Legal Backgrounder

Vol. 34 No. 2 February 15, 2019

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

# With First-of-its-Kind Decision, Pennsylvania High Court Identifies Common-Law Duty to Protect Digital Data

by Andrew C. Glass, David R. Fine, and Roger L. Smerage

In November 2018, Pennsylvania's highest court issued a first-of-its-kind decision in the world of data-breach law, *Dittman v. UPMC.*[1] The state's supreme court reversed a lower court's dismissal of negligence claims, holding that a common-law duty exists to protect personal or financial data stored on internet-connected computer servers. Although a few federal courts have speculated that states might impose such a common-law duty, no state appellate court—let alone a state supreme court—had ever held as much before *Dittman*. The decision could motivate state courts to impose liability for businesses' breach of a common-law duty to secure consumer and employee data. Or the Pennsylvania Supreme Court's decision could become an outlier if courts elsewhere choose to follow the contrary reasoning of other states' intermediate appellate courts that decided the issue before *Dittman*.

**Background**

The plaintiffs in *Dittman* asserted negligence claims, alleging that hackers breached their employer's computer systems and obtained personal and financial information.[2] The trial court dismissed these claims at the pleadings stage, concluding that Pennsylvania law did not impose upon the employer "a duty of reasonable care in its collection and storage of [e]mployees' information."[3] Moreover, the trial court found "that the economic loss doctrine barred" these claims.[4]

The intermediate appeals court affirmed in a split opinion.[5] After considering the factors under which courts in Pennsylvania can create new common-law duties, the majority held "that the trial court properly found that [the defendant] owed no duty to [e]mployees under Pennsylvania law."[6] The court concluded that, among other reasons, "no judicially created duty of care is needed to incentivize companies to protect their employees' confidential information because there are 'statutes and safeguards in place to prevent employers from disclosing confidential information[.]'" The court added "'[e]mployers strive to run their businesses efficiently and they have an incentive to protect employee

[1] 196 A.3d 1036 (Pa. 2018).
[2] *Id.* at 1038.
[3] *Id.* at 1041.
[4] *Id.*
[5] *Dittman v. UPMC*, 154 A.3d 318 (Pa. Super. 2017).
[6] *Id.* at 324.

**Andrew C. Glass** and **David R. Fine** are Partners, and **Roger L. Smerage** is an Associate, at K&L Gates LLP, where they practice in the Appellate Litigation and Financial Institutions and Services Litigation groups.

information and prevent these types of occurrences.'"[7] The appeals court also agreed that the economic-loss doctrine would bar the plaintiffs' negligence claims even if a duty did apply.[8]

**The Supreme Court's Decision**

The Pennsylvania Supreme Court framed the question presented to be whether the defendant had "a legal duty to use reasonable care to safeguard sensitive personal information of its employees when [it] chooses to store such information on an internet accessible computer system."[9] The court determined that the lower courts had not only reached the wrong conclusion, but that they had analyzed the issue under the wrong legal framework. Rather than consider whether this duty could be recognized as a *new* common-law duty, the court reasoned that the proper question was whether to apply "an existing duty to a novel factual scenario."[10] The court explained that "[c]ommon law duties stated in general terms are framed in such fashion for the very reason that they have broad-scale application."[11]

The court held that a general duty exists in a situation involving data security when a party engages in "affirmative conduct."[12] Specifically, parties engaged in "affirmative conduct" owe "a duty to others to exercise the care of a reasonable man to protect them against an unreasonable risk of harm to them arising out of the act."[13] The court concluded that the plaintiffs properly alleged the defendant engaged in "affirmative conduct," which triggered the general duty of reasonable care. The defendant's collection of plaintiffs' personal and financial data, as well as their decision on how to secure that data when storing it on an internet-accessible computer system, the court asserted, constituted "affirmative conduct."[14] The court reasoned that the defendant's "affirmative conduct created the risk of a data breach" such that it owed the plaintiffs "a duty to exercise reasonable care to protect them against an unreasonable risk of harm arising out of" the collection and storage of the data.[15] The "criminal acts of third parties in executing the data breach" did not relieve the defendant of this duty, the court reasoned, because such a breach was "within the scope of risk created by" the defendant's alleged "affirmative conduct."[16]

The court next considered whether the economic-loss doctrine applied, which would bar plaintiffs' claim even if a general duty of care bound the defendants. It acknowledged that the state's economic-loss-doctrine jurisprudence required "a 'reasoned approach' … that 'turns on the determination of the source of the duty plaintiff claims the defendant owed.'" That "reasoned approach" led the court to conclude that the doctrine does not "preclude[] all negligence claims seeking solely economic damages."[17] Thus, "if the duty arises under a contract between the parties, a tort action will not lie from a breach of that duty" but, "if the duty arises independently of any contractual duties between the parties, then a breach

[7] *Id.*
[8] *Id.* at 325.
[9] *Dittman*, 196 A.3d at 1043.
[10] *See id.* at 1046.
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.* at 1047.
[15] *Id.*
[16] *See id.* at 1048.
[17] *Id.* at 1054.

 

of that duty may support a tort action."[18] And, because the court concluded that the defendant's "duty to act with reasonable care in collecting and storing [plaintiffs'] personal and financial information on its computer systems … exist[ed] independently from any contractual obligations between the parties, the economic loss doctrine [did] not bar [plaintiffs'] claims."[19]

**Analysis**

*Dittman*, as noted above, is the first of its kind among state appellate courts. The few state appellate courts to address the issue prior to the Pennsylvania Supreme Court—including the intermediate appellate court in *Dittman* itself—had rejected the existence of such a broad duty.[20] Some federal courts had likewise predicted that state appellate courts would not recognize such a common-law duty.[21]

Other federal courts, however, have predicted that a state common-law duty applies to businesses' data security.[22] *Dittman* may lead more federal courts to predict that appellate courts in states where the issue is undecided would recognize some form of common-law duty to protect personal and financial data. And of course, federal courts applying Pennsylvania law are now bound by *Dittman* on the issue of a general duty to protect customer and employee data.

The parameters of the duty identified in *Dittman* will have to be established through further case-law developments. One could argue that the duty to safeguard data applies only to employment data. The court's reasoning in *Dittman* suggests that the employer-employee relationship may give rise to a distinct extra-contractual duty to secure an employee's personal and financial data.[23] Thus, an open question remains as to whether the *Dittman* duty extends to businesses' collection and storage of consumer or other non-employee data. After *Dittman*, however, businesses can expect to encounter arguments, in suits outside of Pennsylvania, that a general duty to safeguard data exists.

---

[18] *Id.*

[19] *Id.* at 1056.

[20] *McConnell v. Dep't of Labor*, 814 S.E.2d 790, 796-99 (Ga. App. 2018), *cert. granted* No. S18C1317 (Ga. Nov. 15, 2018); *Dittman*, 154 A.3d at 324; *Paul v. Providence Health Sys.-Or.*, 240 P.3d 1110, 1115-16 (Or. App. 2010), *aff'd on other grounds* 273 P.3d 106 (Or. 2012); *Cooney v. Chicago Pub. Schs.*, 943 N.E.2d 23, 28–29 (Ill. App. 2010).

[21] *See*, *e.g.*, *Cmty. Bank of Trenton v. Schnuck Mkts., Inc.*, 887 F.3d 803, 816-18 (7th Cir. 2018) (no duty under Illinois or Missouri law); *Irwin v. Jimmy John's Franchise, LLC*, 175 F. Supp. 3d 1064, 1071 (C.D. Ill. 2016) (no duty under either Arizona or Illinois law). Each of these cases, however, comes with a caveat. When *Community Bank of Trenton* was before the district court, although the court found no duty existed, it suggested that "retailers will have to act more prudently" going forward. No. 15-CV-01125-MJR, 2017 WL 1551330, at *3-4 (S.D. Ill. May 1, 2017). And in *Irwin*, the court found that the plaintiff could proceed under an implied-contract theory under Illinois law because her use of, and defendant's acceptance of, a credit card for payment implied an agreement by the defendant to safeguard the payment information in order "to effectuate the contract" to pay for goods or services. 175 F. Supp. 3d at 1070-71.

[22] *See In re Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *3-4 (N.D. Ga. May 18, 2016); *In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304, 1309-10 (D. Minn. 2014); *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 395 F. Supp. 2d 183, 193-96 (M.D. Pa. 2005) (nevertheless concluding economic-loss doctrine precluded negligence claim against co-defendant who raised that defense), *aff'd* 533 F.3d 162 (3d Cir. 2008) (affirming solely on basis of application of economic-loss doctrine without deciding issue of whether duty existed); *cf. Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421, 426 (5th Cir. 2013) (assuming, without deciding, that duty applies under New Jersey law when deciding that economic loss doctrine would not bar claim at motion to dismiss stage).

[23] *See Dittman*, 196 A.3d at 1047 (discussing the fact that duty arose in the context of data exchange that occurred "as a condition of employment").



ISBN 1056 3059

**Conclusion**

*Dittman* and the duty it identified will likely instigate an increase in data-breach lawsuits in Pennsylvania's state and federal courts. Businesses located in the commonwealth or whose employee or consumer data have a connection to Pennsylvania now face more pressure to make their computer systems and their online storage hacker proof. The litigation to come will clarify the breadth of the duty identified in *Dittman* general duty and to which data it applies. Only time will tell if *Dittman* is an outlier, or whether it will influence other state appellate courts' decisions.

* * *