGENT INFORMATION TECHNOLOGY INVESTMENTS (2006), *available at* http://www.whitehouse.gov/OMB/memornada/fy2006/m06-19.pdf (reporting incidents involving personally identifiable information and incorporating the cost for security in agency information technology investments).

[42] Hamilton, *supra* note 40, at 1.

[43] *See* Caitlin A. Johnson, *Protect Against Medical ID Theft, Medical ID Theft Nearly Ruined a Good Mother's Life* (Oct. 9, 2006), http://www.cbsnews.com/stories/2006/10/09/earlyshow/living/ConsumerWatch/main2073225.shtml.

positive for illegal drugs."[44] Sachs was surprised by the call because she had not recently given birth to any children.[45] The situation worsened the following day. Law enforcement officers threatened to take her actual four children away because of the positive drug test.[46] Only after Sachs worked with the hospital and law enforcement officers was it discovered that someone had stolen her driver's license and went to the hospital to give birth under her name.[47]

This example is by no means the only way the crime is perpetrated. Medical identity theft occurs in many ways and each way potentially exposes the victim to the risk of having inaccurate information stored in his or her medical records.[48] Below are four common examples of how the crime is perpetrated:

- "A person uses…the identity of another…to obtain medical care because the [person] is uninsured."[49]
- "A [person] uses the identity of another to obtain medical care because the [person] does not want [his] health records to include information about his . . . health status." Specifically, the identity thief desires to prevent his current or future employer, or "insurance provider from knowing aspects of [his] true health condition."[50]
- A person uses the victim's identity to obtain a drug prescription for recreational use or criminal distribution.[51]
- A person obtains the victim's health information. Then in a separate incident, the thief also steals the personal indentifying information needed to pose as a physician and submits claims for reimbursement to an insurance provider for services never rendered to any individual.[52] This is not uncommon and can "involve hundreds of identities and the submission of millions of dollars' worth of false claims."[53]

---

[44] *Id*.

[45] *See id.*

[46] *Id*.

[47] *Id.*

[48] Hamilton, *supra* note 40, at 6.

[49] *Id.*

[50] *Id*.

[51] *Id*.

[52] *Id.* "The unique physician identification numbers (UPIN) that are used to bill both private insurance and Medicare/Medicaid are frequently compromised." Kim McKay, *Identity Theft Steals Millions from Government Health Programs*, (Feb. 13, 2008), http://www.govtech.com/gt/260202. Additionally, an individual who receives Medicare/Medicaid also has a special identification number. *Id.* This number is also frequently used to defraud both federal programs and private insurance. *See id.* For example, 38 people in Miami-Dade, Florida, defrauded the Medicare program for $142 million. Lesley Clark, *Feds Arrest 38 in Medicare Fraud Crackdown*, Miami Herald, May 10, 2007, http://www.aegis.com/news/mh/2007/MH070501.html. The thieves defrauded the government of the price wheelchairs, walkers, and other equipment. *See id*.

[53] Hamilton, *supra* note 40, at 6.

When data breach results in medical identity theft, the results can be even more severe than what occurs in regular identity theft.[54] It is more severe because the results of medical identity theft do not simply affect the victim's pecuniary interests; medical identity theft affects the victim's health and privacy interests as well. Specifically, medical identity theft can "result in the exhaustion of the victim's insurance benefits."[55] A victim may also "experience difficulties or delays in receiving future health care services or denial of coverage" altogether because of pre-existing conditions erroneously contained in the victim's medical history.[56] "The victim may be billed for deductibles, co-payments, or other costs the healthcare provider delivered to the thief."[57]

The victim's privacy interest is also affected. Medical identity theft infringes on the trust that patients have with their healthcare providers, commonly referred to as a breach of trust.[58] To illustrate, privacy is of major concern for clinical trial participants and others who have serious health problems.[59] "[W]hen volunteers enroll in a clinical study, they place great trust in the researchers and study staff, expecting them to act both responsibility and ethically."[60] When these breaches of trust occur, "many individuals would feel a sacred trust was violated by healthcare providers and institutions."[61]

---

[54] Stacy Bradford, *Medical Identity Theft Can Happen to You* (June 17, 2009), http://moneywatch.bnet.com/saving-money/blog/family-finance/medical-identity-theft-can-happen-to-you/727/. The stakes are higher because "[u]nlike regular identity theft, this type of fraud could put your health in jeopardy and seems nearly impossible to prevent." *Id*. Additionally, when regular identity theft occurs, the thief uses the information in financial transactions. These can be relatively easy to fix because all financial information is contained in a central location. For example, all credit information flows through credit monitoring agencies. In contrast, medical information is not stored in a central repository. "[H]ealth information often flows to different recipients, such as primary care providers, specialists, health care business associates, insurance plans, researchers, and others." Hamilton, *supra* note 40, at 8. There are ways to counteract the theft of personal health information including examining the explanation of benefits forms, monitoring benefits by asking for a list of claims paid, and checking medical records and correcting inaccuracies. *Id.* at 31.

[55] Hamilton, *supra* note 40, at 8.

[56] *Id*.

[57] *Id*. "Victims are burdened with the task of proving that they are not responsible for the charges, and if they cannot, records of these unpaid costs can affect their credit rating." *Id*.

[58] Ellen Nakashima & Rick Weiss, *Patients' Date on Stolen Laptop*, Washington Post, Mar.24, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/03/23/AR2008032301753.html.

[59] *See id.*

[60] *Id*.

[61] Mark A. Rothstein, *Currents in Contemporary Ethics*, 37 J. L. MED. & ETHICS 507, 510 (2009). A study indicated that only 1% of people surveyed would feel comfortable if medical researchers were free to use their personal health information without their consent. *See* A. F. Westin, *How the Public Views Privacy and Health Research*, 20 (2007), www.hca.wa.gov/hit/documents/westiniomsrvyreport1107.doc.

Regardless of how serious the previously mentioned medical identity theft injuries are, they pale in comparison to the most dangerous consequence of the crime: having incorrect health information entered into the victim's medical records.[62] This is particularly dangerous because a healthcare provider may rely on false health information and provide inappropriate care like "transfusing the wrong blood type, performing procedures that are unnecessary or even harmful," or inadvertently prescribing medications that could cause an adverse reaction.[63] Take, for example, what happened to Lind Weaver.[64] Weaver, a 57-year-old from Palm Coast, Florida, received a bill in the mail from her local hospital requesting payment for the amputation of her right foot.[65] After weeks of clearing up the mess with the hospital, including a hostile meeting with the hospital's chief administrator where she stormed in and kicked her heels on his desk proclaiming, "Obviously, I have both of my feet," all parties presumed that the matter was resolved.[66] Unfortunately, it was not. When Weaver was hospitalized a year later for a hysterectomy, the nurse reviewing her chart said, "I see you have diabetes."[67] This alarmed Weaver, who was not a diabetic.[68] But for the fact that Weaver was conscious while the nurse was reading the information, Weaver could have been seriously injured if not killed during the surgery.[69] This example illustrates the true severity of medical identity theft and why regulations, both state and federal, should be proactive in their approach to preventing the crime.

The reality, however, is that medical identity theft is on the rise. This rise can be attributed to the fact that the street value of personal medical information is more valuable than general personal information.[70] For instance, credit card numbers and bank account personal identification numbers sell from $10 to $20, compared to $150 to $200 for documents containing personal medical information.[71] Another reason, as fully explained later in this note, is that federal regulation regarding privacy of health information has been poorly enforced.[72]

---

[62] Hamilton, *supra* note 40, at 8.

[63] *Id*.

[64] *Diagnosis: Identity Theft*, Business Week, Jan. 8, 2007, http://www.businessweek.com/magazine/content/07_02/b4016041,htm.

[65] *Id*.

[66] *Id.*

[67] *Id*.

[68] *Id*.

[69] *Id*.

[70] *See* Steve Lohr, *The New Hacker Economics*, N.Y. Times, May 8, 2008, http://bits.blogs.nytimes.com/2008/05/08/the-new-hacker-economics/.

[71] *Id.*

[72] *See generally* Rob Stein, *Medical Privacy Law Nets No Fines*, Washington Post, June 5, 2006,

http://www.washingtonpost.com/wp-dyn/content/article/2006/06/04/AR2006060400672.html.

Medical identity theft affects more than just the individual. It also affects payers,[73] providers,[74] federal agencies,[75] and society as a whole.[76] Payers, for example, bear the costs of services provided in incidents of medical identity theft.[77] It is also possible that they incur negative publicity, which could affect the business's reputation and goodwill.[78] Health care providers are affected in that they may rely on corrupted health records and improperly provide medical assistance to a patient.[79] Even though "[the] law is not yet clear on legal actions that can be taken against a provider related to negligence, malpractice, or other legal action," the defense costs and settlement offers alone could be significant.[80]

Federal agencies are also affected by medical identity theft because of the cost of investigating crimes, prosecuting criminals, enforcing federal rules, and payouts to criminals as a direct fraud victim.[81] For example, in 2007 the Department of Justice identified 120 cases of healthcare fraud.[82] In financial terms, nearly three percent of national healthcare costs, or $60 billion, are fraud-related.[83] Given that the federal government is the largest payer of healthcare costs, the financial impact of medical identity theft is substantial.[84]

Finally, society as a whole suffers from the effects of medical identity theft. Private-pay patients pay more for healthcare since providers must offset the losses

---

[73] "[P]ayers are entities that accept responsibility for payment to providers on behalf of enrolled consumers. They include organizations and institutions such as health insurance plans, federal programs, and health care sponsors, such as employers or unions." Hamilton, *supra* note 40, at 10.

[74] "Health care providers are facilities that make health services available to consumers. These include hospitals, skilled nursing homes, long term care facilities, pharmacies, labs, and diagnostic facilities." Nat'l Alliance for Health Info. Tech., *Defining Key Health Information Technology Terms*, U.S. DEPT. OF HEALTH AND HUMAN SERVS., 20 (Apr. 28, 2008), http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10741_848133_0_0_18/10_2_hit_terms.pdf.

[75] This includes Centers for Medicare and Medicaid Services, Indian Health Services, Veterans Administration, Office of the Inspector General, Department of Justice, Federal Trade Commission, Department of Health and Human Services, and the Social Security Administration. Hamilton, *supra* note 40, at 13.

[76] AHIMA e-HIM Work Group on Medical Identity Theft, *Mitigating Medical Identity Theft*, July 7, 2008, 7 Journal of AHIMA 79, (2008) AHIMA e-HIM Work Group on Medical Identity Theft, *Mitigating Medical Identity Theft*, 79 J. AHIMA 7, 63 (2008), *available at* http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_039058.hcsp?dDocName=bok1_039058.

[77] Hamilton, *supra* note 40, at 11.

[78] *Id*.

[79] *Id*.

[80] AHIMA, *supra* note 76.

[81] *See* Hamilton, *supra* note 40, at 13.

[82] *Id*. at 14.

[83] *Id.*

[84] *Id*.

they incur because of medical identity theft.[85] Additionally, taxpayers essentially fund government medical benefit payouts for fraudulent claims and government agency investigations of medical fraud and identity theft.[86]

With medical identity theft being such a severe crime, federal and state legislatures have enacted statutes in an attempt to prevent the crime from occurring. The next two sections explore the federal approach and Ohio's approach to preventing medical identity theft.

III. FEDERAL LEGISLATION TO PREVENT MEDICAL IDENTITY THEFT

The threat of data breaches alone, separate and distinct from the threat of identity theft and medical identity theft, is of major concern for lawmakers in the United States.[87] To deal with the issue of privacy, the federal government has separated privacy issues concerning healthcare from general concerns regarding the privacy of general personal information. The separation is without question due to the public's reasonable expectation of privacy as it relates to medical information.[88] Legislation in this area is likely to continue to develop because, as shown earlier, there are a variety of stakeholders who are adversely affected when data breaches and medical identity theft occurs.

The most prominent federal regulation dealing directly with data breach of medical information is the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[89] amended in 2009 by the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[90] Though separately discussed in this note, they are one cohesive piece of federal legislation that imposes data breach notification requirements on healthcare providers when their information systems are breached. This scheme of data breach notification requirements is designed to be an effective tool to prevent medical identity theft from occurring; however, its lack of enforcement has not produced the type of results necessary to achieve a significant decrease in the number of medical identity theft cases occurring each year.

---

[85] *See* AHIMA, *supra* note 76.

[86] *Id.*

[87] The federal government has enacted specific regulatory schemes for protecting personal information. The Health Insurance Portability and Accountability Act protects health information. 45 C.F.R. § 164.306. Financial Institutions are required to protect the data they possess under the Federal Trade Commissions' Safeguards Rule. 15 U.S.C. §§ 41-58 (LexisNexis 2008). The Gramm-Leach-Bliley Act protects consumers' personal financial information. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 138 (1999). Finally, the Children's Online Privacy Protection Act protects information gathered online about children under the age of thirteen. 15 U.S.C. §§ 6501-6506.

[88] F. LAWRENCE STREET & MARK P. GRANT, LAW OF THE INTERNET §206(6) (Matthew Bender & Company, Inc. eds., 17th ed. 2009).. The reasonable expectation of privacy can be eliminated when patients sign waivers when receiving medical treatment. *Id.* Some waivers, when defined broadly may eliminate the reasonable expectation of privacy altogether. *Id.*

[89] *See* Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936, 1936 (1996).

[90] *See* Health Information Technology for Economic and Clinical Health Act (HITECH Act), Pub. L. No. 111-5, 123 Stat. 115 (2009).

A. HIPAA

The primary privacy regulatory regime for the health care industry is HIPAA.[91] The Act was passed to "improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, *fraud*, and abuse in health insurance . . . ."[92] The Act's regulations are very broad and cover nearly all healthcare entities.[93] It applies to "health plans,[94] health clearing houses,[95] and health

---

[91] Christine Easter, Special Topic, *Auditing for Privacy*, 2 I/S J.L. & POL'Y FOR INFO. SOC'Y 879, 879 (2006).

[92] *See* Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936, 1936 (1996) (*emphasis added*).

[93] A health care provider includes a provider of services, a provider of medical or other health services, and any other person furnishing health care services or supplies. HIPPA, Pub. L. No. 104-191, 110 Stat. 1936, 2022 (1996). "Provider of services" means a hospital, critical access hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program, or, a fund. *Id;* 42 U.S.C.S. § 1395x(u) (LexisNexis 2010).

[94] A health plan means an individual or group plan that provides, or pays the cost of, medical care. It includes any of the following and any combination thereof:

1. A group health plan, but only if the plan
    a. has 50 or more participants; or
    b. is administered by an entity other than the employer who established and maintains the plan.
2. A health insurance issuer.
3. A health maintenance organization.
4. Part A and part B of the Medicare Program under title XVIII.
5. The Medicaid program under title XIX.
6. A Medicare supplemental policy.
7. A long term care policy, including a nursing home fixed indemnity policy (unless the DHHS Secretary determines that such a policy does not provide sufficiently comprehensive coverage of a benefit so that the policy should be treated as a health plan).
8. An employee welfare benefit plan or any other arrangement, which is established or maintained for the purpose of offering or providing health benefits to the employees of 2 or more employers.
9. The health care program for active military personal under title 10 of the United States Code.
10. The veterans health care program.
11. The Civilian health and Medical Program of Uniformed Services.
12. The Indian health service program.
13. The Federal Employees Health Benefit Plan.

HIPPA, Pub. L. No. 104-191, 110 Stat. 1936, 2022-23 (1996).

care providers,[96] who transmit any health information in electronic form in connection with a transaction."[97]

HIPAA has two key provisions. The first is the Security Rule, which protects electronic health information.[98] Unfortunately, the rule is general and vague.[99] For example, it requires covered entities to "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits."[100] Additionally, the rule requires each covered entity to protect against any reasonably anticipated unauthorized uses,[101] "threats, or hazards to the security or integrity of information."[102] These examples show that the Security Rule is vague because it does not set out specific ways for covered entities to comply with these requirements. Instead, the Security Rule merely states that "covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards" listed in the Rule.[103] This rule is aspirational rather than a concrete regulatory scheme where both the covered

---

[95] A health care clearinghouse is a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements. HIPAA, Pub. L. No. 104-191, 110 Stat. 1936, 2021 (1996).

[96] The term health care provider includes a provider of services, a provider of medical or other health services, and any other person furnishing health care services or supplies. HIPAA, Pub. L. No. 104-191, 110 Stat. 1936, 2022 (1996). The term provider of services means a hospital, critical access hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program, or a fund in certain instances. 42 U.S.C. § 1395x(u) (LexisNexis 2010).

[97] HIPAA, Pub. L. No. 104-191, 110 Stat. 1936, 2023 (1996).

[98] 45 C.F.R. § 164.302 (LexisNexis 2010). The information includes "any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of heatlh care to an individual." HIPAA, Pub. L. No. 104-191, 110 Stat. 1936, 2022 (1996).

[99] Easter, *supra* note 91, at 882.

[100] 45 C.F.R. 164.306(a)(1).

[101] § 164.306(a)(3).

[102] § 164.306(a)(2).

[103] § 164.306(d)(1). In deciding how to meet the standards, the covered entity may consider the following factors:

> 1. The size, complexity, and capabilities of the covered entity;
>
> 2. The covered entity's technical infrastructure, hardware, and software security capabilities;
>
> 3. The costs of security measures; [and]
>
> 4. The probability and criticality of potential risks to electronic protected health information.

Id.

entities as well as the agency responsible for enforcing the regulation's requirements know exactly when an entity is in or out of compliance.

The second key provision is the Privacy Rule. "The rule [was designed to] establish the first set of basic national privacy standards and fair information practices that provides all Americans with a basic level of protection and peace of mind that is essential to their full participation in their care."[104] There are four relevant standards expressed in the Privacy Rule. The first is that a covered entity may not use or disclose personal health information, except as permitted or required by the rule.[105] The permitted uses and disclosures include disclosures to the individual for treatment, payment, or otherwise in compliance with the rules, and incident to an otherwise permitted use.[106] The second standard limits a covered entity's use and disclosure of patient information when using the information for reasons other than treatment.[107] The third standard is that covered entities must also use and disclose personal health information subject to any agreed upon restriction the entity may have made with the patient.[108] Finally, an individual has a right to be notified of a covered entity's uses and disclosures of his protected health information.[109]

The Secretary of the U.S. Department of Health and Human Services (DHHS Secretary) enforces HIPAA.[110] This department has promulgated and codified rules.[111] To enforce HIPAA's requirements, the DHHS Secretary can hear complaints or it can conduct compliance audits on its own.[112] "Despite possessing the authority to independently conduct compliance reviews, the DHHS primarily relies on a complaint-driven system that refrains from initiating any sort of 'widespread effort to audit and detect violations.'".[113] The enforcement strategy as a whole was purposely designed "as a reactive, rather than a proactive, process."[114]

---

[104] *See HIPAA Privacy Rule*, RUTGERS UNIV. DIV. OF INFO. PROT. AND SEC., (Mar. 5, 2009, 3:14 PM), http://rusecure.rutgers.edu/content/hipaa-privacy-rule.

[105] 45 C.F.R. 164.502.

[106] *Id*. There are other permitted uses as well as some required disclosures.

[107] *See id*.

[108] *Id*.

[109] 45 C.F.R. § 164.520. There are many exceptions to this rule including exceptions for group health plans and inmates. *See id.*

[110] Carlos A. Leyva & Deborah L. Leyva, *HIPAA Survival Guide for Providers: Privacy and Security Rules* 1, 7 (2009 – 2010), http://www.hipaasurvivalguide.com/hipaa-survival-guide.pdf.

[111] *Id*.

[112] *Id*. at 16; 45 C.F.R. § 160.306; 45 C.F.R. §160.308.

[113] Tobi M. Murphy, Comment, *Enforcement of the HIPAA Privacy Rule: Moving From Illusory Voluntary Compliance to Continuous Compliance Through Private Accreditation*, 54 LOY. L. REV. 155, 171 (2008).

[114] *Id.;* Kevin Fogarty, *Stitching up Health Records: Privacy Compliance Lags*, eWEEK (Apr. 16, 2006), http://www.eweek.com/c/a/Health-Care-IT/Stitching-Up-Health-Records-Privacy-Compliance-Lags (confirming the preference by DHHS that problems between or within organizations be settled independently).

A major flaw in HIPAA's Security and Privacy Rules, as originally enacted, was that it did not provide covered entities with instructions on what to do when data systems were breached. Additionally, the Security and Privacy Rules were vague and overly general, leading to a lack of governmental follow-through in the area of enforcement.[115] For example, as of July 31, 2010, the Office of Civil Rights, which enforces both the Privacy and Security Rules under the direction of the Health and Human Services Department, had received approximately 53,789 complaints of privacy violations, of which 17,381 were referred for additional investigation.[116] The Office of Civil Rights then dismissed 5,960 (34%) complaints as non-violations of the HIPAA Privacy Rule and resolved the remaining 11,421 (66%) complaints through informal actions.[117] At this time, none of the investigations conducted by the Health and Human Services Department have resulted in the issuance of a single civil penalty.[118] In addition, between April 30, 2003 and July 31, 2010, only 474 (less than 1%) of the greater than 53,000 complaints received by the Office of Civil Rights were referred to the Department of Justice for criminal investigation.[119] This lack of government follow through led one commentator to assert that the Act is "like dad telling the kids he's going to count to three and then saying, "One . . . two . . . two and half . . . two and three quarters . . . ."[120]

Because HIPAA did not have data breach notification instructions and its requirements were vague, Congress amended it in 2009 to provide requirements that are more concrete.[121] The data breach notification rules were published on August 24, 2009 and became effective September 23, 2009.[122]

B. The HITECH Act Amends HIPAA

In 2009, the HITECH Act was passed to amend HIPAA.[123] President Obama signed the Act as part of the $787 billion economic American Recovery and

---

[115] *See* Gienna Shaw, *Does Anybody Care About HIPAA Anymore?*, HEALTHLEADERS MEDIA (Feb. 9, 2010), http://www.healthleadersmedia.com/content/TEC-246265/Does-Anybody-Care-About-HIPAA-Anymore.

[116] U.S. Dep't of Health & Human Servs., *HIPAA Enforcement Highlights - Numbers at a Glance*, HHS.gov, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/indexnumbers.html#total%20investigated (last updated July 31, 2010).

[117] *Id.*

[118] *See* U.S. Dep't of Health & Human Servs., *supra* note 116.

[119] *Id.*

[120] Shaw, *supra* note 115.

[121] *See* Womble Carlyle, *Action Required: HIPAA Security Breach Notification Rules* (Sept. 23, 2009), http://www.wcsr.com/client-alerts/action-required-hipaa-security-breach-notification-rules-effective-september-23-2009-additional-hitech-act-provisions-effective-early-next-year.

[122] *See id.*

[123] Dom Nicastro, *Economic Stimulus Act Heightens HIPAA Enforcement*, HCPro (Feb. 17, 2009), http://healthplans.hcpro.com/content.cfm?content_id=228444&topic=WS_HLM2_HEP.

Reinvestment Act of 2009, commonly referred to as the "Stimulus Package."[124] This amendment is significant because the "Stimulus Package" provides financial incentives for healthcare organizations that are willing to take steps to utilize Electronic Health Record technology.[125] As a string attached to these financial incentives, the Act requires certain security measures to be taken to protect patient information.[126] The Act is significant in this context because it specifies security breach notification requirements for covered entities.[127]

The HITECH Act requires HIPAA covered entities dealing with unsecured personal health information[128] to notify each individual whose unsecured protected health information has been breached[129] or is reasonably believed to have been accessed, acquired, or disclosed as a result of a breach.[130] The covered entity must give the notice within 60 calendar days after discovering a breach.[131] When the covered entity provides notice, it must include:

---

[124] *Id.*

[125] Waller Lansden Dortch & Davis, LLP, *Stimulus Package Provides Incentives for the Use of Health Information Technology, Electronic Health Records*, Feb. 14, 2009, http://www.wallerlaw.com/articles/2009/02/14/stimulus-package-provides-incentives-for-the-use-of-health-information-technology-electronic-health-records.8163. The "Stimulus Package" states that healthcare providers, like doctors and hospitals, will be reimbursed by higher Medicare and Medicaid payments if they put the systems in place by 2011. *See id.* "Doctors can receive up to $60,000 and hospitals up to $11 million." Tom Breen, *Stimulus Gives Incentives for e-health Records*, OmniMD (May 11, 2009), http://www.myemrstimulus.com/tag/doctors/.

[126] Gregg Blesh, *HHS' New Civil Rights Chief to Enforce HIPAA*, MODERNHEALTHCARE.COM (Sept. 16, 2009), http://www.modernhealthcare.com/article/20090916/REG/309169988#. The Department of Health and Human Services reiterated the importance of performing HIPAA compliance audits. *See id.* In 2009, "[DHHS] Secretary Kathleen Sebelius appointed Georgina Verdugo, a former prosecutor and Clinton administration official to lead the department's [Office of Civil Rights], which recently took over enforcement of [HIPAA's] security rule . . . " *Id.*

[127] Cynthia M. Conner et al., *American Health Lawyers Association 2008-2009 Year in Review*, 3 J. HEALTH & LIFE SCI. L. 1, 41 (2009). The connection between the 2009 "Stimulus Package" and these breach notification requirements is that "The ["Stimulus Packacge"] contains billions to fund health IT for expanding the implementation and exchange of electronic records." Nicastro, *supra* note 123. "To do [this] successfully and safely, Congress recognize[d] the need for broader and stronger, more explicit privacy and security controls." *See id.*

[128] In this context, "dealing with" means to, "access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information." *See* HITECH Act, Pub. L. No. 111-5, § 13402(a), 123 Stat. 115 (2009). "'Unsecured protected heath information' means protected health information that is not secured through the use of technology or methodology specified by the [DHHS] Secretary." *See* HITECH Act, Pub. L. No. 111-5, § 13402(h)(1)(A), 123 Stat. 115 (2009).

[129] Breach means the "unauthorized acquisition, access, use or disclosure of protected health information, which compromises the security or privacy of such information…" HITECH Act, Pub. L. No. 111-5, § 13400(1)(A), 123 Stat. 115 (2009).

[130] HITECH Act, Pub. L. No. 111-5, § 13402(a), 123 Stat. 115 (2009).

[131] See id. at, § 13402(d)(1).

> (1) A brief description of what happened, including the date of the breach and the date the breach was discovered...; (2) A description of the types of unsecured protected health information that [was] involved in the breach…; (3) The steps individuals should take to protect themselves from potential harm resulting from the breach[;] (4) A brief description of what the covered entity is doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and (5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.[132]

The HITECH Act also provides each state's attorney general the authority to enforce its provisions.[133] For example, on January 15, 2010, Connecticut's attorney general was the first to file a suit against a covered entity under the HITECH Act.[134] When a state's attorney general has reason to believe that an interest of one or more of the residents of that state has been or is threatened by a person violating the Act, the attorney general may bring a civil action on behalf of the residents of the state in federal court.[135] The attorney general may seek an injunction or statutory damages.[136]

State attorneys general do not have exclusive authority to enforce the HITECH Act regulations. The DHHS Secretary also has the authority to assess civil monetary penalties and negotiate monetary settlements for HITECH Act violations.[137] The money received from these penalties and settlements is sent to the Office for Civil Rights, which is an office of the Department of Health and Human Services, to be used to further enforce HIPAA's requirements.[138] As of the publication of this note, all monetary penalties and settlements recovered will go to the Officer for Civil Rights; however, the HITECH Act sets out a plan to get recommendations and implement a system that allows individuals harmed by HIPAA violations to receive a percentage of the money.[139] This plan is to be executed within three years,[140] but even when it is completed, individuals will not have access to civil awards won by

---

[132] *Id.* § 13402(f).

[133] *Id.* § 13410(e).

[134] Keith L. Martin, *Conn. AG Sues Health Net Over "Ethically Unacceptable" Data Breach*, IAFwebnews.com (Jan. 15, 2010), http://ifawebnews.com/2010/01/15/conn-ag-sues-health-net-over-ethically-unacceptable-data-breach/. The attorney general filed suit against Health Net of Connecticut for a data breach jeopardizing the personal information of 446,000 of its members. *Id*. "The [lawsuit] alleges that the insurer failed to effectively supervise and train its workforce on policies and procedures concerning the appropriate maintenance, use, and disclosure of protected health information." *Id.*

[135] HITECH Act, Pub. L. No. 111-5, § 13410(e), 123 Stat. 115 (2009).

[136] *Id.* The total amount of damages imposed may not exceed $25,000 in a calendar year. Additionally, if the attorney general brings a successful action, he may be awarded the costs of the action and reasonable attorney fees to the state. *Id.*

[137] *See id.* § 13410(a).

[138] *Id*. § 13410(c).

[139] *Id*. § 13410(a).

[140] *See id.* § 13410(c)(3).

their respective state attorney general.[141] Unless the individual's respective state law allows a citizen to recover a percentage of an action brought by a state attorney general, the individual will not have access to any monetary penalties won by the state attorney general under HIPAA.[142] This distinction exists because the federal statute only governs the awards the DHHS Secretary receives.[143] In other words, each state is responsible for enacting legislation to govern whether state residents harmed by a data breach will have access to monetary penalties awarded to their state's attorney general and to what extent.[144]

Even though the Act gives state attorneys general the right to enforce its provisions, this right is not absolute. Before an attorney general can file a civil action, he must provide notice to the DHHS Secretary.[145] This is significant because the DHHS Secretary can intervene in the action.[146] The text's plain language leads to the inference that the DHHS Secretary can literally block civil actions initiated by a state attorney general.[147] An additional issue is that the statute's language allows for this intervention, but there is no restrictive language that allows a state attorney general to know when the intervention would be appropriate.[148] This lack of restrictive language leads to the inference that at any time, and for any reason, the DHHS Secretary has the discretion to intervene in a civil action brought by a state attorney general. The DHHS Secretary's ability to intervene may pose a serious threat to a state attorney general's ability to enforce the new data breach notification requirements.

Even if state attorneys general find it difficult to enforce HIPAA and its HITECH Act amendments, the federal statutory scheme gives states the authority, in specific instances, to enforce data breach notification requirements based on their own state laws.

C. Federal Preemption of State Laws

While HIPAA is a robust federal regulatory scheme, it does not completely preempt state law. The Supremacy Clause stands for the proposition that the Constitution and the laws of the federal government are, in most cases, more forceful

---

[141] *See id.* § 13410(c)(1).

[142] *See id.*

[143] *See id.* For civil awards received by the DHHS Secretary, the HITECH Act directs that those funds "shall be transferred to the Office for Civil Rights of the Department of Health and Human Services to be used for purposes of enforcing the provisions of this subtitle . . . ." *Id.*

[144] *See id.*

[145] *See id.* § 13410(e).

[146] *See id.* § 13410(e)(1).

[147] "The State shall serve prior written notice of any action . . . upon the [DHHS] Secretary and provide the [DHHS] Secretary with a copy of its complaint . . . The [DHHS] Secretary shall have the right to intervene in the action." *Id.*

[148] *See id.* The only time where the Act specifically states that a state attorney general may not bring an action is when the DHHS Secretary has already instituted an action against a person. *See id.*

than state laws.[149] Because of this, inconsistent state laws are generally preempted or trumped by federal laws.[150] When the laws are not in conflict, preemption can either be implied or expressly stated in federal legislation.[151]

Here, HIPAA expressly preempts state law and supports state law in certain instances. In general, a HIPAA standard, requirement, or implementation specification that is contrary to a provision of state law preempts the state law.[152] However, a contrary state law may not be preempted if the DHHS Secretary determines that the state law is necessary: "(1) [t]o prevent fraud and abuse related to the provision of or payment of health care; (2) [t]o ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation; (3) [f]or State reporting on health care delivery or costs; or (4) for purposes of serving a compelling need related to public health, safety, or welfare . . . "[153] Additionally, an inconsistent state statute may not be preempted if the DHHS Secretary determines that its principal purpose is the "regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances," or that a "controlled substance by state law."[154]

HIPAA's most unique preemption provision says that a state law relating to the privacy of individually identifiable health information that is more stringent than a HIPAA standard, requirement, or implementation specification will not be preempted.[155] The regulation provides minimal guidance for state laws relating to the privacy of health information. Thus, each state law must be independently examined, and those that are more protective are not preempted.[156] Generally, state laws regarding covered entities are almost always more stringent.[157] Under HIPAA, a state law is more stringent if:

> (1) the state law prohibits or further limits the use or disclosure of protected health information; (2) the state law permits individuals with greater rights of access to or amendment of their individually identifiable

---

[149] *See* U.S. CONST. art. VI, cl. 2. The Supremacy Clause provides:

> This Constitution, and the Laws of the United States which shall be made in Pursuance Thereof; and all Treaties made, or which shall be made, under the Authority of the United States, *shall be the supreme Law of the Land*; and the judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding.

Id. (emphasis added).

[150] *See* Geier v. Am. Honda Motor Co., 529 U.S. 861, 882 (2000).

[151] *See* Int'l Paper Co. v. Ouellette, 479 U.S. 481, 491 (1987).

[152] 45 C.F.R. § 160.203 (2010).

[153] *Id.* §160.203(a)(1).

[154] *Id.* § 160.203(a)(2).

[155] *See id.* § 160.203(b).

[156] *See* Jennifer Guthrie, *Time Is Running Out- The Burdens and Challenges of HIPAA Compliance: A Look at Preemption Analysis, the "Minimum Necessary" Standard, and the Notice of Privacy Practices*, 12 ANNALS HEALTH L. 143, 150 (2003).

[157] *See* Leyva & Leyva, *supra* note 110, at 14.

> health information; (3) the state law provides for more information to be disseminated to the individual regarding use and disclosure of their protected health information; (4) the state law imposes stricter standards for record keeping or accounting of disclosures; or (5) the state law strengthens privacy protections for individuals with respect to any other matter.[158]

Under this regulatory scheme, Ohio has sufficient room to enact legislation to protect its residents from medical identity theft. Regrettably, the state has explicitly opted to leave privacy issues related to healthcare providers to the federal government.

IV. OHIO'S DATA BREACH LAW DOES NOT COVER HIPAA COVERED ENTITIES

Ohio, like many other states,[159] has enacted laws regarding data breach notification. Ohio's law covers breaches of security systems that house personal information.[160] While Ohio's law does cover Ohio governmental agencies, individuals, and entities that conduct business[161] in Ohio, it does not regulate healthcare providers.[162] Specifically, Ohio's data breach notification laws do not apply to any HIPAA-covered entity.[163]

Ohio's statute is limited to protecting general personal information, such as an individual's name, in combination with and linked to the individual's social security number, drivers license number, or account, credit or debit card number with an

---

[158] 45 C.F.R. § 160.202 (2010).

[159] Just about every state has adopted some form of data encryption and regulation law. "As a result, all businesses should understand fully the importance of these new legal requirements…" Michael D. Stovsky, *New Data Encryption Laws and Regulations Require Compliance*, Ulmer Berne, LLP Client Alert (February 2009), http://ulmer.com/articlesalerts/clientalerts/Documents/02%20February%20-%20Data%20Encryption.pdf. Businesses should take steps to comply with these laws because the "laws or regulations apply directly, or because the concepts contained in these new laws or regulations will likely become applicable in one form or another." *Id*.

[160] OHIO. REV. CODE. ANN. § 1349.19(A)(1)(1) (LexisNexis 2010). Ohio defines a breach of the security system as, "unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state." *Id*.

[161] Jeffrey L. Kapp, et al., *Data Protection and Privacy: Ohio Enacts Security Breach Notification Law*, Jones Day (February 2006), http://www.jonesday.com/newsknowledge/publicationdetail.aspx?publication=3129. The concept of "conducting business" is not clearly defined in the notification law and it appears that physical presence in Ohio is not required. *Id.*

[162] *Id.*

[163] OHIO REV. CODE. ANN. § 1349.19(F)(2) (LexisNexis 2010). "This section does not apply to any person or entity that is a covered entity as defined in 45 C.F.R. 160.103 . . . ." *Id.*

access code that would permit access to an individual's financial account.[164] In fact, the statute does not even mention health related information.

The law applies to "any person[165] who owns or licenses computerized data that includes personal information."[166] Because most businesses store customer information in electronic form, virtually every business falls under this statute, unless it is otherwise exempted, such as HIPAA covered entities. The statute requires businesses to notify Ohio residents of data breaches under certain conditions:

> (1) When a business discovers or is notified of a breach to its information system; (2) The business knows or reasonably believes that an Ohio resident's personal information was accessed and acquired by an unauthorized person; and (3) The business believes that the access and acquisition of the Ohio resident's information creates a material risk of identity theft or other fraud.[167]

Ohio requires that the notification be given within 45 days after the discovery of the breach.[168] This notification can be done by letter, e-mail,[169] or phone.[170]

In the event that a business or individual violates any of Ohio's data breach notification requirements, it may be subject to civil liability.[171] Ohio's attorney general has the "exclusive" authority to bring civil actions against companies that violate Ohio's data breach notification laws.[172] The statute authorizes the attorney general to seek temporary restraining orders, preliminary or permanent injunctions,

---

[164] OHIO REV. CODE. ANN. § 1349.19(A)(7)(a) (LexisNexis 2010). The language of the statute does indicates that if the personal information is encrypted, redacted, or altered in a method that makes it unreadable, the personal information does not fall under the statute. *Id.* Encryption means to transform data into a form that has a low probability of assigning meaning without use of a confidential process or key. *Id.* § 1349.19(A)(4). Redaction means to alter the information so that no more than the last four digits of a social security number, driver's license number, state identification card number, account number, or credit or debit card number is accessible as part of the data. *Id.* § 1349.19(A)(8).

[165] Person includes both natural persons and business entities conducting business in Ohio. OHIO REV. CODE ANN. § 1349.19(A)(6).

[166] *Id.* § 1349.19(B)(1).

[167] *See id.*

[168] *See id.* § 1349.19(B)(2).

[169] Electronic notice is only appropriate when the person's primary method of communication with the Ohio resident is through electronic means. *See id.* § 1349.19(E)(2).

[170] *Id.* §1349.19(E). Substitute forms of notice are available if the company can show that it does not have sufficient customer contact information or that the cost of notification would exceed $250,000 or if the number of customers exceeds 500,000. If one of these requirements are met, a company may notify consumers of the breach by e-mail, posting on the customer's website, or through a major media outlet that reaches at least 75% of Ohio residents. *Id.*

[171] *See id.* § 1349.19(I).

[172] *See id.* § 1349.192(A)(1).

and civil penalties.[173] The attorney general has the exclusive authority to bring a civil action and may do so "based on complaints or the attorney general's own inquiries."[174] Penalties that are received as a result of the attorney general's actions are deposited into a consumer protection enforcement fund; however, the money is never given directly to the consumers.[175] "The money in the consumer protection enforcement fund [is] used for the *sole purpose of paying expenses* incurred by the consumer protection section of the office of the attorney general."[176]

Because Ohio has expressly decided not to enact legislation to further protect the privacy of individual's health information, it adds nothing to the national effort to prevent medical identity theft.

V. OHIO SHOULD AMEND ITS DATA BREACH NOTIFICATION LAW

As shown above, Ohio has the authority and the ability to enact state legislation to help prevent medical identity theft. Specifically, there are four things that the state legislature can do to help prevent medical identity theft and provide its citizens relief when the crime occurs. First, the state should amend its data breach notification law to include HIPAA covered entities. Second, the state should require healthcare providers to notify consumers every time their information systems have been breached. Third, healthcare providers should be required to destroy medical records and other data containing patient health information when the provider wishes to discard the information. And finally, Ohio should provide a mechanism for individuals to gain direct access to monetary awards received from healthcare providers that violate the statute's requirement. All of these changes will be proactive steps in helping to prevent medical identity theft from occurring.

A. Ohio's Data Breach Notification Law Should Apply to HIPAA Covered Entities

Ohio should amend its data breach notification statute to reach HIPAA covered entities. As stated earlier, HIPAA does not preempt state laws that impose more stringent requirements on covered entities. This allows states to protect their citizens better. Ohio should take advantage of this authority for two reasons. The first reason is that HIPAA has not been widely enforced. The second reason is that the attorney general can bring suits under Ohio's law and not be subject to intervention by the DHHS Secretary.

Ohio law should cover healthcare entities because HIPAA has been poorly enforced.[177] The Office for Civil Rights[178] reported that since the compliance date in

---

[173] *See id.* The civil penalty under this section is only levied after the attorney general has learned that the business "has intentionally or recklessly failed to comply with the applicable section for more than ninety days." *Id.* § 1349.192(A)(1)(c). After a court finds this, the business may be fined up to $1,000 per day for the first 60 days of noncompliance, up to $5,000 from day 61 to 90, and up to $10,000 for each day thereafter. *Id*.

[174] *Id.* § 1349.191(B).

[175] *Id*. § 1349.192(A)(2).

[176] *Id.* § 1345.51.

[177] California was the first state to require data breach notification and its law explicitly addresses health care organizations. *See* Hamilton, *supra* note 40, at 30.

April 2003, more than half of the cases were closed because they were not eligible for enforcement.[179] In Ohio alone, since 2003, 71% of all complaints were resolved after intake and review,[180] meaning that no formal investigation was ever made before the complaint was dismissed.[181] Of Ohio cases, 11% were found not to have a violation after an investigation.[182] And 17% of the cases were investigated and resolved with a voluntary corrective action or other agreement obtained from the covered entity.[183] This is absurd considering that a recent survey found that one in four of the 196 health organizations that responded "do not conduct a formal risk analysis to identify security gaps in electronic patient data."[184] This is significant because a failure to conduct risk analysis is a direct violation of HIPAA's Security Rule.[185] Even more alarming, the survey revealed that the Department of Health and Human Services has never penalized an organization for violating HIPAA's data risk analysis provision.[186] By the Department of Health and Humans Service's own admission, there is no desire to penalize healthcare providers for these violations. As Susan McAndrew, Deputy Director at the Department of Health and Human Services Office for Civil Rights, said, "[T]he Agency hasn't issued any fines because the goal of enforcement is to nudge doctors, hospitals, and insurers into compliance, not to punish them."[187] She also added that the Department of Health and Human Services has no need "to evoke a penalty scheme in order to get the corrective action."[188]

Ohio should also amend its current data breach notification law to include healthcare providers because it will make enforcement of privacy and security

---

[178] "[T]he agency relies on media reports, complaints, and referrals from other agencies to learn of potential HIPAA rules violations." Joe Eaton, *Patient Data Safety Rules Widely Disregarded, Unenforced* (Jan. 19, 2010), http://www.publicintegrity.org/articles/entry/1906/.

[179] *See* Nicastro, *supra* note 123.

[180] The resolution after intake and review can be accomplished in four ways: (1) the violation did not occur after April 14, 2003; (2) the entity is not covered by the Privacy Rule; (3) the complaint was not filed within 180 days and an extension was not granted; and (4) the incident described in the complaint does not violate the Privacy Rule. U.S. Department of Health & Human Services, *Enforcement Process*, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/index.html.

[181] U.S. Department of Health & Human Services, *Enforcement Results by State*, Dec. 31, 2009, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/nmtosc.html#OH.

[182] *Id.*

[183] *Id.*; *see also* U.S. Department of Health & Human Services, *Enforcement Process*, *supra* note 180.

[184] Eaton, *supra* note 178. The study came to the conclusion that a "number of hospitals, health clinics, and insurance firms are violating federal security rules on patient data and putting sensitive health information at risk." *Id.*

[185] *See* 45 C.F.R. 164.308(a)(1) (2010). The purpose of the risk assessment is to assure that patient information does not fall into the wrong hands. *See generally id.*

[186] *See* Eaton, *supra* note 178.

[187] *Id*.

[188] *Id*.

standards easier. Under HIPAA, when a state attorney general seeks to punish a covered entity for violating one of the statute's requirements, the attorney general must first notify the DHHS Secretary, who may intervene in the action.[189] If Ohio were to apply its data breach notification statute directly to HIPAA covered entities, the attorney general could bypass any possible intervention by the DHHS Secretary and file civil suits based on violations of the Ohio statute.[190]

Applying Ohio law to covered entities provides a better way of enforcing data breach notification law and makes HIPAA's lack of enforcement virtually irrelevant because of the adequacy of the state law.[191] State laws that make enforcement of a federal law virtually irrelevant are not unprecedented. In fact, in areas beyond data breach there are many examples of state regulations being more effective than federal regulations.[192] For example, Congress has delegated the entire regulation and taxation of the insurance industry to the states.[193] Furthermore, "one of federalism's chief virtues . . . is that it promotes innovation by allowing for the possibility that 'a single courageous State may, if its citizens choose, serve as a laboratory; and try

---

[189] *See* HITECH Act, Pub. L. No. 111-5, § 13410(e)(1), 123 Stat. 115, 274 (2009).

[190] In other regulatory schemes, federal regulation agencies do not have the power to intervene. For example, in the field of environmental regulation, while notice is given, the Environmental Protection Agency cannot intervene in an action. *See* 40 C.F.R. § 254.2. The regulation provides no indication that the Environmental Protection Agency can intervene in a civil action brought by a citizen or state attorney general. For example, the regulation states, "[A] copy of the notice shall be mailed to the Administrator of the Environmental Protection Agency, The Regional Administrator of the Environmental Protection Agency for the region in which the violation is alleged to have occurred, and the chief administrative officer of the solid waste management agency for the State in which the violation is alleged to have occurred" *Id.* § 254.2(a)(1).

[191] There is a school of thought that feels that a federal law addressing data breach is unnecessary because state laws are adequate. *See* Samuel Lee, *Breach Notification Laws: Notification Requirements and Data Safeguarding Now Apply to Everyone, Including Entrepreneurs*, 1 ENTREPRENEURIAL BUS. L. J. 125, 142 (2006).

[192] *Examining the Financial Services Industry's Responsibilities and Role in Preventing Identity Theft and Protecting Sensitive Financial Information: Before the S. Comm. On Banking, Housing, and Urban Affairs*, 109th Cong. 728 (2005) (Statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group). A few examples of state privacy leadership:

- "[F]orty states had already enacted 'do not call lists' before the Federal Trade Commission acted in 2003 to establish a national list.
- Seven states enacted free credit report on request laws before Congress enacted one in the 2003 [Fair and Accurate Credit Transactions Act].
- Over a dozen states enacted laws requiring the truncation of credit card numbers on consumer receipts before the provision was made nationwide in the Fair and Accurate Credit Transactions Act."

Id.

[193] *See* McCarran-Ferguson Act, 15 U.S.C. §§ 1011-1015 (2008). The Act provides that the "business of insurance, and every person engaged therein, shall be subject to the laws of the several States which relate to the regulation or taxation of such business." *Id.* § 1012(a).

novel social and economic experiments without risk to the rest of the country.'"[194] It is under this backdrop that Ohio should take the first step and mandate that its data breach notification apply to healthcare providers.

If Ohio were to amend its data breach notification law to reach HIPAA covered entities, there are concerns that amending the state law would be unproductive. Opponents to the amendment may argue that the federal law, HIPAA, should completely preempt state data breach notification laws.[195] The conclusion reached by this school of thought is that data security is a "distinct federal responsibility that requires a targeted federal legislative and regulatory response."[196] This school of thought argues that the federal government should control this because notification requirements differ from state to state and not all states provide protections to organizations that try to protect personal information through encryption.[197] Additional support for this position is that a central regulatory authority enforcing a single law is much better than various state attorneys general enforcing their own state laws because of the difficulty in understanding which conflicting law controls in a given situation.[198]

Supporters of a single federal act that would preempt all state laws on the subject note that one central federal regulatory system would better address the needs of the consumers and HIPAA covered entities. The argument is that state laws are too consumer based because the laws require disclosure based on the residency of the

---

[194] *See* Gonzales v. Raich, 545 U.S. 1, 42 (2005) (O'Conner, J., dissenting) (quoting *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J. dissenting).

[195] *See* Lee, *supra* note 191, at 142.

[196] *See Examining the Financial Services Industry's Responsibilities and Role in Preventing Identity Theft and Protecting Sensitive Financial Information: Before the S. Comm. On Banking, Housing, and Urban Affairs*, 109th Cong. 728 (2005) (Statement of Ira D. Hammerman, Senior Vice President and General Counsel to the Securities Industry Association). Ira D. Hammerman urged the Senate to adopt the following assertions in establishing a national data breach notification law that would preempt all state laws:

1. "A clear national standard to achieve a uniform, consistent approach that meets consumer expectation;
2. Trigger for consumer notice tied to significant risk of harm or injury that might result in identity theft;
3. A precise definition of sensitive personal information tied to the risk of identity theft;
4. Exclusive functional regulator oversight and rulemaking authority;
5. Flexible notification provisions; and
6. Reasonable administrative compliance obligations."

Id.

[197] *See* Jaikumar Vijayan, *Three More States Add Laws on Data Breaches*, Computerworld (Jan. 6, 2006), http://www.computerworld.com/s/article/107574/Three_More_States_Add_Laws_on_Data_Breaches.

[198] *See id.* The difference in state laws is likely to exacerbate the confusion and potential harm to customers. *See* Mierzwinski, *supra* note 192.

consumer, rather than the location where the breach occurred. This means that when a covered entity incurs a data breach, it must comply with the state law of each of its affected consumers.[199] This could easily range from a few different state laws to dozens of state laws depending on the size of the covered entity's personal information database. In essence, supporters of a single federal law support a central regulatory and enforcement body because it would have the expertise to adjust privacy protections over time as threat levels change and the industry's ability to respond to data breaches evolves.[200]

Finally, supporters of one national law argue that because evidence is lacking on the effectiveness of data breach notification statutes in preventing general identity theft,[201] extension of Ohio's law to covered entities may not decrease instances of medical identity theft. A study showed that the passage of data breach notification laws reduced the identity theft rate by less than 6.1 percent on average.[202] Healthcare providers and the legislature fear that extending Ohio's law to covered entities may not effectively prevent cases of medical identity theft, but rather impede e-commerce and stifle technological development by discouraging healthcare providers from innovation using consumers' personal health information.[203]

The concerns of those desiring a national regulatory scheme are outweighed for the reasons stated earlier. Additionally, breach notification statutes provide "an incentive for companies to improve security controls and [allow] consumers to make informed decisions about their individually identifiable information."[204] Furthermore, there is no telling how effective the HIPAA amendments through the HITECH Act will be. It is too soon to tell if the new data breach notification laws

---

[199] *See* Romanosky et. al., *supra* note 23, at 7.

[200] *See* Mierzwinski, *supra* note 192.

[201] *See* Romanosky et. al., *supra* note 21, at 3. "To date, no empirical analysis has investigated the effectiveness of such legislative initiatives in reducing identity theft." *Id.* at 3.

[202] *Id.* at 2. By the study's own admission, the quality of data and the possibility of sampling bias also potentially affected the information. *See id.* However, the argument gains support through comparison to other laws enacted to combat certain behavior. For example, state laws banning the use of handheld devices to make calls or send text messages while driving have not resulted in fewer vehicle crashes, despite the fact that six states and the District of Columbia ban talking on a hand-held device, and 19 states and the District of Columbia ban texting while driving. *See generally Distracted Driving Laws Don't Stop Crashes, Study Shows*, Associated Press, Jan. 29, 2010, *available at* http://www.cleveland.com/business/index.ssf/2010/01/distracted_driving_laws_dont_s.html. The article concludes that the survey leaves more questions than answers because the data did not definitively determine why the laws have not decreased the number of accidents. *Id*. Much like the purpose of data breach notification statutes, these bans are designed to prevent an event from occurring other than the subject matter that the law directly addresses. These bans on activities while driving are designed to prevent accidents, and the data breach regulations are designed to prevent occurrences of identity theft. Comparing the results of legislation in both areas will be helpful in determining their overall effectiveness.

[203] Romanosky et. al., *supra* note 23, at 2.

[204] Hamilton, *supra* note 40, at 31; Romanosky et. al., *supra* note 23, at 2. "Notifications can also enable law enforcement, researchers, and policy makers to better understand which firms and sectors are best [or worst] at protecting consumer and employee data." Romanosky et. al., *supra* note 23, at 2.

will be enforced any differently than the existing HIPAA requirements. Industry commentators have observed, "[W]ith so little proactive intervention by the federal government to date, covered entities have no incentive to take the threat of civil or criminal penalties [introduced through the HITECH Act] seriously."[205] Moreover, even if the state laws provide only an ounce of incentive to prevent medical identity theft from occurring, it is worth a pound of cure.[206]

B. Ohio's Data Breach Notification Law Should Have an Acquisition-Based Trigger

Ohio should amend its data breach notification statute by replacing its risk-based trigger with an acquisition-based trigger. State data breach notification laws can be defined by their trigger. The trigger is the event that requires the organization to notify its customers that a data breach occurred.[207] States differ on the event that triggers organizations to notify consumers of a data breach.[208] There are two types of triggers: acquisition-based triggers and risk-based triggers. Acquisition-based triggers require consumer notification whenever personal data is reasonably believed to have been acquired by an unauthorized person and require no evidence that an unauthorized person actually acquired the data.[209] On the other hand, "[r]isk-based triggers allow for a risk assessment to determine whether any harm has or will be done to those whose records were potentially breached."[210] With risk-based triggers, notification is only necessary where the potential for harm exists.[211]

Ohio should adopt an acquisition-based trigger like California's statute because an acquisition-based trigger puts consumers on notice that an unauthorized individual has accessed their personal information. This is the better model for consumers because under the risk-based trigger, consumers are not notified when an organization cannot determine who accessed consumer information and why.[212] In other words, under the risk-based trigger, a business whose security has been breached has no duty to notify consumers if it does not know how the information is,

---

[205] Tobi M. Murphy, *Comment: Enforcement of the HIPAA Privacy Rule: Moving From Illusory Voluntary Compliance to Continuous Compliance Through Private Accreditation*, 54 LOY. L. REV. 155, 182 (2008).

[206] *See* David Harlow, *HIPAA Enforcement by State Attorneys General: The Shape of Things to Come* (Jan. 14, 2010), http://healthblawg.typepad.com/healthblawg/2010/01/hipaa-enforcement-by-state-attorneys-general-the-shape-of-things-to-come.html.

[207] Julie A. Heitzenrater, *Identity and Data Loss: Data Breach Notification Legislation: Recent Developments*, 4 I/S: A J.L. & POL'Y FOR THE INFO. SOC'Y 661, 663 (2009).

[208] Michael E. Jones, *Privacy on the Internet and in Organizational Database: Data Breaches: Recent Developments in the Public and Private Sectors*, 3 I/S: A J. L. & POL'Y FOR THE INFO. SOC'Y 555, 561-62 (2007).

[209] Heitzenrater, *supra* note 207, at 663-64. This type of trigger is used in about half the states that have data breach notification statutes. Jones, *supra* note 208, at 562.

[210] Heitzenrater, *supra* note 207, at 664.

[211] *Id.*

[212] *Examining the Financial Services Industry's Responsibilities and Role in Preventing Identity Theft and Protecting Sensitive Financial Information: Before the S. Comm. On Banking, Housing, and Urban Affairs*, *supra* note 192 (Statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group).

or might be used by an unauthorized user.[213] This leaves the burden of uncertainty on consumers, by virtually leaving them in the dark.[214] This burden can be extremely severe as it pertains to medical identity theft because unlike regular identity theft, there is no guarantee that the consumer will even find out about the medical identity theft. Even if the consumer finds out about it, there is no central repository of information where the consumer can call and get matter corrected. Additionally, risk-based triggers are not useful in preventing medical identity theft because they allow companies, which have an interest in keeping data breaches secret, to decide if notice is required.[215] The acquisition-based trigger provides an incentive for businesses to invest more in data security because they know they are obligated to notify consumers of every data breach.[216]

The opposition to acquisition-based triggers argues that too much reporting will lead to consumer apathy about the risk of medical identity theft.[217] The purpose is to ensure that notification is always linked to some sort of demonstrable risk of harm to the customer.[218] Furthermore, the risk-based trigger considers the interests of the businesses responsible for notification[219] because it allows the organization to consider the cost of breach notification and the actual likelihood that the breached information will be used to harm the individual. An acquisition-based trigger would increase overhead costs because healthcare providers would be forced to notify the public any time a data breach occurred.

---

[213] *Id.*

[214] *Id.*

[215] *Id.* at 10.

[216] *Id.*

[217] *Id*. This allows companies to unilaterally issue notifications whenever they feel disclosure is appropriate. *Id*.

[218] *Examining the Financial Services Industry's Responsibilities and Role in Preventing Identity Theft and Protecting Sensitive Financial Information: Before the S. Comm. On Banking, Housing, and Urban Affairs*, *supra* note 192 (Statement of Ira D. Hammerman, Senior V.P. and Gen. Counsel, Sec. Indus. Ass'n.).

[219] It is yet to be seen how the United States Supreme Court decision in *Citizens United v. Federal Election Commission* will play out in the area of healthcare legislation. *See generally* Citizens United v. Fed. Election Comm'n, 130 S. Ct. 876 (2010). It is very possible that healthcare lobbyists will be able to persuade legislators, at the federal and state level, for more favorable laws and regulations. *See generally The Court's Blow to Democracy*, N. Y. TIMES EDITORIAL (Jan. 22, 2010), http://www.nytimes.com/2010/01/22/opinion/22fri1.html. Healthcare lobbyists may be able to persuade legislators like never before because the decision in *Citizens United* struck down decades-old limitations on corporate political expenditures by permitting businesses and unions to spend freely on commercials for or against candidates. *See* Jess Bravin, *Court Kills Limits on Corporate Politicking*, WALL ST. J. (Jan. 22, 2010), http://online.wsj.com/article/SB10001424052748703699204575016942930090152.html. President Obama called the decision, "[a] major victory for big oil, Wall Street banks, *Health insurance companies* and other powerful interests that marshal their power every day in Washington to drown out the voices of everyday Americans." Adam Liptak, *Justices, 5-4, Reject Corporate Spending Limit*, N.Y. TIMES (Jan. 22, 2010), http://www.nytimes.com/2010/01/22/us/politics/22scotus.html (*emphasis added).*

While these concerns to the corporate welfare are important, they fail to address the fact that corporations have a duty to protect the consumer information that they possess. Based on the number of data breaches occurring every year, it is undisputed that healthcare providers and other organizations are simply incapable of protecting information. This inability puts patients and consumers at risk. At the very least, healthcare providers should be required to inform patients when information systems are breached. Additionally, the term "risk-based trigger" is somewhat of an oxymoron because corporations are incapable of truly determining when and how an unauthorized user of consumer information is going to do with that information. It is very common for a hacker to steal personal information from an organization and wait months or even years before attempting to use the stolen information.[220] The bottom line is that consumers have the right to know when an organization they trusted has failed to safeguard their personal information. Customers also have the right to decide what course of action they will take to protect themselves from potential medical identity theft attempts. Healthcare providers and other businesses, which have a vested interest in not notifying customers and are incapable of determining what an unauthorized person will do with customers' information, should not be able to take these rights away.

C. Ohio's Data Breach Notification Law Should Require Healthcare Providers to Destroy or Encrypt Discarded Medical Records

Ohio should amend its data breach notification statute to require covered entities to destroy data that the entity wants to dispose of.[221] This requirement is important because careless document disposal is the leading way for identity thieves to get personal information.[222] In fact, only 12% of identity theft is perpetrated online.[223] For example, a fourth-grade schoolteacher in Salt Lake City purchased scrap paper for her students that turned out to be medical records of twenty-eight patients.[224] Included in the records that were inadvertently sold as surplus paper were the medical history, personal contact information, insurance information, and social security numbers for each patient.[225] This example is merely illustrative of the vast

---

[220] Darrow & Lichtenstein, *supra*, note 20, at 25.

[221] Ohio's statute establishes a safe harbor for information that is encrypted. *See* OHIO REV. CODE ANN. § 1349.19(A)(7)(a) (LexisNexis 2010). No state requires corporations to provide notification of a data breach if the compromised information is encrypted. *See* Bruce E. H. Johnson et al., *Data Breach Notice Legislation: New Technologies and New Privacy Duties?*, 865 PLI/PAT 203, 216 (2006). This creates a safe harbor for corporations to avoid data breach notification requirements by encrypting all electronic consumer information. *Id.*

[222] Lisa Black & John Keilman. *Paper Trail: Personal Data Found Blowing in the Wind* (Jan. 30, 2010), http://articles.chicagotribune.com/2010-01-30/news/1001300085_1_social-security-documents-paperwork/2; *see also* Better Business Bureau, S*pring-Cleaning? Prevent ID Theft by Following BBB Advice on What to Keep and What to Shred,* (Apr. 2, 2008), http://www.bbb.org/us/article/spring-cleaning-prevent-id-theft-by-following-bbb-advice-on-what-to-keep-and-what-to-shred-4149.

[223] *See* Better Business Bureau, *supra* note 222.

[224] *See Medical Records Sold to Teacher as Scrap Paper*, MSNBC.COM (Mar. 10, 2008), http://www.msnbc.msn.com/id/23561667/?GT1=43001.

[225] *Id.*

majority of identity theft cases that occur when the thief has direct contact with the victim's personal information through a stolen or lost wallet, or by rifling through the victim's mailbox or trash.[226] This means that an effective and proactive way to prevent medial identity theft even before it happens is to properly destroy data containing personal information when it is no longer useful.[227]

Ohio should implement one of two types of data destruction laws. The first option is a data destruction law that specifically enumerates how the data must be destroyed.[228] California, for example, requires businesses to destroy customers' records that are no longer being maintained.[229] The provision states that:

> A business shall take all reasonable steps to dispose, or arrange for the disposal of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.[230]

---

[226] *See id*. Identity thieves often dumpster dive or look through trash for private information that can be harvested and used for unlawful purposes. *See* New York State Consumer Protection Board, *Shred the Word! To Prevent Identity Theft at a Free Public Shredding Day in Amsterdam, NY* (Sept. 21, 2009), http://www.consumer.state.ny.us/pressreleases/2009/sept212009.htm.

[227] *See generally* Better Business Bureau, *supra* note 222.

[228] States that have passed this type of law include Arkansas, California, Georgia, Indiana, Kansas, Massachusetts, Michigan, Montana, Nevada, New Jersey, New York, Oregon, Rhode Island, Texas, Vermont. *See* Scott & Scott LLP, *Data Destruction Law (Business and Technology Law)* (Oct. 5, 2007), http://blawg.scottandscottllp.com/businessandtechnologylaw/2007/10/data_destruction_laws.html.

[229] Doe 1 v. AOL LLC, 552 F.3d 1077, 1080 (9th Cir. 2009).

[230] CAL. CIV. CODE § 1798.81 (West 2010). California is not the only state that has the disposal requirement. For example, Colorado's law states: "Each public and private entity in the state that uses documents during the course of business that contain personal identifying information shall develop a policy for the destruction or proper disposal of paper documents containing personal identifying information." COLO. REV. STAT. § 6-1-713(1) (2010).

Additionally, New York has a similar provision:

> No person, business, firm, partnership, association, or corporation, not including the state or its political subdivisions, shall dispose of a record containing personal identifying information unless the person, business, firm, partnership, association, or corporation, or other person under contract with the business, firm, partnership, association, or corporation does any of the following: (a) shreds the record before the disposal of the record; or (b) destroys the personal identifying information contained in the record; or (c) modifies the record to make the personal identifying information unreadable; or (d) takes actions consistent with commonly accepted industry practices that it reasonably believes will ensure that no unauthorized person will have access to the personal identifying information contained in the record. Provided, however, that an individual person shall not be required to comply with this subdivision unless he or she is conducting business for profit.

NY GEN. BUS. § 399-h (McKinney 2010).

The other type of data destruction simply mandates the use of a disposal system that meets a reasonableness standard.[231] Maryland's law, for example, states that:

> [W]hen a business is destroying a customer's records that contain personal information of the customer,[232] the business shall take reasonable steps to protect against unauthorized access to or use of the personal information, taking into account: (1) The sensitivity of the records; (2) The nature and size of the business and its operations; (3) The costs and benefits of different destruction methods; and (4) Available technology.[233]

Regardless of which form of data destruction law the Ohio adopts, there is considerable value in requiring firms to destroy unwanted medical information. As Better Business Bureau CEO Director Michelle Corey stated, "[s]tudies show that most thieves obtain personal information through trash cans or unsecured places in the home or office, and the easiest way to protect identity is to shred personal documents."[234]

D. Ohio's Data Breach Notification Law Should Be Amended to Give Residents a Method of Recovering Monetary Awards Against Covered Entities That Violate Ohio's Law

Ohio's data breach law should be amended to give citizens some mechanism to recover monetary awards when a business violates the law and the citizen is injured as a result of the violation. The mechanism to recover should be either a civil action brought directly by the citizen against the healthcare provider or a civil action brought by the attorney general entitling a citizen harmed by the statutory violation to a portion of the monetary penalty.[235]

Ohio residents should be able to bring private lawsuits under the amended statute. There are a number of states that allow private causes of action under their data breach notification statutes.[236] These civil actions provide an incentive for

---

[231] States that have adopted this form of record destruction include: Arkansas, Colorado, Illinois, Maryland, Nevada, North Carolina, Oregon, Utah, and Washington. *See* Scott & Scott LLP, *supra* note 228.

[232] Customer means an individual residing in the State who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business. MD. CODE ANN., COM-LAW § 14-3502(a) (LexisNexis 2010).

[233] MD. CODE ANN., COM. LAW. 14-3502(b) (LexisNexis 2009).

[234] Press Release, Ill. Att'y Gen. Lisa Madigan, Madigan Co-Sponsors "Shred Day" to Help Eliminate ID Theft (Mar. 29, 2006), http://www.ag.state.il.us/pressroom/2006_03/20060329.html.

[235] For example, if a healthcare provider does not notify an individual that their personal information was accessed in a breach, and as a result of that breach the citizen's medical identity is stolen, the person should be able to recover from the healthcare provider who violated the statute.

[236] In the District of Columbia, "[a]ny District of Columbia resident injured by a violation of this subchapter may institute a civil action to recover actual damages, the costs of the action, and reasonable attorney's fees." D.C. CODE § 28-3853(a) (2010). "Actual damages shall not include dignitary damages, including pain and suffering." *Id.* In Louisiana, "[a] civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the

corporations to comply with data breach laws by exposing them to financial penalties.[237] The result is that many corporations have strengthened their compliance programs to reduce the potential for violations.[238]

As displayed in other areas of regulation, specifically environmental protection, civil actions are effective tools in enforcing statutory requirements. In environmental regulation, "no program of environmental protection is better than its enforcement system."[239] A primary concern of environmentally regulated entities is avoiding liability.[240] Under the environmental regulation system, companies are potentially liable to the Environmental Protection Agency (EPA), state regulatory agencies, and private citizens,[241] who can bring toxic tort, nuisance, or other types of actions against the business.[242] The EPA enforcement policy, for instance, calls for penalties equal to the economic benefit the violator enjoyed, multiplied by a gravity

---

disclosure of a person's personal information." LA. REV. STAT. ANN. 51:3075 (2010). In Tennessee, "[a]ny customer of an information holder who is a person or business entity, but who is not an agency of the state or any political subdivision of the state, and who is injured by a violation of this section, may institute a civil action to recover damages and to enjoin the person or business entity from further action in violation of this section." TENN. CODE ANN. § 47-18-2107(h) (2009). "The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law." *Id.*

[237] *See generally* John S. Moot, *Compliance Programs, Penalty Mitigation and the FERC*, 29 ENERGY L. J. 547 (2008).

[238] *See id.* Generally, a duty-based liability induces firms to undertake optimal policing measures such as monitoring, investigating, and reporting. Jennifer Arlen & Reiner Kraakman, *Controlling Corporate Misconduct: An Analysis of Corporate Liability Regimes*, 72 N.Y.U. L. REV. 687, 694 (1997). However, it presents weaker incentives to adopt preventative measures because of the difficulty of determining ex post whether the duty has been met. *Id.* at 705.

[239] Matthew D. Zinn, *Policing Environmental Regulatory Enforcement: Cooperation, Capture, and Citizen Suits*, 21 STAN. ENVTL. L. J. 81, 82 (2002). Most regulatory agencies prefer to work informally with violators: bargaining with them or helping them reach voluntary compliance rather than punishing their noncompliance in formal administrative or judicial actions to deter future violations. *Id.* at 83. Each citizen suit is an opportunity for oversight of the regulatory enforcement process. *Id*. at 84.

[240] *See* Allison F. Gardner, *Beyond Compliance: Regulatory Incentives to Implement Environmental Management Systems*, 11 N.Y.U. ENVTL. L.J. 662, 668 (2003).

[241] Under the Resource Conservation and Recovery Act Section 7002, citizens are authorized to bring enforcement actions against potential or actual violators and against the Environmental Protection Agency in federal district court. *RCRA Enforcement Process and Authorities*, ENVTL. PROT. AGENCY, http://www.epa.gov/oecaearth/civil/rcra/rcraenfprocess.html (last updated May 18, 2010).

[242] 40 C.F.R. 254.1 (2010). "The Solid Waste Disposal Act . . . authorizes suit by any person to enforce the Act." *Id.* These suits may be brought where there is alleged to be a violation by any person of any permit, standard, regulation, condition, requirement, or order which has become effective under the Act, or a failure of the Administrator to perform any act or duty under the Act, which is not discretionary with the Administrator. *Id*. These actions are to be filed in accordance with the rules of the district court in which the action is instituted. *Id.*

component based on the severity and blameworthiness of the violation.[243] There are clear indicators that adversarial enforcement of environmental regulations discourages targeted regulated entities from violating the law.[244] While cooperative enforcement, which eschews penalties altogether, results in a minimal material incentive for companies to avoid noncompliance.[245]

In addition to the incentive that private lawsuits would give healthcare providers to comply with Ohio's data breach notification law, Ohio residents need a cause of action under the amended statute because common law suits with regard to data breaches have been widely unsuccessful.[246] Ohio, like other states, provides for administrative enforcement of its data security law but does not bar relevant common law causes of action by private citizens.[247] While the statute allows for common law actions, it does not allow a citizen to use the statute itself as a source for duty or liability in civil cases.[248] Many lawsuits have emerged in the last decade from citizens filing common law civil actions seeking damages from businesses that lost their personal information. While all of these suits have involved data breaches and regular identity theft, they provide insight into how courts will likely deal with future common law actions concerning medical identity theft.

Generally, when citizens bring a lawsuit, it is under one of three causes of action: breach of contract, negligence, or breach of fiduciary duty.[249] It has been suggested

---

[243] *See* Envtl. Prot. Agency, Policy on Civil Penalties (Feb. 16, 1984), *available in* 17 Envtl. L. Rep. (Envtl. L. Inst.) 35,083 (1987). The adversarial approach's goal is to establish a credible punitive response that produces specific and general deterrence through the systematic imposition of penalties. *See* Zinn, *supra* note 239, at 88. Imposing penalties eliminates the economic benefit a firm derives from noncompliance and makes noncompliance more expensive than compliance. *See id*.

[244] *See id.* at 96.

[245] *See id*. at 97.

[246] *See generally* Key v. DSW Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006). The court determined that the plaintiff lacked standing to sue. *See id.* The class action lawsuit failed because the court noted that any named plaintiffs, who represent a class, must allege and show that they personally have been injured, not that injury has been suffered by another, unidentified member of the class to which they belong and which they purport to represent. *Id.* at 687. The complaint failed because the plaintiff did not personally experience any injury other than an increased risk of identity theft or other related financial crimes. *Id.* at 688. Furthermore, the plaintiff lacked standing because the alleged injury is dependent upon the perceived risk of future actions of third parties that were not before the court. *Id.* at 689.

[247] *See* OHIO REV. CODE ANN. § 1349.192(A)(1)(c) (West 2010). "The rights and remedies that are provided under this section are in addition to any other rights or remedies that are provided by law." REV. CODE ANN. § 1349.192(C) (West 2010). The first major hurdle that potential plaintiffs need to overcome is to show that they have standing to sue in the first place. To have standing a plaintiff must meet three requirements. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992). First, a plaintiff must demonstrate that he has suffered an injury in fact, which is actual, concrete, and particularized. *Id*. Second, the plaintiff must show a causal connection between the conduct complained of and the injury. *Id*. Finally, the plaintiff must establish that the injury will be redressed by a favorable decision. *Id.*

[248] *See* Pinson, *supra* note 22, at 41.

[249] An underlying theme that evolves from all the cases that deal with this topic is that injury is an extremely difficult element to prove. Often times, plaintiffs advance the cost of

that the breach of contract is the best basis to bring a data breach claim; however, this cause of action almost always leaves victims with little or no recourse.[250] This is because it is difficult, if not impossible to discover, let alone prove with a legal certainty, which organization was responsible for losing the personal information that caused the identity theft.[251] Additionally, compensable damages are an element of a breach of contract cause of action and these can also be very difficult to establish in an identity theft context.[252]

Citizens seeking recovery under a negligence theory are also unlikely to receive favorable rulings. In a negligence action, a plaintiff must prove the following elements to recover damages: (1) existence of a legal duty; (2) breach of that duty; (3) causation of harm due to the breach; and (4) resulting damages.[253] The biggest hurdle in making a prima facie case for negligence is proving that the individual has been harmed. Courts have held that time spent correcting a case of identity theft, the increased threat of identity theft,[254] and the cost of credit monitoring systems[255] are not compensable injuries. Causation may also be equally difficult to prove.[256]

---

credit monitoring as an injury. They also assert that the cost of future monitoring is an injury that deserves compensation. Courts often reject these arguments by comparing future health monitoring in the toxic tort context and future financial health monitoring in the data breach context. For example, in *Stollenwerk v. Tri-West Healthcare Alliance*, the court noted that future health monitoring is as sufficient injury because it necessarily and directly involves human health and safety and credit monitoring cases do not. Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906, at 4 (D. Ariz. Sept. 6, 2005). It is this public health interest that justifies departure from the general rule that enhanced future risk of injury cannot form the sole basis for a negligence action. *See* Amfrac Distrib. Corp. v Miller, 673 P.2d 792, 793-94 (Ariz. 1983). As a side note, courts may consider an exception with regard to the effects of medical identity theft; however, this theory is untested in the medical identity theft context.

[250] Darrow & Lichtenstein, *supra* note 20, at 28.

[251] *See* Kathryn E. Picanso, *Protecting Information Security under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 377 (2006); *see also* Bell v. Acxiom Corp., 2006 U.S. Dist. Lexis 72477 *10 (E. D. Ark. Oct. 3, 2006) (plaintiff's complaint was dismissed because the plaintiff did not know whether her name and information was contained within the databases stolen).

[252] *See* McCalment v. Eli Lilly & Co., 860 N.E. 2d 884, 894 (Ind. Ct. App. 2007). For example, in *Pisciotta v. Old National Bancorp*, the plaintiffs could not recover on their breach of contract claim because of their failure to establish compensable damages. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 639-40 (7th Cir. 2007). The court noted that without more than allegations of increased risk of future identity theft, the plaintiffs had not suffered a harm that the law was prepared to remedy. *Id*. at 639.

[253] Nye v. CSX Transp., Inc., 437 F.3d 556, 563 (6th Cir. 2006). The threat of future harm, not yet realized, will not satisfy the damage requirement. Guin v. Brazos Higher Educ. Serv. Corp., 2006 WL 288483 at 5 (D. Minn. Feb. 7, 2006). The defendant's motion for summary judgment was granted in the case because the plaintiff failed to show that he himself was victim of identity theft or some other fraud. *Id*. at 5-6. The court held that the negligence action could not be sustained. *Id*.

[254] In the identity theft context, courts have embraced the general rule that an alleged increase in risk of future injury is not an actual or imminent injury. Consequently, courts have held that plaintiffs lack standing, or have granted summary judgment for failure to establish damages in cases involving identity theft or claims of negligence and breach of confidentiality

Breach of fiduciary duty has not provided a viable cause of action for victims either. For a breach of fiduciary duty claim to be effective, the victim must prove that entrusting the data collector with personal information creates a quasi-fiduciary relationship that is more similar to an agency relationship than to an arm's length relationship.[257] As a fiduciary, it could be argued that the data collector assumed the duty to act for the benefit of the consumer with respect to matters within the scope of the relationship.[258] This duty includes the duties of loyalty, trust, and confidentiality.[259] This cause of action is largely untested and there is room for further consideration.[260] However, when the cause of action is used, the plaintiff still must establish an injury, which, as already discussed, can be extremely difficult.[261]

While is it clear that most common law civil actions with regard to data breach fail because the plaintiff cannot prove damages, there will be cases where the plaintiff is a victim of medical identity theft and can prove damages. When a suit like this arises, rather than leaving the damages award up to a jury based on a common law action, the more reasonable approach would be to allow individual citizens to sue under the Ohio data breach notification statute. Like California's statute,[262] Ohio's statute could set the monetary penalties to be awarded to a plaintiff

---

brought in response to a third party theft or unlawful access to financial information from a financial institution. *Key*, 454 F. Supp. 2d, at 689; *see* Giordano v. Wachovia Sec., 2006 U.S. Dist. Lexis 52266 at 1 (D. N.J. July 31, 2006).

[255] The cost of measures to avoid identity theft fraud, courts typically have found these efforts not to be harms themselves, but merely voluntary actions taken in anticipation of potential harm. James Graves, *"Medical" Monitoring for Non-medical Harms: Evaluating the Reasonable Necessity of Measurers to Avoid Identity Fraud After a Data Breach*, 16 RICH. J.L. & TECH. 2, 8 (2009). In other contexts medical monitoring damages allow recovery of costs of medical tests designed to detect and prevent the onset of diseases resulting from the defendant's actions. *Id*. at 12. Plaintiffs have sought damages for the cost of monitoring the long-term effects of physical injuries, pharmaceuticals, tobacco, insecticides, asbestos, and other harmful substances. *Id*. Courts are reluctant to extend this judicial principal to non-physical injuries. *Id.* at 27.

[256] One court noted that as a requirement to a negligence action, the plaintiff must show that there is evidence that the thieves or other unauthorized individuals were able to access the information or if accessed that it would be used for unlawful purposes. *See* Kahle v. Litton Loan Servicing LP, 486 F. Supp. 2d 705, 712-13 (S. D. Ohio 2007). This shows that the plaintiff must know, and prove legal certainty, which organization lost the information and the unlawful purposes the information was in. *See id.*

[257] *See* RESTATEMENT (THIRD) OF AGENCY § 8.01 (2006).

[258] See RESTATEMENT (SECOND) of TORTS § 874 cmt. a (1979).

[259] *See id.*

[260] *See generally* Brandon Faulkner, *Hacking into Data Breach Notification Laws*, 59 FLA. L. REV. 1097, 1122 (2007).

[261] Shafran v. Harley-Davidson, Inc., 2008 U.S. Dist. Lexis 22494, 8 (S.D.N.Y. Mar. 24, 2008) (plaintiff's breach of fiduciary duty among other causes of action failed for failure to show damages).

[262] In California, a private citizen can file suit "for a willful, intentional, or reckless violation" of California's data breach statute and recover a civil penalty up to $3,000 per violation. *See* CAL. CIV. CODE § 1798.84(c) (West 2009). The citizen may also sue to enjoin

who brings a successful action. Lawsuits under the statute are the best for both parties. Healthcare providers are protected because a victim must still have standing to bring suit and the maximum potential award the provider would be responsible for is already set. Consumers are protected because they would have direct access to monetary recovery from a healthcare provider and the statute provides the standard of care to show that the healthcare provider acted either negligently or willfully.

Even if Ohio does not allow for private civil actions under the statute, it should allow Ohio residents to access the awards earned by the Ohio Attorney General through suits brought under the Ohio amended data breach notification law and HIPAA. Under Ohio's current law, the attorney general has the exclusive authority to bring a civil action in a court of common pleas.[263] Even though an individual may have filed the complaint with the Ohio attorney general that provided the basis to file suit, the current statute does not provide that individual access to the civil award. Ohio should adopt a policy similar to the plan articulated in the HITECH Act,[264] where citizens receive a portion of the penalties received as a result of their complaint to the attorney general. This access to attorney general monetary recoveries is important because it is extremely difficult for an individual citizen to bring a successful private action. Additionally, some financial injuries to certain medical identity theft victims may be so small that the cost of a lawsuit may make litigation unfavorable. When the attorney general files lawsuits on behalf of similarly situated individuals, those individuals should have direct access to the awards to compensate for their injuries, no matter how small. After all, the role of the Ohio Attorney General is not to make money exclusively for his own office. His role is to "protect Ohio families from predatory financial practices through [its] enforcement authority in the areas of consumer protection, antitrust, charitable organizations, and *health care fraud*."[265]

Amending the statute to allow Ohio residents access to monetary recovery does raise concerns about the effect it will have on healthcare providers. These entities already spend money on data breach prevention and data breach remediation. The remediation costs include printing and postage of notification letters, hiring a law firm to address legal issues, offering credit monitoring subscriptions to customers,

---

any business that violates or proposes to violate the statute. *See id*. § 1798.84(e). When the citizen wins the lawsuit, he is entitled to recover his or her reasonable attorney's fees and costs. *See id*. § 1798.84(g).

[263] *See* Richard Cordray, *Security Breaches and Compromise of Personal Information For Ohio Businesses*, OHIO ATT'Y GEN. (2009), http://www.ohioattorneygeneral.gov/files/Publications/Publications-for-Victims/Identity-Theft-Information/Business-Breach. If it appears that a person has failed or is failing to comply with the Act's requirements, a court, upon a finding of such failure, should impose a civil penalty of a specified amount per day for each day the person fails to comply with the Act. *Id*

[264] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13410(a), 123 Stat. 115 (2009).

[265] OHIO ATTORNEY GEN., *About the Ohio Attorney General*, OHIO ATT'Y GEN., http://www.ohioattorneygeneral.gov/getattachment/aa8e59f3-6ecc-485f-b8fe-a344821d06a5/About-the-AG-Brochure.aspx (last visited February 16, 2010) (emphasis added).

customer defections,[266] and implementing a customer support hotline.[267] Healthcare providers may argue that being subjected to additional litigation imposes too much of a cost. However, the purpose of data breach notification statutes is to increase the standards of data security and ensure notice to the public when these systems are breached. Litigation simply sheds light on contested administrative practices and decisions, bringing such practices to the attention of legislative oversight.[268]

In opposition to further consumer access to monetary penalties for statutory violations, companies also offer an alternative to adversarial enforcement. The alternative is that firms may use self-regulated notifications as a market differentiator.[269] In other words, if data breach notification is important to consumers, the market will respond accordingly favoring firms with stricter notification policies.[270] As an alternative, voluntary compliance can be very effective with providers who are motivated to establish adequate data breach systems because this strategy seeks to avoid conflict and reduces the cost associated with enforcement.[271] Unfortunately, this plan fails to address a major concern in the fight against data breaches. It offers no solution for less-motivated providers where voluntary compliance schemes without penalties can result in a lack of corporate commitment to comply with the privacy standards putting consumers at risk.[272] This purely economic model should be rejected because it provides no regulatory authority to the state government, which has an interest in protecting its citizens.

VI. CONCLUSION

Time will tell if HIPAA's 2009 amendments will provide the incentive covered entities need to protect personal health information better. However, time is a commodity that patients and consumers don't have. Every day, there are more and more victims of medical identity theft. This note in no way, shape, or form

---

[266] Customer defection means losing business. *See* Total Quality Management, *Customer Focus and Satisfaction*, September 12, 2008, http://totalqualitymanagement.wordpress.com/2008/09/12/customer-focus-and-satisfaction/. It occurs when unhappy customers decide to stop hiring a company or purchasing a company's services or products. *See id.* Customers also decide to find some other suitable alternative that satisfies their needs. *Id.*

[267] Robert Westervelt, *Survey: Data Breach Costs Surge* (Oct. 31, 2006), http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1227119,00.html. The study consisted of 31 companies and each company revealed losses ranging from less than $1 million to more than $22 million in 2006 because of data breaches. The survey noted that costs can be "borne primarily by marketing to avoid customer turnover and customer support." *Id.*

[268] *See* Harold J Krent, *Explaining One-Way Fee Shifting*, 79 VA. L. REV. 2039, 2047 (1993). "Most individuals will bring suit only when they can expect to receive relief sufficient to compensate them for the expense and risk of litigation." *Id.* at 2048. "Litigation to enforce statutory and constitutional rights may benefit a wide swath of society, even when the stakes for any one individual are too small to prompt suit. *Id.*

[269] *See* Romanosky et. al., *supra* note 23, at 3.

[270] *See id.*

[271] *See* Murphy, *supra* note 205, at 184-85.

[272] *See id.* at 185.

encourages Ohio's legislature to jump haphazardly into creating statutes to give the appearance that it cares about the privacy of its resident's health information. However, the legislature should strongly consider all of the interests involved and conduct further research to determine the best proactive course of action. After all, Ohio's constitution conveys that "[w]e, the people of the State of Ohio, [are] grateful to Almighty God for our Freedom, to *secure its blessings and promote our common welfare*."[273] It would be illogical to conclude that the intent of this constitutional mandate was for the state legislature to punt its responsibilities to protect Ohio citizens to the federal government.

[273] OHIO CONST. pmbl.