STATE OF MAINE
SUPREME JUDICIAL COURT
SITTING AS THE LAW COURT

LAW COURT DOCKET NO. BCD-24-481

IN RE MOUNT DESERT ISLAND HOSPITAL DATA SECURITY INCIDENT LITIGATION

JOHN DESJARDIN, LINDEN BUZZELL, BEATRICE GRINNELL, DEREK HANNAN, NICOLE BRIGHT & ERIN WALSH,

Plaintiffs-Appellants

v.

MOUNT DESERT ISLAND HOSPITAL, INC.,

Defendant-Appellee

On Appeal from the Business and Consumer Court
Docket No. BCD-CIV-2023-00070

APPELLANTS' REPLY BRIEF

Peter L. Murray, ME Bar #1135
Richard L. O'Meara, ME Bar #3510
75 Pearl Street, P.O. Box 9785
Portland, ME 04104-5085
Tel. (207) 773-5651

David K. Lietz (pro hac vice)
5335 Wisconsin Avenue, NW
Suite 440
Washington, DC 20015
Tel. (866) 252-0878

Counsel for Plaintiffs-Appellants

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Plaintiffs-Appellants submit this Reply Brief to address issues raised by the Mount Desert Island Hospital Inc.'s Appellee's Brief.

ARGUMENT

1. DEFENDANT-APPELLEE'S ARGUMENTS RELATED TO DATA BREACHES SEEKS TO ABSOLVE THOSE WHO ARE IN THE POSITION TO PREVENT A HARM WHEN THEY FAIL TO PROTECT THOSE THEY ARE IN A POSITION TO PROTECT.

As an overarching theme throughout this matter, the question of allocations of risk and duties in a modern information-based society is lurking in the background. Defendant-Appellee characterizes data breaches as everyday events that are essentially the background noise of modern life. Plaintiff-Appellants have stated that they are experiencing substantial fear, alarm, and anxiety that those who have been entrusted with sensitive information are not taking the necessary steps to protect that information. The Court addressed a cousin of this issue in *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 4 A.3d 492 (Me. 2010), with the less personally sensitive data involved with credit cards. It must now, fifteen years later as the world changes to elevate privacy and informational security issues, consider the more serious question of

how we will address those who fail to maintain the security of the most personal information entrusted to them.

Defendant-Appellees seek to characterize the harms that befell Plaintiffs-Appellants as "the typical annoyances or inconveniences that are a part of everyday life" rather than injuries that are the result of its own inadequate protection of sensitive information. Appellee's Br. at 3. This self-serving view denies a basic fact about modern life: privacy is difficult for an individual to maintain, and valuable to sustain. It is valuable, precious, and often at risk such that the security of private information, particularly the most sensitive private information contained in medical records, is something those who are entrusted with this data must take seriously. To downplay and diminish the importance of data security the way the Business and Consumer Court and the Defendant-Appellee do absolves those entrusted to maintain private facts from their failures to adequately vindicate their duties.[1] As a matter of law, but even more as a matter of policy, this is wrong.

[1] Since this case has been on appeal, the Business and Consumer Court has denied a motion to dismiss in *Doe v. Eastern Maine Healthcare Systems d/b/a Northern Light Health*, 2025 WL 283195 (Me. B.C.D. Jan. 9, 2025). In *Doe*, the Court referred to the matter as a non-traditional data breach case because it involved the placement of a "pixel" on the hospital website that transmitted information to Meta, Inc., or more specifically, Facebook. The court, while not addressing standing specifically, did deny

Stepping back and stripping out the jurisprudential minutiae, as a matter of common sense this position taken by Defendant-Appellee and the Business and Consumer Court is untenable. As at least one federal court has noted, to claim there is no injury when a person's sensitive personal information is taken by criminals defies common sense.

> At first glance, this seems an odd case to be arguing about standing and damages. Krupa is not a random plaintiff speculating about future risks of harm or seeking to assert the rights of others—he personally is a victim of a data breach that actually happened. His social security number was stolen, and he alleges that TIC had it been more careful could have prevented the theft. If this were a bank robbery no one would blink. It is a classic adversarial case. The only way TIC can prevail on its motion to dismiss, then, is if it can show that the exposure of Krupa's social security number to hackers was not an injury at all.
>
> And, again at first glance, that seems an odd position to take. Having one's social security number stolen seems an obvious harm. If it were not a harm, why should TIC (or anyone else) take any data security measures? TIC might as well leave its customer lists in a spreadsheet on its website. Then there would be no data breach to report; potential plaintiffs would likely never learn their social security numbers were exposed by TIC; and anyone who did identify and sue TIC over the resulting identity theft could be stymied by proof-of-fact issues as to where the thief got the victim's number. That offends all reason. There is a common-sense expectation—which TIC implicitly recognizes through its attempts at data security—that social security numbers are best kept private

---

Defendant's motion to dismiss on claims for Negligence, Unjust Enrichment, and Violation of the Maine Unfair Trade Practices Act, with analysis that would not appear to be different had it been a traditional data breach case.

> and that their exposure to hackers is a harm (whether or not identity theft has yet occurred).

Krupa v. TIC Int'l Corp., No. 1:22-CV-01951-JRS-MG, 2023 WL 143140, at *2 (S.D. Ind. Jan. 10, 2023) (internal citations omitted). Moreover, a decision not to enforce a duty to secure sensitive data creates a serious moral hazard.

> The Court declines the Defendant's invitation to hold that it had no legal duty to safeguard information even though it had warnings that its data security was inadequate and failed to heed them. To hold that no such duty existed would allow retailers to use outdated security measures and turn a blind eye to the ever-increasing risk of cyber attacks, leaving consumers with no recourse to recover damages even though the retailer was in a superior position to safeguard the public from such a risk.

In re: The Home Depot, Inc., Customer Data Sec. Breach Litig., No.1:14-MD-2583-TWT, 2016 WL 2897520, at *4 (N.D. Ga. May 18, 2016). The Court should avoid the result that permits negligence and protects those who fail to properly safeguard sensitive information entrusted to them.

2. PLAINTIFFS-APPEELLANTS HAVE PROPERLY ALLEGED INJURY IN FACT AND STANDING

Defendant-Appellee states "None of these Plaintiffs have alleged a cognizable injury fairly traceable to an action of MDIH." Appellee's Br. at 5. But Plaintiff Grinnell did allege that she suffered actual misuse and fraud, and all Plaintiffs alleged they "suffered injury from a loss of

privacy the moment that [their] Private Information was accessed and exfiltrated by a third party without authorization." *See, e.g.,* App. at 35 ¶¶ 71-72. Defendant-Appellee and the Business and Consumer Court's assumption that fraudulent charges are reimbursed is both a conclusion outside the pleadings and misses the point. *See id*. at 34 (*citing In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.,* 440 F. Supp. 3d 447, 494-95 (D. Md. 2020) (the trial court "turns the pleading requirement on its head. The pleadings do not indicate that plaintiffs were reimbursed.")); *see also In re Mednax Services, Inc., Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1201 (S.D. Fla. 2022) ("The threat of future identity theft has been considered 'certainly impending' or a 'substantial risk' in cases where plaintiffs have alleged 'actual misuse or actual access to personal data.'").

The point here is that the misuse or fraud, even if otherwise reimbursed, gives credence to the reality of the theft, that this was not some innocent leak, but that Plaintiffs' sensitive data is now actually in the hands of criminals who have taken it for the purpose of using it.[2] *See,*

[2] Plaintiffs-Appellants do not waive any argument about the reality of time spent mitigating injuries as a form of damage. While for most people, and courts, time is money, the Business and Consumer Court does not appear to accept this.

e.g., App. at 30-40 (CCAC) ¶ 39 ("The purpose of exfiltrating Plaintiffs' and Class Members' Private Information is to list it on the black market and sell it. Therefore, it is likely this information is already available on the dark web."); ¶59 ("Plaintiff Buzzell has recently received notices from Equifax, Experian, and TransUnion alerting him to the presence of his sensitive information on the dark web. Additionally, someone attempted to file federal and state tax returns in his name using his Social Security number."); ¶73; ¶102; ¶115. Unlike a credit card data breach, the personal information at issue is durable and will remain in the hands of criminals long after a compromised credit card would be viable to a criminal. *Id.* ¶¶ 143-48. It is hard to imagine how this is not an outcome that represents an injury to the rights and interests of Plaintiffs worse than a compromised credit card.[3]

Courts regularly find that there is a substantial risk of future harm when sensitive PII and PHI are stolen in a data breach, and that this is sufficient for standing. *See, e.g., In re: Netgain Tech., LLC*, No. 21-CV-

[3] Defendant-Appellees and the Business and Consumer Court draw a direct parallel between the inconvenience of a credit card breach, with the limited time frame for exploitation and simple monetary reimbursement, and the diminished privacy one experiences from having sensitive personal information in the hands of criminals. This false equivalency trivializes Plaintiffs' injuries and should be resisted.

1210 (SRN/LIB), 2022 WL 1810606, at *5 (D. Minn. June 2, 2022) ("[C]aselaw supports Plaintiffs' argument that they have adequately alleged a substantial risk of future harm in this case because their PII and PHI was stolen."). This has nothing to do with whether the monetary losses are reimbursed at the time they are incurred, because it is about the likelihood of future harms, which are made more real by the existence of actual misuse. This Court should look similarly toward the future harms that are very real here, and recognize that Plaintiffs have standing.

3. PLAINTIFFS-APPELLANTS HAVE STATED CLAIMS THAT SHOULD SURVIVE A MOTION UNDER RULE 12(b)(6)

Defendant-Appellee relies heavily on *Hannaford*, wherein the Maine Supreme Court, in the context of a credit card data breach, limited recovery for negligence and contract claims in the context of a motion for summary judgment. Again, the injuries to Plaintiffs-Appellees in having their sensitive personal information taken is not the same thing. Whatever privacy right there might be in a credit card number, it is not of the same scope as for social security numbers and other Personally

Identifiable Information and Protected Health Information ("PII" and "PHI").

Defendant-Appellee essentially conceded the necessity of mitigating future harms by providing "credit-monitoring and identity protection services" for a year. Had Plaintiffs purchased this service, these costs would certainly be compensable under *Hannaford*. 4 A.3d at 496 ("A corollary of the mitigation doctrine permits the plaintiff to recover for costs and harms incurred during a reasonable effort to mitigate."). Plaintiffs have alleged they will need to monitor their identity for several years to come. CCAC ¶ 188 ("The 12 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.") Plaintiffs-Appellants should have had the opportunity to make Defendant pay for those extra years of identity coverage to recover for these future costs and harms. By denying them the opportunity to make that claim, the Court has improperly determined that one year of credit

monitoring is enough. That is not a decision that should be made at a motion to dismiss.

Defendant-Appellee compares this case to the Ninth Circuit's "conjectural" discussion concerning drivers' licenses in *Greenstein v. Noblr Reciprocal Exch.*, No. 22-17023, 2024 WL 3886977, at *2 (9th Cir. Aug. 21, 2024). The issue arises out of ambiguity in the notice as to whether or not the information was actually taken. But giving a data breach defendant the power to eliminate standing through the wording of a notice they are legally required to provide subverts the intent of the notice statute.

> If any other person who maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the person shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State **if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur**.

10 M.R.S. § 1348 (emphasis added). Defendant-Appellee now seems to be arguing that Plaintiffs should mitigate the risk of future harm, but should not take this too seriously, that they are not reasonable in ascertaining a *real* risk of future harm and acting to mitigate that risk of

future injury. This is inconsistent both with the notice and the purpose of the notice. Any ambiguity as to the actual exposure can be determined on a more fulsome record, but Plaintiffs-Appellants should be permitted to move forward on the basis of the notice as sufficient evidence that they must expend the resources to mitigate.

Defendant-Appellant's, and the Business and Consumer Court's attitude toward the risk of future harm is unreasonably dismissive. Again, the references to *Hannaford* ignore the differences between a stolen credit card and compromised sensitive personal information. *See, e.g.,* Appellee's Br. at 17-18. Defendant-Appellee's assertions that actual credit card fraud, which is readily reimbursable through a credit card contract process, is the same as the broader categories of harms from identity theft for which there is nobody else in line to reimburse the injured party, misunderstands the difference between the theft in *Hannaford* and the issues properly before this Court. Plaintiffs-Appellees will be dealing with the theft of their Private Information for a lot longer, and much more seriously, than loss of a credit card that is subsequently cancelled. Plaintiffs alleged the risks from identity theft in great detail. CCAC ¶¶ 18, 127-28, 174-86. Plaintiffs alleged that this is not identity

theft like that which occurs with a credit card data breach. *Id.* ¶¶ 132-48. The Business and Consumer Court and Appellant-Defendant's disregarding of these differences and attempts to create a congruence with *Hannaford*, is wrong.

4. THE ECONOMIC LOSS RULE IS NOT INTENDED TO BE COMPLETELY EXCULPATORY

Defendant-Appellee concludes with a mere passing reference to the economic loss rule. While there is no real argument provided here by Defendant-Appellees, Plaintiffs-Appellants will address this newly raised issue.

The Court first addressed the economic loss doctrine in Maine in 1995, in the case *Oceanside at Pine Point Condo. Owners Ass'n v. Peachtree Doors, Inc.*, 659 A.2d 267 (Me. 1995). In *Oceanside,* the Court distinguished between claims in tort and warranty or product liability—issues that are not present here. 659 A.2d at 271 ("Plaintiffs' claims for economic damages—'the costs of all repairs, renovation, corrections and replacements related to the Defendant's defective performance of its contract'—are properly addressable under a warranty theory. The trial court correctly determined that the plaintiffs may not recover for these

damages in tort."). Since that time, the Court has not addressed the so-called economic loss rule

Federal courts applying the Rule as described in *Oceanside* have tended to confine the application to products cases. *See, e.g., Banknorth, N.A. v. BJ's Wholesale Club, Inc.*, 394 F. Supp. 2d 283, 287 (D. Me. 2005) ("Although Maine has adopted the economic loss doctrine in products liability cases, *see Oceanside [ ]*, the Law Court has not yet elucidated its reach beyond the realm of products. Another court in this district has inferred from *Oceanside* that Maine's economic loss doctrine extends to disputes over professional service contracts."); *Maine Rubber Int'l v. Envtl. Mgmt. Group, Inc.*, 298 F. Supp. 2d 133, 137–38 (D. Me. 2004) ("But whatever the applicability of the economic loss doctrine to suits against lawyers and accountants, the logic of *[Oceanside]* encompasses the relationship here. These were two commercial entities able to bargain over the terms of their agreement, and they entered into a written contract to govern their relationship. There was no risk of harm either to people or to other property.").

The result of the Rule is not to immunize a defendant who creates economic harms,[4] but is in effect an election of remedies.

> Almost every breach of contract involves actions or inactions that can be conceived of as a negligent or intentional tort .... if tort law and contract law are to fulfill their distinctive purposes, they must be distinguished where it is possible to do so. The Economic Loss Doctrine serves as a basis for such a distinction.

Pendleton Yacht Yard, Inc. v. Smith, CIV.A. CV-01-047, 2003 WL 21714927, at *3 (Me. Super. Mar. 24, 2003) (quoting *Princess Cruises, Inc. v. Gen. Elec. Co.*, 950 F. Supp. 151, 156 (E.D. Va. 1996)). While this is not a completely binary situation, the Economic Loss Rule would not apply here to eliminate damages if there is no contractual relationship, and damages would be presumed if there was a contractual relationship that was breached. *Id.* (quoting Horton & McGehee, *Maine Civil Remedies* (1991)) ("the circumstances surrounding the contract may give rise to an independent duty to exercise due care or similar duty in tort,

[4] Plaintiffs are not waiving emotional distress, which is outside the Economic Loss Rule's purview. Courts around the country have recognized the emotional harm, anxiety, and stress that victims of data breach suffer and find them to be recoverable. *See In re Mednax Servs., Inc., Customer Data Security Breach Litig.*, 603 F. Supp. 3d at 1203 (the increased risk of identity theft, coupled with the allegations of emotional distress, are sufficient to establish damages); *In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 587 (N.D. Ill. 2022) ("emotional harms such as anxiety and increased concerns for the loss of privacy . . . are recoverable non-economic damages").

in which case a breach may be actionable under both tort and contract theory.")).

The Economic Loss Rule does not absolve Defendant from any and all liability, but it does raise another issue that warrants the Court find damages sufficient to state a claim and to maintain this action. Either in contract or in tort, at least nominal damages are available. *Crosby v. Plummer*, 111 Me. 355, 89 A. 145, 146 (1913) ("The liability of defendant for such breach or omission of duty being shown, the plaintiff is entitled at least to nominal damages."); *Baker v. Farrand*, 26 A.3d 806, 812, n.3 (Me. 2011) ("Nominal damages are recoverable for a violation of a plaintiff's legal right—that is, an 'injury'—when that injury is not accompanied by actual loss or harm, or when the extent of the loss or harm is not proven."). Plaintiffs-Appellants had a right, whether a property right, a contractual right, or a right to expect a duty of care by Defendant-Appellee, to have the security of their sensitive data maintained, and the violation of that right should permit at least nominal damages.

CONCLUSION

The Court should reject Defendant-Appellee's attempts to shed responsibility for failing to live up to its data security duties and remand this matter to the Business and Consumer Court for further adjudication after finding Plaintiffs-Appellants have standing and have stated viable claims.

Respectfully submitted,

/s/*Peter L. Murray*
Peter L. Murray, Maine Bar No. 1135

/s/Richard L. O'Meara
Richard L. O'Meara, Maine Bar. No. 3510

MURRAY, PLUMB & MURRAY
75 Pearl Street, P.O. Box 9785
Portland, ME 04104-5085
Tel. (207) 773-5651
pmurray@mpmlaw.com
romeara@mpmlaw.com

/s/David K. Lietz
David K. Lietz (*pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
dlietz@milberg.com

Counsel for Appellants