

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
----------	-------------------------------	------	---------------

Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.
-------	--

Present: The Honorable	BEVERLY REID O’CONNELL, United States District Judge
------------------------	---

Kane Tien

Not Present

N/A

Deputy Clerk

Court Reporter

Tape No.

Attorneys Present for Plaintiffs:

Attorneys Present for Defendants:

Not Present

Not Present

Proceedings: (IN CHAMBERS)

MOTION FOR JUDGMENT ON THE PLEADINGS [42]

On November 5, 2012, Plaintiffs Benjamin Bell and Christopher Spellman filed a class action complaint on behalf of themselves and all other similarly situated against Defendant Blizzard Entertainment, Inc. (Dkt. 1.)¹ The Complaint alleges eight causes of action: (1) violation of the Delaware Consumer Fraud Act (“CFA”) on behalf of the Authenticator Class, (2) violation of the CFA on behalf of the August 4 Class, (3) Unjust Enrichment on behalf of the Authenticator class, (4) Unjust Enrichment on behalf of the August 4 Class, (5) Negligence Per Se, (6) Negligence, (7) Breach of Contract, and (8) Bailment. Defendant brought this Motion for Judgment on the Pleadings for all claims, or in the alternative dismissal of Counts I and II under Rule 9(b). (Dkt. 42.) For the reasons set forth below, the Court **GRANTS** in part and **DENIES** in part Defendant’s Motion.

I. FACTUAL BACKGROUND

Defendant Blizzard is a video game developer that produces a variety of video games, ranging in price from \$14.99 to almost \$200.00. (Compl. ¶ 17.) Blizzard’s video games include Diablo, StarCraft and World of Warcraft. Purchasers of Defendant’s games are required to create a “Battle.net” account before playing any Blizzard game. (*Id.* ¶ 18.) To create a Battle.net account, a customer must provide personal information such as his or her full name, date of birth, and e-mail address. (*Id.* ¶ 21.) Additionally,

¹ The original complaint named an additional defendant, Activision Blizzard Inc., which was subsequently dismissed from the litigation. (Dkt. 38).

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

users must create a password and provide an answer to a “secret question,” such as “Your city of birth” or “Name of your first pet.” (*Id.*) Battle.net has a feature known as “Battle.net Balance,” which allows account holders to add funds to their Battle.net accounts in order to purchase supplementary goods and services from Defendant. (*Id.* ¶ 20.) However, using the Battle.net Balance feature requires additional personal information, including a credit card number, credit card expiration date, billing address, and phone number. (*Id.* ¶ 22.)

When registering a Battle.net account, account holders agree to the Battle.net Terms of Use (“TOU”) and Blizzard Privacy Policy (“Privacy Policy”). (*Id.* ¶ 23; Notice of Errata Ex. A (Ex. C))². The Privacy Policy provides assurances that Defendant will take steps to securely store any personal information collected. (*Id.* ¶ 24.) Despite this, account holders have experienced security breaches of their Battle.net accounts, commonly referred to as “hacks.” (*Id.* ¶¶ 3, 29–31, 35.)

In 2008, in an effort to increase account security, Blizzard introduced the “Authenticator.” (*Id.* ¶ 26.) Authenticators create a random code which account holders must enter when logging in, providing an extra layer of security beyond the username and password. (*Id.*) Authenticators come in two forms: a physical keychain (“Key Ring Authenticator”) or a downloadable smart phone app (“Mobile Authenticator”). (*Id.* ¶ 27.) The Key Ring Authenticator costs \$6.50, while the Mobile Authenticator is free. (*Id.*)³

On August 4, 2012, Defendant became aware that hackers had gained access to account holders’ information (“August Breach”). (*Id.* ¶¶ 35–36.) Five days later, on August 9, 2012, Defendant announced the August Breach to Battle.net account holders through a post on its company website. *Id.* During the August Breach, hackers gained access to Battle.net account holders’ e-mail addresses, answers to personal security

² Plaintiffs’ original complaint was filed with no exhibits attached. To remedy this, they filed a Notice of Errata. (Dkt. 4.) To avoid confusion, the Court will cite to specific sections of the TOU when referencing this exhibit.

³ Plaintiffs provide conflicting information as the price of the Mobile Authenticator. (*Compare* Compl. ¶ 27 (“the cost for a Mobile Authenticator varies depending upon the mobile device”); *with* Compl. ¶ 31 (Battle.net Mobile Authenticator is “a free app”).

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

questions, and cryptographically scrambled versions of Battle.net passwords. (*Id.*) Hackers also accessed information that could potentially compromise the integrity of Mobile Authenticators. (*Id.* ¶ 37.)

On May 21, 2012, Plaintiff Bell had purchased Diablo III and created a Battle.net account. (*Id.* ¶ 9.) Bell has not purchased or acquired an Authenticator. (*Id.*) Plaintiff Spellman has video games in all of Defendant’s major franchises: Diablo, StarCraft, and World of Warcraft. (*Id.* ¶ 10.) Spellman has owned a Battle.net account since 2004 and has both a Mobile Authenticator and Key Ring Authenticator. (*Id.*)

Bell and Spellman purport to represent two classes: (1) a class consisting of all United States residents who purchased a Blizzard game after the introduction of the Authenticator in 2008 (“Authenticator Class”), and (2) a class consisting of all United States residents whose private information was stolen during the August 4, 2012, data breach (“August 4 Class”). (*Id.* ¶ 60.)

Plaintiffs brought the instant suit alleging various theories of fault for Defendant’s failure to protect Class members’ personal information.

II. LEGAL STANDARD

After the pleadings are closed but early enough not to delay trial, any party may move for judgment on the pleadings. Fed. R. Civ. P. 12(c). The standard applied to a Rule 12(c) motion is essentially similar to that applied on Rule 12(b)(6) motions; all allegations of fact by the party opposing the motion are accepted as true and the complaint is construed in the light most favorable to them. *McGlinchey v. Shell Chemical Co.*, 845 F.2d 802, 810 (9th Cir. 1988). However, “conclusory allegations without more are insufficient to defeat a motion [for judgment on the pleadings].” *Id.*

As with Rule 12(b)(6) motions, “[g]enerally, a district court may not consider any material beyond the pleadings[.] . . . However, material which is properly submitted as part of the complaint may be considered.” *Hal Roach Studios, Inc. v. Richard Feiner & Co.*, 896 F.2d 1542, 1555 n.19 (9th Cir. 1990) (citations omitted); William W Schwarzer, et al., California Practice Guide: Federal Civil Procedure Before Trial (“Rutter Guide”)

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

§ 9:339.1 (2005). Similarly, “documents whose contents are alleged in a complaint and whose authenticity no party questions, but which are not physically attached to the pleading, may be considered in ruling on a Rule 12(b)(6) motion to dismiss[,]” or on a Rule 12(c) motion, without converting the motion into a motion for summary judgment. *Branch v. Tunnell*, 14 F.3d 449, 454 (9th Cir. 1994) (citing *Romani v. Sherson Lehman Hutton*, 929 F.2d 875, 879 n. 3 (1st Cir. 1991)). If the documents are not physically attached to the complaint, they may be considered if their “authenticity . . . is not contested” and “the plaintiff’s complaint necessarily relies” on them. *Parino v. FHP, Inc.*, 146 F.3d 699, 705–06 (9th Cir. 1998). “The district court will not accept as true pleading allegations that are contradicted by facts that can be judicially noticed or by other allegations or exhibits attached to or incorporated in the pleading.” 5C Wright & Miller, *Federal Practice & Procedure* § 1363 (3d ed. 2004).

III. ANALYSIS

As a preliminary matter, neither party has briefed the proper choice of law to be applied in this case. However, at this “stage in the litigation—before the parties have submitted briefing regarding either choice-of-law or class certification—plaintiff is permitted to assert claims under the laws of different states in the alternative.” *Donohue v. Apple, Inc.*, 871 F. Supp. 2d 913, 923 (N.D. Cal. 2012). Because both Plaintiffs and Defendant argue the present motions under Delaware law, the Court assumes that Delaware law applies to all class members’ claims.⁴ *See In re Toyota Motor Corp. Hybrid Brake Mktg., Sales, Practices & Prods. Liab. Litig.*, 890 F. Supp. 2d 1210, 1216 n.6 (C.D. Cal. 2011) (holding that choice of law would be decided on a later motion for class certification and applying California law to non-resident Defendants where Plaintiff did not contest that law’s application).

⁴ Although the TOU specify that Delaware law will govern all disputes arising from the contract, Defendants reserve the right to assert that California law is applicable in later proceedings. *See Mtn* at p.6 n.4 (TOU §17(A)).

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

A. Counts I and II (CFA)

In Count I, Plaintiffs allege violations of the Delaware Consumer Fraud Act (“CFA”) on behalf of the Authenticator Class, and in Count II allege violations of the CFA on behalf of the August 4 Class. Both counts assert that Defendant violated the CFA by omitting or misrepresenting the quality of its security protocols.

Under Delaware law, “The act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, or the concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, *in connection with the sale*, lease or advertisement of any merchandise, whether or not any person has in fact been misled, deceived or damaged thereby, is an unlawful practice.” 6 Del. C. § 2513(a) (emphasis added). Courts “cannot ignore the clear language of the statute which restricts its application to deceptive practices ‘in connection with the sale or advertisement’ of the merchandise.” *Norman Gershman’s Things to Wear, Inc. v. Mercedes-Benz of North America, Inc.*, 558 A.2d 1066, 1074 (Del. Super. Ct. 1989).

Fraud in Delaware “depart[s] from the common law in the following ways: (1) a negligent misrepresentation is sufficient to violate the statute, (2) a violation of the statute is committed regardless of actual reliance by the plaintiff, and (3) the plaintiff need not show intent [by the defendant] to induce action or inaction by the plaintiff.” *Eames v. Nationwide Mut. Ins. Co.*, 412 F. Supp. 2d 431, 437 (D. Del. 2006) (internal quotation marks omitted).

Further, because violation of the CFA, 6 Del. C. §2511 *et seq.*, is a claim sounding in fraud, it must be plead with particularity. *See* Fed. R. Civ. P. 9(b); *Vess v. Ciba-Geigy Corp. U.S.A.*, 317 F.3d 1097, 1107 (9th Cir. 2003) (holding that a district court may dismiss any claim grounded in fraud for failing to satisfy Rule 9(b)); *In re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1424 (3d Cir. 1997) (“While dismissal on Rule 12(b)(6) alone would not have been proper, the dismissal on Rule 9(b) grounds was.”).

Both counts assert the same violations of the CFA. Defendant violated the CFA by: (1) misrepresenting the quality of its security protocols; (2) failing to disclose that

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

consumers would need to provide private information to play Defendant’s games; and (3) failing to disclose that consumer’s private information would be at increased risk of theft unless an Authenticator was purchased.⁵ (*Compare* Compl. ¶¶ 72, 73, *with* Compl. ¶¶ 78, 79.)

1. Misrepresentation of Security Quality

Plaintiffs claim that Defendant made assurances that account holders’ private information will remain “completely secure”. (Compl. ¶ 23.) However, the Blizzard Privacy Policy, on which Plaintiffs base this assertion, clearly states that “Blizzard has *taken steps* to assure that all information collected will remain secure.” *Id.* ¶ 24 (emphasis added). The Privacy Policy goes on to provide that “access to all Personal Information is strictly controlled.” *Id.*

Plaintiffs do not allege facts showing that Blizzard failed to take steps to ensure the security of account holders’ personal information or that access to that information was not strictly controlled. The Court finds that, under the alleged facts, Defendant did not fraudulently misrepresent the security of Plaintiffs’ personal information.

2. Failure to Inform Consumers That They Must Provide Private Information to Play Defendant’s Game

Plaintiffs also allege that although Defendant’s video game box points out that users must sign up for a Battle.net account to play Defendant’s video game, it does not reveal that signing up for a Battle.net account entails providing personal information. (Compl. ¶¶ 25, 73.) However, all that is required to sign up for a Battle.net account is an e-mail address, password, and an answer to a security question. Defendant’s failure to disclose that such information must be provided before playing cannot plausibly be an omission of a material fact in violation of the CFA. Although users may later choose to

⁵ Count II asserts an additional violation of Delaware’s Data Breach Notification laws under 6 Del. C. § 12B-101, *et seq.* This alleged violation is better discussed in Count V, under negligence *per se*, because that count deals exclusively with the Data Breach Notification statute.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

add features such as Battle.net Balance, which requires entering credit card information, any omission related to additional features is not made “in connection with the sale”

3. Failure to Inform Consumers That an Authenticator is Required for Account Safety

Additionally, Plaintiffs contend that Blizzard should have disclosed that to have security in their account safety, Battle.net account holders had to purchase an Authenticator. (Compl. ¶ 72.) Plaintiffs point out that Defendant’s Privacy Policy, which was provided at the point of purchase of Defendant’s video games, makes no mention of how often Battle.net accounts are hacked, despite Defendant’s acknowledgement that accounts are hacked much more commonly when new games are launched. (Compl. ¶¶ 51, 31.)

At the hearing on this matter, Defense counsel urged the court to examine Footnotes 14 and 15 of the Complaint, which are articles showing that hacks affecting Battle.net account holders are the result of individual security issues rather than a problem with Defendant’s security. (*Id.* ¶ 30 n.14; ¶ 31 n.15.) However, an examination of these footnotes and the arguments contained in Defendant’s motion fails to provide any explanation for why Defendant omitted telling consumers about Authenticators at the point of sale; particularly when Defendants admittedly knew that many Battle.net account holders experienced hacks that an Authenticator would protect against.

Accordingly, because the Defendant failed to provide any explanation for how it’s omissions regarding the necessity of an authenticator for account safety does not violate the CFA, the Court **DENIES** Defendant’s motion for judgment on the Pleadings for Counts I and II.

B. Counts III and IV (Unjust Enrichment)

In Counts III and IV, Plaintiffs allege that Defendant was unjustly enriched when it sold products that lost value as a result of the security breaches, and then passed costs associated with system security on to Class members. (Compl. ¶¶ 92–94, 100–103.)

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

Under Delaware law, an unjust enrichment claim has five elements: (1) enrichment, (2) impoverishment, (3) relationship between the enrichment and impoverishment, (4) absence of justification, and (5) absence of a remedy provided by law. *BAE Sys. Info. & Elec. Sys. Integration v. Lockheed Martin Corp.*, 2009 Del. Ch. LEXIS 17, *25–26 (Del. Ch. Feb. 3, 2009). When breach of contract and unjust enrichment claims are pled as alternative theories of recovery, the two claims “*may* survive a motion to dismiss.” *Narrowstep, Inc. v. Onstream Media Corp.*, 2010 Del. Ch. LEXIS 250, *55 (Del. Ch. Dec. 22, 2010) (emphasis in original). However, “if a contract comprehensively governs the parties’ relationship, then it alone must provide the measure of the plaintiff’s rights and any claim of unjust enrichment will be denied.” *BAE Sys.* 2009 Del. Ch. LEXIS 17, at *26.

In Counts III and IV, Plaintiffs contend that Defendant accepted monetary benefits for its video games but failed to abide by the assurances made in the Privacy Policy. This allegedly resulted in an unjust enrichment because Plaintiffs have not received the full benefit of the contract. (*See* Compl. ¶¶ 93–95.) Accordingly, Plaintiffs base their unjust enrichment claim on the contractual terms of the TOU and the Privacy Policy and claim no relationship with Defendant outside of their contractual relationship. Therefore, the “contract comprehensively governs the parties’ relationship.” *BAE Sys.* 2009 Del. Ch. LEXIS 17, at *26.⁶

Plaintiffs rely on *Narrowstep*, claiming that an unjust enrichment claim can be maintained when the allegations of that claim are interrelated with a fraud claim, notwithstanding the parties have entered into a contract. 2010 Del. Ch. LEXIS 250, at *59 (allowing both a breach of contract claim and unjust enrichment claim to proceed where, during a merger, Defendants fraudulently represented their intention to merge in

⁶ Notably, the Count III allegations of unjust enrichment, on behalf of the Authenticator Class, do not allege that Defendant has been enriched by Authenticator Class members’ purchases of Authenticators. No contract in evidence governs the purchase of Authenticators; therefore, any such purchase might be used to show unjust enrichment. However, the Authenticator Class is not comprised of individuals who have purchased an Authenticator. (Compl. ¶ 60.) Instead, it is comprised of people who signed up for Battle.net accounts after Defendants began offering Authenticators for sale. (*Id.*) Accordingly, there is no evidence of a transaction that gives rise to an extra-contractual relationship between Plaintiffs and Defendant.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

order to steal Plaintiff’s customers). However, in *Narrowstep*, the alleged fraud was not limited to the terms of the contract, but instead included representations made outside of the contract. *Id.* Conversely, here, the alleged fraud is wholly based upon misrepresentations and omissions made within Defendant’s TOU and Privacy Policy, and the Defendant has made no representations to Class members outside of those found in the contract.

Accordingly, because Plaintiffs have failed to challenge Defendant’s conduct on a basis not comprehensively governed by a contract, the Court **GRANTS** Plaintiffs’ Motion for Judgment on the Pleadings on Counts III and IV.

C. Count V (Negligence Per Se)

In Count V, Plaintiffs allege that the Defendant was negligent *per se* for failing to inform Battle.net account holders of the August Breach in a timely manner, as required by 6 Del. C. §12B-101 *et seq.* (“Data Breach Notification Law”). (Compl. ¶ 112.) The alleged delay in notification prevented Plaintiffs from taking remedial steps to protect their private information after the August Breach. (*Id.* ¶ 111.)

In Delaware, “negligence *per se* requires the defendant to have committed an unexcused violation of a statute or regulation.” *Hudson v. Old Guard Ins. Co.*, 3 A.3d 246, 251 (Del. 2010). Delaware’s Data Breach Notification Law requires notice to be given as soon as possible after an investigation determines that the misuse of a Delaware resident’s personal information has occurred, or is reasonably likely to occur. 6 Del. C. §12B-102. The Data Breach Notification Law defines personal information:

4. “Personal information” means a Delaware resident’s first name or first initial and last name in combination with any 1 or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted:
 - a. Social Security number;
 - b. Driver’s license number or Delaware Identification Card number; or

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

c. Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident’s financial account.”

6 Del. C. § 12B-101. Accordingly, the duty to notify is triggered only if “personal information” was accessed during the August Breach.

Here, Plaintiffs fail to allege that personal information, as defined by the Delaware statute, was taken. Although Plaintiffs use the shorthand “Personal Information” in their Complaint and Opposition to mean “sensitive personal, private, and financial data,” and claim that such “Personal Information” was taken, they do not plead facts showing that Class members’ names, social security numbers, driver’s license numbers, or credit card numbers were illegally accessed. (Compl. ¶ 1.)

Plaintiffs point to a press release by Blizzard stating that “the hackers had gained access to e-mail addresses, answers to personal security questions, and ‘cryptographically scrambled versions of Battle.net passwords’” as well as “information . . . that could potentially compromise the integrity of North American Mobile Authenticators.” (Compl. ¶¶ 36, 37.) However, the press release goes on to state that “[a]t this time, there’s no evidence that financial information of any kind has been accessed. This includes credit cards, billing addresses, names, or other payment information.” (*See* Compl. ¶ 37 n.23.) Plaintiffs never allege that any additional information was taken or that Blizzard misrepresented the extent of the data accessed in the August Breach.⁷

Further, the Complaint does not specify what additional personal information would be accessed if hackers deciphered the stolen passwords and gained access to Battle.net accounts. Absent an assertion of what information, personal or otherwise, is displayed when logging into a Battle.net account, it is unclear how a hacker’s illegal

⁷ Plaintiffs point to an internet source that claims that the server-side verifier database was also taken. (Compl. ¶ 39.) However, Plaintiffs never assert that this actually happened. Instead, Plaintiffs point out that hackers have obtained illegal access to accounts after the breach. (*Id.* ¶ 43.) However, because hackers also obtained access to user accounts before the August Breach, there is not even an inference that, during the August Breach, more user information was accessed than what was disclosed by Defendant.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

access of a Battle.net account triggers a duty to provide a breach notification under Delaware law.

Therefore, Plaintiffs only allege that their e-mail address, secret question answers, and cryptographically scrambled passwords were taken during the August Breach. This is not “personal information” within the plain text of the statute. Accordingly, Count V is **DISMISSED** with leave to amend.

D. Count VI (Negligence) and Count VII (Breach of Contract)

In Counts VI and VII, Plaintiffs allege that Defendant negligently safeguarded Class members’ private information and, in doing so, breached the terms of their contract with Class members. (Compl. ¶¶ 118, 131.) Because Plaintiffs allege identical harm in both claims, and Defendant challenges only the harm element of each claim, the Court analyzes these claims together. (See Compl. ¶¶ 127, 132.)

Under Delaware law, the elements of negligence are “duty, breach, causation, and harm.” *Hudson*, 3 A.3d at 251. To show breach of contract, the plaintiff must show the existence of a contract, a breach of an obligation imposed by that contract, and resultant damage to the plaintiff. *VLIW Tech., LLC v. Hewlett–Packard Co.*, 840 A.2d 606, 612 (Del. 2003).

In both counts, Plaintiffs allege that they were harmed because their Private Information was compromised, viewed, and/or stolen. (Compl. ¶¶ 125, 131.) Plaintiffs claim that they suffered actual harm because their personal information was stolen and they incurred actual damages in the form of expenses for credit monitoring, anxiety, emotional distress, loss of privacy, and the diminution in the value of their video games.⁸

⁸ Defendant contends that damages for anxiety and emotional distress are not applicable to this case, absent a physical injury. *E.I. DuPont de Nemours & Co. v. Pressman*, 679 A.2d 436, 444-45 (Del. 1996) (“Damages for emotional distress are not available for breach of contract in the absence of physical injury”); *Mergenthaler v. Asbestos Corp. of Am.*, 480 A.2d 647, 651 (Del. 1984) (holding that any claim for mental anguish requires physical injury). Additionally, Defendant points out that, under Delaware law, invasion of privacy is tort of its own, rather than a measure of damages. See, e.g., *Fanean v. Rite Aid Corp. of Del., Inc.*, 984 A.2d 812 (Del. Super. Ct. 2009) (allowing separate causes of action for negligence and invasion of privacy). Because Plaintiffs do not oppose this position in their Opposition,

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

(Compl. ¶¶ 127, 132.) Defendant attacks these claims by asserting that Plaintiffs cannot satisfy the harm element of each respective claim.

1. Increased Risk

Plaintiffs do not allege they have been the victims of identity theft.⁹ Rather, they assert they were harmed because their Private Information was subjected to hackers, creating an increased risk of identity theft. (Compl. ¶¶ 5; 58–59.) Specifically, Plaintiffs claim they incurred credit monitoring expenses incurred to protect themselves from potential identity theft. (Compl. ¶ 127.)

A Delaware court has noted that in cases where personal identifying information has been negligently released, courts have dismissed “purported class actions in which plaintiffs seek damages for the loss of personal identification information through accident or theft.” *Slaughter v. AON Consulting, Inc.*, 2012 Del. Super. LEXIS 91, *6–7 (Del. Super. Ct. Jan. 31, 2012) (internal quotation marks and citations omitted). In *Slaughter*, the court dismissed a similar claim, where 22,000 retirees’ personal information, including their Social Security Numbers, was posted on a public website and accessed by Chinese computer servers. *Id.* at *1. Although this situation was “new to Delaware,” the court examined “the nationwide string of similar cases” and concluded that the claims should be dismissed because, while “the string of cases is troubling,” “the string of dismissals is unbroken.” *Id.* at *7, 10; *see Cooney v. Chi. Pub. Schs*, 943 N.E.2d 23, 31 (Ill. App. Ct. 1st Dist. 2010) (“the purchase of these [credit monitoring] services, without more, is not an economic injury”); *Pisciotta v. Old Nat’l Bancorp*, 499 F.3d 629,

the Court deems this point conceded. *See Canatella v. Stovitz*, 365 F.Supp.2d 1064, 1083-84 (N.D. Cal. 2005) (holding that a point is apparently conceded where no response is offered in opposition). Additionally, although Plaintiffs claim in their Opposition that they seek “the cost of the Key Ring Authenticator” as damages, the complaint clearly reveals that this is not the case. (*See Opp’n.* at 16; Compl. ¶¶ 127, 132.)

⁹ Plaintiffs assert that after the August Breach, various potential Class members have had their Battle.net accounts illegally accessed. (Compl. ¶ 43, 58.) However, it does not appear to the Court that the unauthorized access of an online video game account is what Plaintiffs mean by “identity theft”.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

639 (7th Cir. 2007) (“[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy”).

Plaintiffs fail to cite to a case that holds that increased risk of future harm, in the context of identity theft, is a type of harm sufficient to support a negligence claim. Instead, Plaintiffs only point to medical cases that recognize the increased risk of future harm in the context of a strong public health concern. *See Shepard v. A.C. & S. Co.*, 498 A.2d 1126, 1134 (Del. Super. 1985) (“latent disease cases justify a change in our perception . . . of inherently unknowable claims”); *United States v. Anderson*, 669 A.2d 73, 78 (Del. 1995) (“Plaintiff’s life expectancy has been shortened because he has a higher risk of death from testicular cancer. Accordingly, he should be compensated.”). The risk of future identity theft does not present the same public health concerns as in *Shepard* or *Anderson*, and instead fits squarely into the holding of *Slaughter*.

2. Diminution of Video Game Value

Plaintiffs allege that the value of the video games they purchased from Defendant has decreased as a result of the data breaches. Defendant contends this type of damage is barred in Count VI, for negligence, by the economic loss doctrine and, in Count VII, for breach of contract, because any such damage is speculative at this point.

a. Economic Loss Doctrine

The economic loss doctrine prohibits recovery in tort where a product has damaged only itself, causing a purely economic injury rather than personal or property damage. *Sycamore Farms, Inc. v. Barnes Elec., Inc.*, 2011 Del. Super. LEXIS 470, *2 (Del. Super. Oct. 20, 2011). However, “[t]he threshold issue for determining whether the economic loss doctrine applies is whether the defendant breached a duty independent of its contractual obligations.” *Id.* at *3. “[W]here an action is based entirely on a breach of the terms of a contract between the parties and not on a violation of an independent duty imposed by law, a plaintiff must sue in contract and not in tort.” *Edelstein v. Goldstein*, 2011 Del. Super. LEXIS 86, *23 (Del. Super. Ct. Mar. 1, 2011).

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

Here, Plaintiffs admit that the duty to safeguard Class members’ information was created by contract. (Compl. ¶¶ 23–24, 129.) Plaintiffs have not pleaded any facts showing that a duty to safeguard Class members’ information arose independently as a matter of law. Accordingly, because the duty in this case is contractual, Plaintiffs may not recover damages resulting from the diminution of the video games’ value asserted in a tort claim, such as negligence.

b. Speculative Damages

In Count VII, Plaintiffs contend that the constant threat of cybercriminal hacks has lowered the value of the video games they purchased. (Compl. ¶ 126.) Defendant avers that the alleged diminution in value of the video games is speculative because Plaintiffs have not, and cannot, resell the games they have purchased from Defendant. *See Dalton v. Ford Motor Co.*, 2002 Del. Super. LEXIS 132, *22–23 (Del. Super. Ct. Feb. 28, 2002) (holding that Plaintiffs could not assert damages based on the speculative diminution of value of their Ford vehicle, which resulted from a wiring defect with only the potential to cause future damage).

Plaintiffs admit that “the appropriate measure of damages is the difference between the value of the [product] before the breach and the value of the [product] after the breach.” Opp’n at p. 21 (citing to *Devincentis v. European Performance, Inc.*, 2012 Del Super. LEXIS 200, *14–15 (Del. Super. Apr. 17, 2012)). Because the governing contract does not allow Battle.net users to sell or transfer their accounts, the resale value of Plaintiff’s games both before and after the August Breach was effectively zero. (Notice of Errata Ex. A at 52 (Ex. C) (TOU §9(B)).)

Accordingly, Plaintiffs cannot show that they have suffered any harm. Rather, any harm suffered as a result of the August Breach is speculative. The court **GRANTS** Defendant’s motion for judgment on the pleadings for COUNT VI and VII with leave to amend.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

E. Count VIII (Bailment)

In Count VIII, Plaintiffs allege that a duty of bailment arose when Class members deposited their personal information with Defendant in order to create a Battle.net account. (Compl. ¶¶ 134, 135.) Class members could then terminate the bailment by closing their Battle.net account. (Notice of Errata Ex. A, at 60 (Ex. C.))¹⁰

Under Delaware law, “[a] bailment occurs when one party retains legal title to a chattel but control and possession of the property is transferred to the bailee.” *Golt by Golt v. Sports Complex*, 644 A.2d 989, 992 (Del. Super. Ct. 1994); *see also Lee Tire & Rubber Co. v. Dormer*, 108 A.2d 168, 170 (Del. 1954).

No court has held that personal information is a chattel that can be bailed. Plaintiffs incorrectly rely on *Rinaldi v. Iomega Corp* for the proposition that data stored on a computer drive is personal property. 1999 Del. Super. LEXIS 563 (Del. Super. Ct. 1999). In *Rinaldi*, external computer drives became corrupted as a result of a design defect, rendering any data stored on them inaccessible. *Id.* at *2. However, the *Rinaldi* court never took into account whether the data itself was considered personal property because the physical device on which the data was stored met that description.¹¹

¹⁰ Plaintiffs’ position is that terminating a Battle.net account triggers Defendant’s duty to delete any personal information utilized in the account’s creation, thus ending the bailment. However, the TOU clearly state that “[i]n some cases we may not be able to delete your personal information and will retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.” (Notice of Errata Ex. A at 60 (Ex. C.)) This further supports the fact that there is no bailment relationship between Plaintiffs and Defendant, because Plaintiffs could not retrieve the bailment.

¹¹ Plaintiffs’ reliance on *Bridge Tower Dental, P.A. v. Meridian Computer Ctr., Inc.*, 272 P.3d 541 (Idaho 2012) likewise is misplaced. In that case, a bailment was created when plaintiff gave defendant two hard drives—one that was failing and another that was in good condition with patient data files mirrored from the first—with the expectation that defendant replace the failing hard drive with a functional hard drive containing the proper data. As such, the scope of the bailment necessarily included not just the two hard drives, but also the data contained on them. When defendant erased the data on the functional, mirrored hard drive, the court held that the property was returned in a damaged state. That situation is not analogous to this case—here, the compromise of the data’s security does not mean that the data embodies an analogous damaged state and the information contained in patient files is unlike

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

Further, because Plaintiffs allege in Count VIII that Defendant negligently breached a duty of care to safeguard Plaintiffs' private information as provided by contract, the claim for bailment is duplicative of the negligence and breach of contract claims. *See Colbert v. Goodville Mut. Cas. Co.*, 2010 Del. Super. LEXIS 270, *9 (Del. Super. Ct. June 30, 2010) (dismissing a tort claim because "the basis of the [tort] claim is nearly identical to the basis of the plaintiff's contract claims"); *Pandisc Music Corp. v. Red Distrib., LLC*, 2005 U.S. Dist. LEXIS 4336, *3–4 (S.D.N.Y. Mar. 18, 2005) (dismissing a bailment claim as duplicative of a breach of contract claim); *D'Napoli Food Prods. v. Wisconsin Farm Lines*, 1985 U.S. Dist. LEXIS 23758, *3–4 (N.D. Ill. May 16, 1985) (dismissing a bailment claim as duplicative of both the breach of contract and negligence claims).

Accordingly, the Court **GRANTS** Defendant's motion to dismiss Count VIII with prejudice.

IV. CONCLUSION

For the foregoing reasons, the court **GRANTS** in part and **DENIES** in part Defendant's Motion for Judgment on the Pleadings. Specifically, Defendant's Motion with respect to:

1. Count I for violations of the CFA is **DENIED**.
2. Count II for violations of the CFA is **DENIED**.
3. Count III for Unjust Enrichment is **GRANTED** with leave to amend.
4. Count IV for Unjust Enrichment is **GRANTED** with leave to amend.

personal identifying information such as an e-mail address and password. *Bridge Tower* does not directly support the proposition that personal information can be chattel that is subject to a bailment. Moreover, that case was decided under Idaho law, while the present case is a California court applying Delaware law.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	12-CV-09475 BRO (PJWx)	Date	July 11, 2013
Title	Benjamin Bell, et al. v. Blizzard Entertainment, Inc.		

5. Count V for Negligence Per Se is GRANTED with leave to amend.
6. Count VI for Negligence is GRANTED with leave to amend.
7. Count VII for Breach of Contract is GRANTED with leave to amend.
8. Count VIII for Bailment is GRANTED and the claim is dismissed with prejudice.

IT IS SO ORDERED.

Initials of
Preparer

:

KTI
