CELEBRATING 125 Years 1890 2015

Pepper Hamilton LLP
Attorneys at Law

Client Alert

March 24, 2015

Berwyn | Boston | Detroit | Harrisburg | Los Angeles | New York | Orange County | Philadelphia | Pittsburgh | Princeton | Silicon Valley | Washington, D.C. | Wilmington

Federal Court Holds that Data Breach Plaintiffs Have No Standing Unless They Show Misuse

Jan P. Levine | levinej@pepperlaw.com, Angelo A. Stio III | stioa@pepperlaw.com
T. Stephen Jenkins | jenkinst@pepperlaw.com

Storm v. Paytime, Inc. — a recent case decided by the U.S. District Court for the Middle District of Pennsylvania — gives companies that have suffered third-party data breaches another decision to support dismissing class actions at an early stage. Coming four years after the U.S. Court of Appeals for the Third Circuit decided *Reilly v. Ceridian Corp.*,[1] *Storm* reaffirms that plaintiffs lack standing to bring data breach cases "unless plaintiffs allege actual misuse of the hacked data or specifically allege how such misuse is certainly impending."[2]

Procedural and Factual History

On June 13, 2014, Daniel Storm, along with other purported class plaintiffs, filed an action against Paytime, Inc., asserting negligence and breach of contract claims (*Storm*) for alleged injury as the result of a data breach to Paytime's computer systems on April 7, 2014.[3] Paytime, a national payroll processing services company with clients throughout the United States, entered into contracts with the *Storm* plaintiffs' employers and/or former employers for payroll processing.[4] By the nature of the contract, the plaintiffs' employers and/or former employers provided Paytime with the plaintiffs' confidential personal and financial information. As a result of the data breach, the plaintiffs alleged that third-party hackers gained access to the confidential personal and financial information[5] that was submitted to Paytime through the plaintiffs' employers.[6]

On June 27, 2014, Barbara Holt, along with other purported class plaintiffs, also filed an action against Paytime, alleging breach of contract and claims under Pennsylvania's Unfair Trade Practices and Consumer Protection Law (*Holt*) for the same data breach. Subsequently, Paytime moved to dismiss both cases.[7] After the cases were consolidated, the court dismissed the consolidated case for lack of standing.[8]

> Plaintiffs must show that their ill-acquired information was actually misused prior to bringing a data breach claim.

The Court's Holding

Although the court sympathized with the plaintiffs' data breach concerns and recognized that hacking has become commonplace,[9] the court had little trouble dismissing the consolidated case for lack of standing.[10] The court noted that data breach plaintiffs, like all plaintiffs in federal court, have the burden of establishing that they have standing to sue.[11] Judge John E. Jones ruled that the plaintiffs needed to show "personal injury [that was] fairly traceable to the defendant's allegedly unlawful conduct [and that could] be redressed by the requested relief."[12] More specifically, that injury must be "actual or 'imminent,' not 'conjectural' or 'hypothetical'."[13]

In the context of data breaches, the Third Circuit in *Reilly* held that, "in the event of a data breach, a plaintiff does not suffer a harm, and thus does not have standing to sue, unless [the] plaintiff alleges actual 'misuse' of the [plaintiff's] information, or that such misuse is imminent."[14] The *Reilly* plaintiffs sued the defendant under negligence and breach of contract theories of liability and alleged that, "due to the data breach, they were subject to an increased risk of identity theft, had incurred costs

to monitor their credit activity and suffered from emotional distress."[15] The Third Circuit, however, affirmed the district court's dismissal of the case on standing grounds because the plaintiffs' "future harm resulting from the security breach was . . . significantly attenuated . . . [and] . . . dependent on entirely speculative, future actions of an unknown third party."[16]

Similar to the *Reilly* plaintiffs, the *Paytime* plaintiffs unsuccessfully attempted to allege two forms of injury. First, the plaintiffs alleged they had to expend money to take measures to prevent identity theft after the data breach.[17] Second, the plaintiffs alleged that at least one plaintiff suffered injury due to his employer's suspending his security clearances after the data breach.[18] This plaintiff alleged that, after reporting the data breach to his employer, his employer suspended his security clearances for a period of time during which the employer investigated the situation.[19] The employer also required the plaintiff to work at a different job site that was further away.[20] Thus, the plaintiff claimed he suffered actual injury "in the form of increased commute time and related expenses."[21]

The *Paytime* court did not find either alleged injury compelling — seeing no factual distinction between the *Paytime* plaintiffs and the *Reilly* plaintiffs.[22] In regard to the alleged "increased risk of identity theft," the court held that a plaintiff must show that he or she has become an *actual* victim of identity theft to show injury.[23] Likewise, the court held that the alleged "increased commute time and related expenses" was "different in form but not in substance" from other preventive measures.[24] Because neither alleged injury was the result of misuse of the plaintiffs' data, the preventive expenditures by themselves could not constitute actual injury.

Despite the data breach, the plaintiffs were unable to allege that they suffered any actual injury as result of the data breach — such as their bank accounts being accessed, credit cards being opened in their names or Social Security numbers being used to impersonate them.[25] Therefore, the plaintiffs lacked standing. The court held that, "[a]lthough this stringent standard for standing [occasionally] leave[s] [plaintiffs] to foot the bill for their preventive measures taken," it is wise from a policy perspective.[26] With a rampant increase in data breaches, it would be unduly burdensome to allow every data breach to go forward without proof of actual identity theft or some other cognizable injury.[27] Accordingly, courts — at least in the Third Circuit — must strictly adhere to threshold of actual injury before conferring standing.

Conclusion

The *Paytime* opinion joins a list of decisions in the Third Circuit that hold that a data breach plaintiff must show that his or her ill-acquired information was actually misused prior to bringing a data breach claim. Yet, not every court adheres to such a stringent threshold. The attorneys in Pepper Hamilton LLP's Privacy, Security and Data Protection group are equipped to help you navigate the challenging issues associated with data breaches.

Endnotes

1. *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011).
2. Opinion Dismissing Consolidated Cases *Storm v. Paytime, Inc.* and *Holt v. Paytime Harrisburg* at 13, No. 14-cv-1138 (M.D. Pa. Mar. 13, 2015) [hereinafter *Paytime* Opinion].
3. *Id.* at 3, 7–8.
4. *Id.* at 7.
5. This confidential information included full legal names, addresses, bank account information, Social Security numbers and dates of birth. *Id.*
6. *Id.*
7. *Id.* at 4–5.
8. *Id.* at 3.
9. *See id.* at 2.
10. *See id.* at 17.
11. *Id.* at 10 (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)).
12. *Id.* (citing *Allen v. Wright*, 468 U.S. 737, 751 (1984)).
13. *Id.*
14. *Id.* at 11–12 (citing *Reilly*, 664 F.3d at 42).
15. *Id.* at 12 (citing *Reilly*).
16. *Id.* (internal quotations and citations omitted).
17. Although not part of its holding, the court noted that Paytime arranged to provide one year of free credit monitoring for breach victims, which meant the plaintiffs would not have to pay for "many of their reasonable preventive costs." *Id.* at 18, n. 7.
18. *Id.* at 18.

19. *Id.* at 14.
20. *Id.*
21. *Id.*
22. *Id.* at 13–14.
23. *Id.* at 16.
24. *Id.* at 18.
25. *Id.* at 14
26. *Id.*
27. *Id.* at 18–19.

Litigation Cybersecurity Practice

Sharon R. Klein	kleins@pepperlaw.com
Jan P. Levine	levinej@pepperlaw.com
Pamela S. Palmer	palmerp@pepperlaw.com
Angelo A. Stio III	stioa@pepperlaw.com
Charles E. Leasure, III	leasurec@pepperlaw.com
Tambry L. Bradford	bradfordt@pepperlaw.com
Matthew A. Chiachetti	chiachettim@pepperlaw.com
Kevin Crisp	crispk@pepperlaw.com
T. Stephen Jenkins	jenkinst@pepperlaw.com
Matthew Ladner	ladnerm@pepperlaw.com
Rebekah A.Z. Monson	monsonr@pepperlaw.com
Suzanne M. Noyes	noyess@pepperlaw.com
Eli M. Segal	segale@pepperlaw.com
William M. Taylor	taylorw@pepperlaw.com
Brian R. Zurich	zurichb@pepperlaw.com