STATE OF MAINE
CUMBERLAND, ss.

BUSINESS & CONSUMER DOCKET
DOCKET NO. BCDWB-CV-2020-18

DAWN CHABOT and TAMARA BISBEE, individually and all others similarly situated,	)	
Plaintiffs,	)	ORDER GRANTING CENTRAL MAINE ORTHOPAEDICS' MOTION TO DISMISS PLAINTIFFS' CLASS ACTION COMPLAINT
v.	)	
SPECTRUM HEALTHCARE PARTNERS, P.A. d/b/a CENTRAL MAINE ORTHOPAEDICS,	)	
Defendant.	)	

Plaintiffs Dawn Chabot ("Chabot") and Tamara Bisbee ("Bisbee") ("Plaintiffs"), individually and on behalf all other patients similarly situated, have brought a five count Class Action Complaint against Defendant Spectrum Healthcare Partners, P.A., d/b/a Central Maine Orthopaedics ("CMO") stemming from a phishing attack.[1] Plaintiffs allege *inter alia* that they have been harmed by a phishing attack on a CMO employee's email, that CMO's failure to prevent the phishing attack constitutes a trespass of chattels, and that the theft of their data constitutes a bailment breach. In response to the Class Action Complaint, CMO has filed a Motion to Dismiss contending that Plaintiffs have not pled actual harm, and that Plaintiffs have failed to plead elements necessary to their property tort claims. This case presents the question of what constitutes legally cognizable, actual injury to patients in the wake of a phishing attack on a health care provider's email. For the reasons discussed below, the Court grants CMO's Motion to Dismiss.

[1] Plaintiffs have since filed a First Amended Complaint, also with five counts. The five counts are as follows: Court I: Negligence – Including Negligence Per Se; Count II: Invasion of Privacy; Count III: Breach of Contract; Count IV: Trespass of Chattel; Count V: Bailment.

STANDARD OF REVIEW

In reviewing a motion to dismiss under Rule 12(b)(6), courts "consider the facts in the complaint as if they were admitted." *Bonney v. Stephens Mem. Hosp*., 2011 ME 46, ¶ 16, 17 A.3d 123. The complaint is viewed "in the light most favorable to the plaintiff to determine whether it sets forth elements of a cause of action or alleges facts that would entitle the plaintiff to relief pursuant to some legal theory." *Id*. (quoting *Saunders v. Tisher*, 2006 ME 94, ¶ 8, 902 A.2d 830). "Dismissal is warranted when it appears beyond a doubt that the plaintiff is not entitled to relief under any set of facts that he might prove in support of his claim." *Id*. Although Maine's notice pleading requirements are forgiving, *Desjardins v. Reynolds*, 2017 Me 99, ¶ 17, 162 A.3d 228, conclusory statements, even if factually true, are legally deficient to ward off dismissal if a plaintiff fails to allege sufficient facts. *Carey v. Bd. of Overseers of Bar*, 2018 ME 119, ¶ 23, 192 A.3d 589, as corrected (October 11, 2018). Further, a court is not bound to accept legal conclusions. *Id.*A complaint must allege facts sufficient to demonstrate that a plaintiff has been injured in a legally cognizable way. *America v. Sunspray Condo. Ass'n*, 2013 ME 19, ¶ 20, 61 A.3d 1249 (quoting *Burns v. Architectural Doors & Windows*, 2011 ME 61, ¶ 17, 19 A.3d 823).

FACTS

The operative pleading in this case is the First Amended Complaint ("Amended Complaint" or "Pl.'s Amd. Compl."). According to the Amended Complaint, Spectrum Health Partners, P.A. ("Spectrum") is a Maine corporation with a principal office in Portland, Maine. Plaintiff's Amended Complaint (Pl.'s Amd. Compl.) ¶ 7. Spectrum is Maine's largest statewide multispecialty, physician-owned and -directed professional organization. (Pl.'s Amd. Compl. ¶ 8.) CMO is one of Spectrum's offices and is located in Auburn, Maine. (Pl.'s Amd. Compl. ¶ 9.) Chabot and Bisbee are both current patients of CMO. (Pl.'s Amd. Compl. ¶¶ 5-6.)

On or about November 5, 2019, an unauthorized individual gained access to a CMO employee's email account. (Pl.'s Amd. Compl. ¶¶ 28, 29, Exh. B.) CMO detected the unauthorized access on November 14, 2019. (Pl.'s Amd. Compl. ¶ 30, Exh. B.) CMO conducted an investigation and determined that information about the Plaintiffs may have been contained in the email account. (Pl.'s Amd. Compl. ¶ 27, Exh. B.) The information may have included Plaintiffs' names, dates of birth, addresses, amounts owed to CMO, health insurance information, and other clinical and treatment information related to care received at CMO (the "Information"). (Pl.'s Amd. Compl. ¶ 28, Exh. B.) By letters dated January 10, 2020, CMO notified Plaintiffs of the incident. (Pl.'s Amd. Compl. ¶ 27, Exh. B.)

At some point subsequent to the incident,[2] an unknown actor attempted to login to Chabot's Facebook account. (Pl.'s Amd. Compl. ¶ 73.) Chabot's primary Facebook login credential is her email, which she provided to CMO in the past. *Id.* In order to mitigate the risk of identity theft, Chabot has purchased identity theft protection through McAfee. (Pl.'s Amd. Compl. ¶ 74.) In addition to her out-of-pocket expense, Chabot has expended time and effort to mitigate the risk of identity theft. (Pl.'s Amd. Compl. ¶ 75.)

In December 2019, someone attempted to use Bisbee's debit card five times to get an Uber. (Pl.'s Amd. Compl. ¶ 76(a).) Only one of the five charges went through, but she was reimbursed by the bank. *Id.* Sometime between December 2019 and January 2020, Bisbee's credit card was compromised, but she does not specify how. (Pl.'s Amd. Compl. ¶ 76(b).) Recently, upon applying for a car loan, the credit union informed Bisbee that five additional social security numbers were associated with her name. (Pl.'s Amd. Compl. ¶ 76(c).) Bisbee also reports that she receives notifications that her Apple and Amazon accounts have been compromised (Pl.'s Amd. Compl. ¶

[2] The Amended Complaint does not disclose when.

76(d)), although the Complaint does not specify the manner in which they were compromised. Both accounts use the name, address and email address she provided to CMO. (Pl.'s Amd. Compl. ¶ 76(d).) Finally, Bisbee received a notification from Credit Karma on April 2, 2020 that her data had been compromised, but the Amended Complaint does not specify how or what data was compromised. (Pl.'s Amd. Compl. ¶ 76(e).) In an attempt to mitigate these incidents, Bisbee has purchased identity theft protection through LifeLock. (Pl.'s Amd. Compl. ¶ 77.)

According to the Amended Complaint, CMO wrongfully failed to safeguard its employee's email account and embedded information from unauthorized access. (Pl.'s Amd. Compl. ¶¶ 32, 48, 49-58.) As a result, Plaintiffs (and those similarly situated) claim they now face and will continue to face, a heightened risk of identity theft and fraud for the rest of their lives. (Pl.'s Amd. Compl. ¶ 67.) In particular, Plaintiffs claim they have suffered or are at increased risk of suffering: loss of the opportunity to control how their Information is used; diminution in value of their Information; compromise, publication and theft of their Information; out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud, including the purchase of identity theft protection insurance and detection services; lost opportunity costs and lost wages associated with the time and effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the data disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen Information; the continued risk to their Information, which remains in the possession of CMO and is subject to further breaches as long as CMO fails to undertake appropriate measures to protect the Information in its possession; and current and future costs related to the time, effort, and money that will be expended to prevent, detect, contest, remediate

and repair the impact of the incident for the remainder of Plaintiffs' lives. (Pl.'s Amd. Compl. ¶ 71.)

DISCUSSION

The unauthorized access of a CMO employee's email account on November 5, 2019, constitutes what is commonly referred to as a phishing attack. (Pl.'s Amd. Compl. ¶ 29.) CMO argues that Plaintiffs have failed to allege that the phishing attack caused them actual harm, and thus the Amended Complaint must be dismissed.[3] Plaintiffs contend that the phishing attack itself constitutes actual harm, but if the attack alone is not enough, then Plaintiffs have suffered actual harm in the form of increased risk, out of pocket costs, lost time and effort, and other harms. Most of the issues presented by this case have previously been addressed by this Court's decision in *Gonzales v. Sweetser*, BCD-CV-20-21 (Bus. & Consumer Ct. Oct. 13, 2020), which relies heavily on the Law Court's decision in *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 2010 ME 93, 4 A.3d 492. As discussed below, even in the face of a phishing attack which creates a future risk of identity theft, Maine law requires alleging facts sufficient to plead legally cognizable, actual injury. The first three counts of Plaintiff's Amended Complaint fail to cross this essential threshold and must be dismissed.[4]

I. The Complaint Fails to Allege Facts Sufficient to Establish Actual Injury for Counts I-III.

Legally cognizable, actual injury is a necessary element of negligence (Count I), invasion of privacy (Count II), and breach of contract (Count III). *See Bell ex rel. Bell v. Dawson*, 2013 ME 108, ¶ 17, 82 A.3d 827 (negligence); *Nelson v. Maine Times*, 373 A.2d 1221, 1223 (Me. 1977)

[3] CMO also argues that Plaintiffs have failed to satisfy the pleading requirements of claims for Trespass to Chattels and Bailment.

[4] And as further discussed below, Plaintiffs have failed to make out the elements necessary to support claims in Counts IV and V for Trespass to Chattels and Bailment.

(privacy); *Tobin v. Barter*, 2014 ME 51, ¶ 10, 89 A.3d 1088 (contract); *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 2010 ME 93, ¶ 16, 4 A.3d 492 (implied contract). Time and effort expended to avoid foreseeable harm is not a cognizable injury under Maine law. *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 2010 ME 93, 4 A.3d 492 (applying rule to negligence and implied contracts); *Gonzales v. Sweetser*, BCD-CV-20-21,*6 and n.8 (Bus. & Consumer Ct. Oct. 13, 2020, *Duddy, C.J.*) (extending rule to include invasion of privacy). Here, unlike the plaintiff in *Gonzales*, Bisbee alleges a fraudulent charge (which was reimbursed) occurred to her credit card, and both Chabot and Bisbee allege attempted fraud and identity theft. In these regards, however, Bisbee and Chabot are similar to the plaintiffs in *Hannaford Bros*.

In *Hannaford Bros.*, 2010 ME 93, 4 A.3d 492, data thieves breached Hannaford's computer system and stole a large quantity of financial and other personal identity information pertaining to customers. 2010 ME 93, ¶ 2, 4 A.3d 492. A group of plaintiffs brought a complaint in federal district court against Hannaford seeking damages for the expenditure of time and effort to remedy the disruption of their financial affairs, and for various fees, charges, and lost reward points. *Id.* ¶ 4. The plaintiffs consisted of two groups[5]: those who had never experienced a fraudulent charge as a result of Hannaford's computer system being breached, and those who had experienced fraudulent charges that had been reversed. *Id.* ¶¶ 6, 7. The federal district court certified the question of whether, under the circumstances, time and effort to avoid or remediate reasonably foreseeable harm constitutes a cognizable injury for which damages can be recovered under the Maine law of negligence or implied contract. *Id.* ¶ 1.

[5] In the federal case, there was a third class of plaintiff consisting of a single plaintiff who still had outstanding fraudulent charges. *Id.* at ¶ 6. However, the plaintiff's charges were eventually reimbursed, reducing the number of plaintiff classes to two. *Id.* at ¶ 7.

The Law Court began its analysis by noting that the plaintiffs, including those who had actually experienced fraudulent charges (subsequently reversed), "have suffered no physical harm, economic loss, or identity theft." *Id*. ¶ 8. The Court next confirmed the requirement of Maine law that "actual injury or damage" is an element of both negligence and contract claims. *Id*. ¶ 8. The Court then explained that a plaintiff is only entitled to damages for time and effort to monitor, remediate, and mitigate future harm, when there is actual injury or damage.[6] *Id*. ¶¶ 9-16. Since none of the plaintiffs had experienced actual injury or damage, the Court held that their time and effort expended to avoid reasonably foreseeable harm was not a cognizable injury under the Maine law of negligence or implied contract. *Id*. ¶¶ 14, 16.

The *Hannaford* decision disposes of most, if not all, of the types of injuries claimed by Chabot and Bisbee in this case. Someone attempted to login to Chabot's Facebook account, but there is no allegation the attempt was successful. The one fraudulent charge on Bisbee's credit card was reimbursed. Someone attempted to use Bisbee's debit card, but there is no allegation the attempts were successful. Chabot and Bisbee both expended time and effort mitigating the risk of identity theft, and purchased services to assist in their efforts, but none of those asserted harms rise to the level of legally cognizable, actual injury under *Hannaford*.

Moreover, there are fatal flaws in Plaintiff's factual allegations. Chabot alleges that she uses her email to login to her Facebook account, but there is no allegation that patient email addresses were contained in the Information subject to the phishing attack. Bisbee alleges fraudulent activity with her debit and credit cards, but there is no allegation that patient debit and

[6] The Court notes that in addition to time and effort, the plaintiffs in *Hannaford Bros.* incurred "various fees, charges." *Id.* ¶ 4. Thus, although Plaintiffs in this case incurred out-of-pocket expenses as part of their mitigation efforts, those expenses are not compensable as damages unless a plaintiff has suffered a legally cognizable injury. *See In re Hannaford Bros. Co*., 2010 ME 93, ¶¶ 9-14, 4 A.3d 492. A plaintiff cannot manufacture injury by voluntarily spending money mitigating the possibility of future harm. *See id.*

credit card data were in the Information subject to the phishing attack. Bisbee also alleges issues with social security numbers, but again there is no positive, factual allegation that patient social security numbers were included in the Information subject to the phishing attack.[7] Bisbee's allegations concerning her Apple and Amazon accounts, and the Credit Karma report, are too speculative to infer any nexus to the phishing attack. Notably, neither Plaintiff points to any use or misuse of their clinical and treatment information. Thus, there is no factual basis to support Plaintiffs' specific claims of injury resulting from CMO's failure to prevent the phishing attack.

Plaintiffs' more general allegations of harm fare no better. It follows as a necessary corollary of the *Hannaford* holding, that the risk of future harm is also not a legally cognizable injury. Indeed, the whole premise of the Law Court's reasoning in *Hannaford* is that none of the plaintiffs, including those in the first group who only experienced a "risk of injury," had suffered actual injury or damage as a result of the phishing attack. *Hannaford*, 2010 ME 93, ¶¶ 6, 8. If the time and effort actually incurred to avoid risk of future harm fails as a cognizable injury, even after sensitive customer financial data is exposed to data thieves who hacked into a computer system, then neither the phishing attack itself nor the risk of future harm constitute legally cognizable, actual injury. *See Bernier v. Raymark Industries, Inc.*, 516 A.2d 534, 543 (Me. 1986) (exposure to asbestos is not itself actual injury; a judicially cognizable injury does not occur until there has been a manifestation of physical injury to a person resulting from the exposure); *see also Michaud v. Steckino*, 390 A.2d 524, 530 (Me. 1978) ("a mere possibility" of future pain or suffering or some

[7] Plaintiffs attempt to use a double negative to establish the existence of a positive fact. In Paragraph 30 of the Amended Complaint, Plaintiffs allege that "the notification letter does not represent that Social Security Numbers were not included in the" Information. (Pl.'s Amd. Compl. ¶ 30.) Based on this allegation, Plaintiffs apparently want the Court to infer that social security numbers were contained within the Information. *See, e.g.,* Pl.'s Amd. Compl. ¶ 65. Significantly, however, Plaintiffs fail to allege that they even gave CMO their social security numbers. (Pl.'s Amd. Compl. ¶ 14.) Under the circumstances, it would be unreasonable to infer Plaintiffs' social security numbers were included in the Information. *See Ginn v. Penobscot Co.*, 334 A.2d 874, 880 (Me. 1975) (an inference requires reasonable deduction from proof of other facts).

later injury not sufficient to warrant damages). Accordingly, to the extent Plaintiffs assert they are at risk of experiencing a long list of harms as the result of the phishing attack on CMO, neither the phishing attack itself nor the risk of those harms constitute legally cognizable actual injury.

The only allegations of harm that remain are Plaintiffs' claims for lost opportunity to control how their Information is used; diminution in value of their Information; compromise, publication and theft of their Information; delay in receipt of tax refund monies; and unauthorized use of stolen Information. Under Maine law, however, none of these allegations amount to legally cognizable, actual injury. First, the allegations contain legal conclusions. For instance, it is a legal conclusion that Plaintiffs' Information lost value. The Court is not bound at the motion to dismiss stage to accept conclusions of law as admissions, *Seacoast Hangar Condo. II Ass'n v. Martel*, 2001 ME 112, ¶ 16, 775 A.2d 1166, and therefore the allegation fails to satisfy the requirement for pleading legally cognizable, actual injury.

Second, to the extent these allegations contain factual components, the factual components of the allegations are vague, uncertain, and contingent. For instance, there are no factual details pled as to loss of control; the monetary worth of the Private Information; or whether the Information was actually publicized. Indeed, although CMO is a health care provider, there are no factual details pled as to the use or misuse of Plaintiffs' clinical and treatment data. Further, there are no details alleged regarding whether Plaintiffs are entitled to tax refunds for any specific year, or the extent of the delay in receipt of tax refunds. "Damages must be grounded on established positive facts or on evidence from which their existence and amount may be determined to a probability." *Michaud*, 390 A.2d at 530. In Maine, damages are not recoverable when uncertain, contingent, or speculative. *Id*.; *Wood v. Bell*, 2006 ME 98, ¶ 21, 902 A.2d 843; *Snow v. Villacci*, 2000 ME 127, ¶ 13, 754 A.2d 360; *Gottesman & Co. v. Portland Terminal Co.*,

27 A.2d 394, 395 (Me. 1942). In this case, the general averments of harms are highly speculative, and thus the Complaint fails to allege any legally cognizable, actual injury.

For the reasons set forth above, Court I: Negligence – Including Negligence Per Se; Count II: Invasion of Privacy; and Count III: Breach of Contract are DISMISSED.

II. The Complaint Fails to Allege Facts Sufficient to Establish a Trespass to Plaintiffs' Chattels.

In Count IV, Plaintiffs claim a trespass to chattel has occurred because "they have alleged their [Information] was transmitted to Defendant for a specific purpose, that the [Information] was dispossessed and impaired due to Defendant's negligence underlying the breach, and Plaintiffs and the Class were damaged thereby." (Pl.'s Opp'n to Def.'s Mot. Dismiss 18.) Plaintiffs further claim that by negligently allowing a third-party to access their data, CMO intentionally trespassed on the Information. The Amended Complaint, however, fails to state a claim on which relief can be given for trespass to chattels.

First, the Information is not chattel. A chattel is commonly defined as "[a]n article of personal property, as opposed to real property." *Bahre v. Pearl*, 595 A.2d 1027, 1033-34 (Me. 1991) (citing Black's Law Dictionary 215 (5th ed. 1979)). As such, the term "chattel" is generally used to encompass tangible items. *See Colquhoun v. Webber*, 684 A.2d 405, 409 (Me. 1996) (citing the Restatement (Second) of Torts § 624 cmt. c. (1977) which distinguishes intangible things from chattels); Restatement (Second) of Torts, § 647 cmt. c. (separating intangible things from chattels). When "chattel" is used in reference to intangible items, the intangible item has a tangible component. *See Bahre,* 595 A.2d 1034 (discussing stock certificates as chattel due to the tangible nature of the certificate); *Danton v. Kerr*, CV-18-18, 2018 Me. Super. LEXIS 134, at *12 (Aug. 13, 2018) ("[i]ntangible personal property represented by and/or merged into tangible instruments

or documents may be subject to conversion [and thus trespass to chattels], such as for example intangible interests represented by promissory notes…whether negotiable or non-negotiable, insurance policies and savings bank books. Restatement (Second) of Torts, § 242 cmt. b (1979)"). In this case, the Information consists of digital data attached to an email.[8] The Information lacks a tangible component. Accordingly, the Information does not constitute chattel.

Second, even if the Information can be considered chattel, the tort of trespass to chattel requires wrongful intent. Restatement (Second) of Torts, §§ 216, 217; *see Pearl Investments, LLC v. Standard I/O, Inc.* 257 F. Supp. 2d 326, 354 (D. Me. 2003) (quoting *America Online, Inc. v. IMS*, 24 F. Supp.2d 548, 550 (E.D. Va. 1998) (citing Restatement (Second) of Torts § 217(b) "A trespass to chattels occurs when one party intentionally uses or intermeddles with personal property in rightful possession of another without authorization."). While the common law formerly recognized the ability to trespass a chattel by negligence, the tort has since been limited to intentional acts characterized by a wrongful intent. Restatement (Second) of Torts § 217cmt. b-c (negligent trespasses to chattel are normally governed by the ordinary rules of negligence).

In this case, Plaintiffs have not alleged any facts establishing that CMO engaged in intentional bad acts, i.e. that CMO intentionally allowed or aided a third party's phishing attack. CMO had authorization to possess and use Plaintiffs' Information. (Amd. Cmplt. ¶¶ 14, 25). CMO's alleged negligence may have allowed the Information to be accessed and used by an unauthorized third party, but the alleged negligent conduct does not constitute intentional wrongful use or intermeddling of the Information by CMO. Further, there are no allegations that CMO acted intentionally during the phishing attack. As a result, Plaintiffs have failed to allege facts sufficient to establish the element of intentional action necessary for the tort of trespass to chattels.

[8] Moreover, the Amended Complaint fails to allege whether the Information was stored on a tangible server at the CMO office, at a third party's server like those utilized with "cloud computing," or in some other location.

Plaintiffs resist this conclusion on the strength of *Pearl Invs. LLC v. Standard I/O, Inc.,* 257 F. Supp. 2d 326, 354 (D. Me. 2003)), but the facts of that case are very different. First, the conduct in issue involved physically plugging a server into the plaintiff's router and other hardware.[9] *Id.* at 354. Second, the Court did not need to reach the question of intentional action, because plaintiff's network was unimpaired. *Id.* (quoting *American Online* 24 F. Supp.2d at 550. "One who commits a trespass to a chattel is liable to the possessor of the chattel if the chattel is impaired as to its condition, quality, or value.") Here, there was an unknown, third party, phishing attack on a CMO employee's email, and no allegation that CMO plugged in a server or otherwise flipped a switch allowing the phishing attack to occur. Thus, Plaintiffs can find no support in *Pearl Invs.* for their claim. For all the above reasons, Count IV: Trespass to Chattels is DISMISSED.

III. The Complaint Fails to Allege Facts Sufficient to Establish a Claim for Bailment.

In Count V, Chabot and Bisbee claim that there was a breach of bailment. In support of their claims, Plaintiffs ask the Court to apply *Levesque v. Nanny*, 142 Me. 390, 53 A.2d 703, 703-04 (1947). In *Leveseque,* the plaintiff hung up a coat and gold pin on a row of clothes hooks while she was getting her hair treated by the defendant. *Id*. The navy blue coat had been worn twice, and was worth $69.95, while the gold pin was worth $15.00. *Id.* After her hair services had been completed, the plaintiff went to retrieve her coat and pin, but they were not there. *Id.* She conducted a diligent search for her coat, yet neither coat nor pin could be located.

The *Levesque* Court said for a bailment claim, "[i]t is necessary that there should be proof of actual or constructive delivery of the personalty to the bailee, and acceptance by him for a particular purpose, and upon an express or implied contract." *Id.* at 391-92. The personal property

[9] There is a legal trend of asserting common law torts like trespass to chattels in response to cyberspace activities, but generally the trend is based on digital trespass to physical servers by known actors. *See* Laura Quilter, *The Continuing Expansion of Cyberspace Trespass to chattels*, 17 Berkley Tech. L. J. 421 (2017) (providing an overview of courts application of trespass to chattel in cyberspace).

must be within the defendant's, not the plaintiff's, care. *Id.* When the personal item is delivered to, accepted, and controlled by a defendant, there *must* be a demand for return for the personal property, and evidence of negligence by the bailee (defendant). *Levesque*, 142 Me. at 392, 53 A.2d at 704; *see also Chouinard v. Berube,* 124 Me. 75, 76, 126 A. 180, 180 (1924) (*prima facie* bailment case requires pleading a "refusal to redeliver on demand"); *Levasseur v. Field*, 332 A.2d 765, 767 (Me. 1975) (plaintiff's delivery and defendant's acceptance for *temporary* possession establishes a bailment) *Daigle v. Pelletier*, 139 Me. 382, 31 A.2d 345, 346 (1943) (an essential element of a contract for bailment is an agreement that the property will be returned).[10]

In this case, Plaintiffs fail to allege that return of their Information was a term or part of any contract or agreement between the parties. Plaintiffs also fail to allege that they demanded CMO return their Information to them, and that CMO refused to redeliver the Information. Accordingly, Plaintiffs' are unable to make out a *prima facie* case for bailment. For the foregoing reasons, Count V- Bailment is also DISMISSED.

CONCLUSION

For all the foregoing reasons, CMO's Motion to Dismiss is GRANTED on all counts, and the action is dismissed with prejudice.

Pursuant to M.R. Civ. P. 79(a), the Clerk is instructed to incorporate this Order by reference on the docket for this case.

So Ordered.

Dated: January 14, 2021

/s
Michael A. Duddy
Judge, Business and Consumer Docket

[10] Since there was no establishment of a bailment, the Court need not go further into the bailment analysis.