**No. 16-7108**

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

---

CHANTAL ATTIAS, Individually and
on behalf of all others similarly situated,
et al.
Appellants,

v.

CAREFIRST, INC., *et al.*,
Appellees.

---

On Appeal from the United States District Court
for the District of Columbia, Civil
1:15-cv-882 (CRC)
Hon. Christopher R. Cooper

---

# AMICUS BRIEF OF THE NATIONAL CONSUMERS LEAGUE

---

Tracy D. Rezvani (#49685)
**The Rezvani Law Firm LLC**
199 E Montgomery Avenue, Suite 100
Rockville, MD 20850
Phone: (202) 350-4270 x 101
Fax: (202) 351-0544
tracy@rezvanilaw.com

## CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rule 28(a)(1), *Amicus Curiae* National Consumers League ("NCL") certifies that:

### A. Parties, Interveners, and Amici

#### 1. Parties and Amici

| | |
|---|---|
| Plaintiffs-Appellants: | Chantal Attias, Individually and on behalf of all other similarly situated |
| | Andreas Kotzur, Individually and on behalf of all others similarly situated |
| | Richard Bailey, Individually and on behalf of all others similarly situated |
| | Latanya Bailey, Individually and on behalf of all others similarly situated |
| | Curt Tringler, Individually and on behalf of all others similarly situated |
| | Connie Tringler, Individually and on behalf of all others similarly situated |
| | Lisa Huber, Individually and on behalf of all others similarly situated |
| Defendants-Appellees: | CareFirst, Inc. |
| | Group Hospitalization and Medical Services, Inc. |
| | CareFirst of Maryland, Inc. |
| | CareFirst BlueChoice |
| Amicus on behalf of Plaintiffs-Appellants: | National Consumers League |

**B. Ruling under Review**

References to the ruling at issue appear in the Corrected Brief of Appellants.

**C. Related Cases**

The case on review has not previously been before this Court or any other court.

NCL is not aware of any related cases as defined by D.C. Circuit Rule 28(a)(1)(C).

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

## Cases



## Other Authorities

## CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 28(a)(2), *amicus curiae* states that the National Consumer League is a non-profit membership organization exempt from taxation pursuant to Section 501(c)(3) of the Internal Revenue Code, and is not a publicly held corporation that issues stock. It has no parents, subsidiaries, or stockholders.

## IDENTITY AND INTEREST OF *AMICUS*

The National Consumers League ("NCL"), founded in 1899, is the nation's oldest consumer organization. The NCL has a recognized history of contributing as an *amicus curiae* in cases that impact public policy dating back to when future Supreme Court Justice Louis Brandeis filed the first "Brandeis brief" in 1908 on behalf of the NCL in *Muller v. Oregon*, 208 U.S. 412 (1908), a landmark Supreme Court case that upheld restrictions on working hours of women.

The mission of the NCL is to protect and promote social and economic justice for consumers and workers in the United States and abroad. The NCL is a non-profit advocacy group representing consumers in marketplace and workplace issues. On behalf of the general consuming public, the NCL appears before legislatures, administrative agencies, and the courts on a wide range of issues, and works for the enactment and effective enforcement of laws protecting consumers.

The NCL also educates consumers on ways to avoid fraud in the marketplace through its National Fraud Center.

Of relevance to this underlying litigation, the NCL regularly educates consumers regarding the importance of data security and the perils of identity theft including credit, tax and medical identity theft.[1] In fact, as one of its Policy Statements,[2] the NCL advocates for health information privacy as well as related safeguards and security for all health data.

## SUMMARY OF ARGUMENTS

Corporate America's increasing use of digitized data, and of personally identifiable information ("PII") and personally identifiable health information ("PHI") requires courts to re-evaluate how it analyzes legal concepts. When there is a hack of digitized data, the greatest burden tends to fall not on companies who gather this data and improperly secure it, but on consumers who are far less able to bear the financial liability and responsibility for keeping that data safe. In fact, although consumer data in its digitized form has significant value to businesses, and although businesses promise to protect this data – data which consumers are often required to supply - they too often throw the burden onto the consumer after a breach, including the cost and responsibility to re-secure the data. This occurs

[1] http://www.fraud.org/identity_theft
[2] http://www.nclnet.org/policy_statements

even though consumers have no ability to (a) protect the data once it is provided or (b) affect the business's data security policies. In other words, consumers who have no control over data security are often held responsible for the aftermath when the lax security inevitably fails. The law has been slow to catch up with technology; but catch up it must.

## ARGUMENT

### A. The Real Risk of Medical Identity Theft

Medical identity theft, a term coined by Pam Dixon of the World Privacy Forum, is a sub-species of the identity theft crime, has doubled in the last five years—reaching nearly 500,000 cases a year. *See* Ponemon Institute, Fifth Annual Study on Medical Identity Theft, at 7-8 (Feb. 2015); Testimony of Pam Dixon, Executive Director, World Privacy Forum, Before the U.S. Senate Committee on the Judiciary, Subcommittee on Privacy, Technology, and the Law, Data Brokers-Is Consumers' Information Secure?, at 2 (Nov. 3, 2015). It occurs when someone uses an individual's name and personal identity to fraudulently receive medical services, prescription drugs and/or goods, and includes attempts to commit fraudulent billing. Ponemon at 1; Federal Trade Commission, Medical Identity Theft, FAQs for Health Care Providers and Health Plans, at 1.

Victims of privacy breach and identify theft "estimate[d] the total value of all charges on fraudulent accounts in their name" at $87,303 on average. *See* Soma,

et al., *Corporate Privacy Trend: The "Value" Of Personally Identifiable Information ("PII") Equals The "Value" Of Financial Assets*, 15 Rich. J. L. & Tech. 11, *44 (Spring 2009). Moreover,

> resolution of privacy breaches takes the consumer significant time and funding. While it is estimated that the consumer spends ninety-seven hours to repair the damage when an existing account has been used to affect fraud, if a new account has been created in the victim's name, resolution of the breach skyrockets to 231 hours. In 2006, the average consumer's out-of-pocket costs to resolve breaches for existing or new accounts averaged $1,884 and $1,342 respectively. Not surprisingly, "theft or loss of personal and financial information is the No. 1 concern of consumers worldwide (64 percent)."

Soma, at *44; *see also* Ponemon at 2-3 (200 hours for 2015 study); Michelle Andrews, The Rise of Medical Identity Theft, Consumer Reports (Aug. 25, 2016).

A consumer's medical health insurance is valuable and vulnerable. When it gets into the wrong hands it can be used to steal expensive medical services—even surgeries—and prescription drugs or to procure medical devices or equipment such as wheelchairs. Andrews, *supra*. A consumer's medical identity is a commodity that can be hijacked and used to falsify insurance claims or fraudulently acquire government benefits such as Medicare or Medicaid. *Id.; see also*, §B, *infra.* A person's medical information may also be sold on the black market, where it can be used to create entirely new medical identities. Andrews, *supra*.

Medical identity theft is a greater "sleeper" crime than credit account breaches. Unless and until the medical bills show up through debt collection, the police show up for prescription drug abuse arrests, medical care is denied due to a non-existent condition, or loans or jobs are denied, a consumer is generally unaware of the violation. Ponemon, at 3, 12, 16; *see also* Andrews, *supra*; FTC FAQs at 1; Laura Shin, What's Behind the Dramatic Rise in Medical Identity Theft?, Fortune (Oct. 19, 2014); Identity Guard, 3 Ways Patients are at Risk for Medical Identity Theft (June 12, 2106). For this reason, 80% of consumers would want reimbursement for money spent mitigating future harm and damages. Ponemon at 7.

While credit card or Social Security numbers from a medical file have obvious value for basic financial fraud, thieves also sell the medical information. Shin, *supra*. The thief could steal the file and sell the Social Security number, *and then* sell other useful parts of the file to others: almost like laundering the information or stripping cars for parts. For example, a medical file's PII (Social Security number and other financial information) is sold directly to one type of "customer" on the black market. The rest of the patient data, goes to another "customer" on the black or grey market. For example, information on cancer diagnosis and treatments can be sold on the grey market which eventually will reach data brokers who sell it to marketers such as pharmaceutical companies or

hospitals that want to target those with cancer. *Id.* This is the best case scenario. The worse case scenario is that medical data is used to foster a more complete (and false) profiles for visas and passports. *Id.*

**B. Liability Should be Borne by those who Demand the Data**

As Professor Daniel J. Solove noted "[d]ata security is quickly becoming one of the major concerns of the Information Age." Daniel J. Solove, The New Vulnerability: Data Security and Personal Information.[3] Recent events on the world stage have underscored the vital importance of data security and the fallout suffered by the public if security is not adequately maintained. As Solove further notes:

> Increasingly, extensive digital dossiers about us are being constructed, as businesses and the government gather pieces of personal data and assemble them in data bases. Hundreds—perhaps thousands—of entities may have our personal information. Our dossiers play a profound role in our lives. …Because so many critical decisions are based on our dossiers, ensuring that they are accurate and protected from tampering is of paramount importance.

*Id.* at 111.

Corporate America's increasing dependence on digitized data necessitates a re-examination of not only of traditional conceptions of corporate assets but of

[3] Found in SECURING PRIVACY IN THE INTERNET AGE (Radin & Chander, eds., Stanford University Press 2008)(Chapter 6, p.111).

traditional conceptions of Article III standing. *See* Soma, at *1. PII and PHI, which companies obtain at little cost, has quantifiable value that is comparable to the value of traditional financial assets. *Id.* Yet while corporations may realize the importance of data security, the steady rise of data breaches suggests that the decision makers who form internal policies for these companies have yet to grasp a fundamental reality of the modern business world. *Id.* at *3. Namely, individuals who own the data stored by business have a right to "informational privacy," which is defined as a "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." *Id.* at *7.

The companies who demand the PII and PHI in digitized form do so because it has value *in that form*. It is simpler and cheaper to store, simpler and cheaper to manipulate, and simpler and cheaper to generate the myriad of decisions required based on that data. *Id.* at *10-11 ("The difference in cost between paper and electronic insurance claim processing illustrates the enormous savings the electronic alternative provides…. the cost of processing an electronic claim is $0.25 to $0.75--a fraction of the $2 to $12 cost of processing the same claim using paper."). In addition to the cost saving value of digitized data, consumer information in digital form has additional value as a source of marketing. *Id.* at *14-15 ("PII, if used properly, can generate legitimate profits that require very

little input."). Whether reselling the data or using it for personalized advertising, companies like Respondent use PII and PHI to obtain and then retain their consumers. *Id.* at *12-13. For these very reasons, it is appropriate to view digitized data demanded by companies as a commodity.[4] *Id.* at *14. "The potential for increased profits and cost savings serve as a substantial impetus for companies to ensure their actions do not compromise access to this valuable resource." *Id.* *15. In fact, over a decade ago, even before the surge of data brokers marketing on consumer data worldwide,[5] the market for personal information was estimated to be $1.5 billion per annum. Christopher F. Carlton, The Right to Privacy in Internet Commerce: A Call for New Federal Guidelines and the Creation of an Independent Privacy Commission, 16 ST. JOHN'S J. LEGAL COMMENT. 393, 405 (2002). For this reason, implementing effective safeguards to protect against abuses in digital information is also critical to the success of Internet commerce. *See id.* at 406.

[4] And this commodity has real value to thieves. In 2006, "a consumer's address can be purchased for 50 cents, an unpublished number for $17.50, a Social Security number for a mere $8, and so on." Luis Salazar, Part I: Technology Explosion Creates Personal Privacy Tensions, 25 AM. BANKR. INST. J. 18, 18 (Nov. 2006). In fact, in 2010, Symantec Corporation's Norton brand created a software application that valued a person's identity on the black market.

[5] For an article describing the role of data brokers and aggregators in the medical field, *see* ID Watchdog, An Obscure Data Broker is Selling Your Medical Secrets (May 26, 2016); *see also* Testimony of Pam Dixon, *supra*.

As corporate America becomes more dependent upon the electronic use of PII and PHI, and as the costs of failing to protect that information rise, the internal decision makers must accept the reality that data management and protection demands a greater allocation of company resources. Soma at *21. Concomitant with this realization has to be the allocation of liability and risk onto the actors who demand the commodity as a condition of doing business. The alternative is what currently prevails in the marketplace: corporate America demanding consumer data in a manner most profitable to them, while providing lax security and then placing the burdens of re-securing informational privacy on the hapless consumer. This fundamental unfairness cannot be underscored. Respondent, and similar corporations, are in the best, and frankly in the *only*, position to protect this commodity *and* the informational privacy interests of the individuals to whom the information belong. *Id.*at *9. It is clear, therefore, that the leaders of corporate America must acknowledge the real value of PII and PHI by proactively protecting against the threats posed to data and respecting an individual's privacy interest in such information. *Id.* at *48. Yet the trial court, limiting standing concepts to a different age, dismissed the underlying case and placed the burden on consumers to secure information held by third-parties—information these very same third-parties promised to protect.

Placing the burden and liability on the entity holding, controlling, and promising its security is the appropriate response. Moreover, there is plenty of precedent to support such a finding. Solove, at 122; *see also id.* at 129-30 & n. 106 (discussing *Whalen v. Roe*, 429 U.S. 589 (1977) and progeny which find duty to protect consumer data and informational privacy by the data collector).

### C. Traditional Common Law Concepts are Flexible to Reach Informational Privacy

The bridge between traditional tort and privacy law is incomplete. Soma, at *33. Not enough thought has been given to how the law should understand and address these problems. Solove, at 112. Frequently, the misuse of personal information is often viewed by trial courts as a technology problem. *Id.* Yet

> technology is not the root cause of many abuses of personal information. Misuse, but at the core, the problem stems from a set of business and government practices. The problem is caused in significant part by the law, which has allowed the construction and use of digital dossiers without adequately regulating the practices by which companies keep them secure. The shift to a digital environment certainly facilitates information companies readily disseminate the personal information they have collected to a host of other entities and sometimes even to anyone willing to pay a small fee. … Even a fortress with impenetrable walls is hardly secure if the back gate is left open.

Solove, at 112-13. The law is slow to change and, to a great extent, fails to focus on the causes of information abuses; to identify all the responsible parties; and to fashion appropriate remedies to respond to these abuses. *Id.* at 113. As here, the

responsibility for protecting data demanded by merchants, stored by those merchants, and promised to be protected by those merchants, is left entirely to the consumer *who has no control over* the merchant's internal security controls. *See* Solove, at 121 ("the collectors and users of our personal information are frequently not accountable to us. Information is gathered and used, and we have little knowledge about and ability to control how secure it remains.").

Professor Solove points out that "data abuse" comes in three forms:[6]

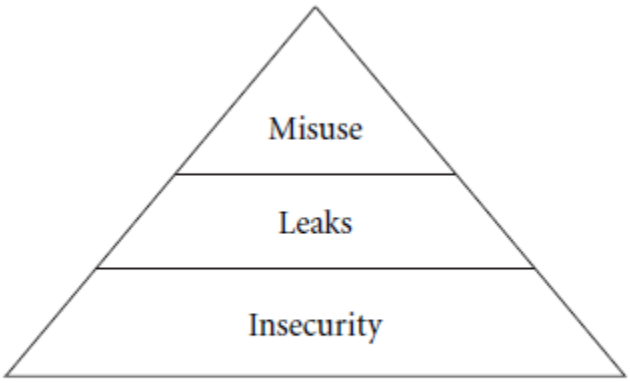


**Figure 6.1.** The data abuse pyramid.

The law currently attempts to respond to actual misuses of information. *Cf.* Solove at 115 *with e.g. Stollenwerk v. Tri-West Health Care Aliiance*, 254 Fed. Appx. 664, 667-68 (9th Cir. 2007), *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1323 (11th Cir.

[6] The final form of data abuse, mere insecurity due to inadequate architecture, is not an issue faced by the Court here. Although it is this insecurity that is capitalized on by criminal actors to create leaks and later misuse. Solove, at 121.

2012); *Kuhn v. Capital One Fin. Corp.*, 855 N.E.2d 790 (Mass. App. Ct. 2006); *Shames-Yeakel v. Citizens Fin. Bank*, 2009 U.S. Dist. LEXIS 75093 (N.D. Ill. Aug. 21, 2009). However, using criminal law as the main legal method to combat information abuses has thus far proven ineffective since these actors are difficult to track, often international, and have significantly more resources than government actors. *See id.* Although the injury and harm is easy to understand, the law must also recognize that a duty was breached and that this breach caused the harm. *Id.* The law often views the only culprit as the thief, the hacker, or the abuser of the data. *Id.* The companies from which the data is taken are perceived as victims themselves and therefore get a pass from the legal system. Who then is protecting consumers who have supplied the data required and get assurances that their personal information is being well protected?

Leaks, in turn, cover improper dissemination or access of consumer data—the issue posed by the underlying litigation. Solove, at 117. With a leak, the harm consists of the increased risk of exposure to identity theft (personal or medical), fraud (financial or medical), or even physical danger. *Id.* Consumers also suffer anxiety because there is little they can then do to recover the data and prevent downstream abuses of them. *Id.*

Courts, however, have had difficulty in recognizing the injury and harm, preferring to await the actual misuse (damages). *Id.* Most of the laws applied pre-

dated the Internet, computers, and even electricity. *See* Center for Democracy & Technology, Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology, 2-3 (2006) (discussing shortcomings of the law and Justice Breyer's book, *Active Liberty*, and his opinions that technology is outpacing privacy laws); Carlton, at 405 ("But the legal system has not sufficiently evolved and technological advances have made the legal protections developed over the last few centuries obsolete."). The law, no matter how old, can and should at least recognize that a company may have done something wrong when it did not safeguard property to which it was entrusted. The law should recognize that waiting until the increased risk of identity theft materializes in actual misuse, while convenient and comfortable under laws centuries old, leaves consumers holding the bag for a lax policy of protecting data. Existing legal responses to data security leave "the architecture of vulnerability unchanged." Solove, at 121. The law serves to only patch up the cracks in the surface of the "data abuse pyramid," but leaves the foundations shaky and barely supported. *See id.*

## CONCLUSION

The risk to consumers in the Information Age must be borne by those demanding the information and promising to safeguard it. Liability should be borne by those who benefit the most by having the information in digitized form. It is fundamentally unfair to consumers to bear the price (literal and metaphorical)

of corporate misdeeds when they fail to protect sensitive PII and PHI. The law is dynamic enough to recognize that a consumer is injured, suffers harm, and incurs damages when their right to information privacy is violated, the safety and security of their financial and medial identity compromised, and they are forced to spend money--out-of-pocket—to monitor the fallout from a company's breach of duty. In no other situation does the law find a breach of duty insufficient to incur standing. And in this instance, the law should finally recognize that technology does not give a "pass" to Corporate America who breach their duties.

Dated: January 26, 2017

Respectfully submitted:

/s/ *Tracy D. Rezvani*

Tracy D. Rezvani
**The Rezvani Law Firm LLC**
199 E. Montgomery Avenue, #100
Rockville, MD 20850
(202) 350-4270 x101

*Counsel for Plaintiff National Consumers League*

## CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 3995 words, *including* the parts of the brief exempted by Fed. R. App. P. 32(f).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(5)-(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2016 in Times New Roman 14 point type.

## CERTIFICATE OF SERVICE

I certify that on the 27 day of January 2017, I served a true copy of the foregoing on all counsel of record using the Court's ECF/CM system on:

Matt Gatewood
**Sutherland Asbill & Brennan LLP**
700 Sixth Street, NW, Suite 700
Washington, DC 20001

*Counsel for Carefirst, Inc., Carefirst of MD, CFBC, GHS*

Robert D. Owen
**Sutherland Asbill & Brennan LLP**
The Grace Building, 40th Floor
1114 Avenue of the Americas
New York, NY 10036

*Counsel for Carefirst, Inc., Carefirst of MD, CFBC, GHS*

*/s/ Tracy D. Rezvani*